GÜVEN VEREN TEKNOLOJİ

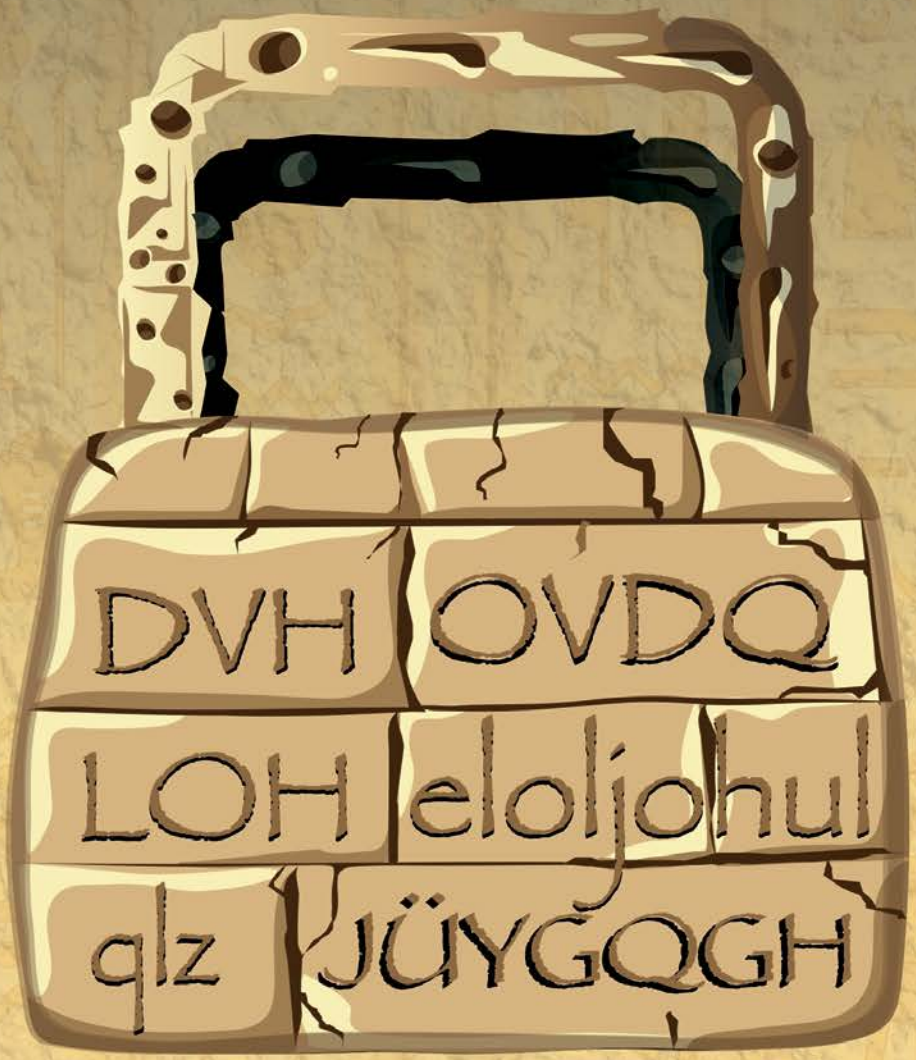
SAYI 121 / ARALIK 2024

aselsan DERGİ

ISSN 1300-2473

TÜRK SİLAHLI KUVVETLERİNİ GÜÇLENDİRME VAKFI

ASELSAN A.Ş
Türk Silahlı Kuvvetlerini Güçlendirme Vakfı kuruluşudur.



AĞ GÜVENLİĞİ VE KRİPTOLOJİ

Birliktelik

Birliktelik değerimizin ASELSAN kültüründeki karşılığı:

- Her durumda birlikte sorumluluk üstleniriz.
- Birbirimizle her durumda dayanışma içinde oluruz.
- Ortamda bulunmayanın hakkını koruruz.
- Ekip amaçları için birbirimizi cesaretlendiririz.
- İş sonuçlarına katkı sağladığını düşündüğümüz davranışları takdir ederiz.
- Bölümler arası iş süreçlerinin uyumu için bilgiyi ve deneyimi paylaşır, iş birliği yaparız.
- Farklılıklara saygı gösterir, farklılıklardan sinerji yaratırız.

Güven

Güven değerimizin ASELSAN kültüründeki karşılığı:

- Söylediğimizi yapar, yaptığımızı söyleriz.
- Açık, net ve şeffaf iletişim kurarız.
- Verdiğimiz sözleri tutarız.
- İşleri zamanında ve tam olarak teslim ederiz.
- Hatayı kimin yaptığına değil, sorunun çözümüne odaklanırız.

Gelişim

Gelişim değerimizin ASELSAN kültüründeki karşılığı:

- Sürekli öğrenir ve kişisel gelişimimizin sorumluluğunu alırız.
- Potansiyelimizi zorlayıcı hedeflerle keşfeder ve geliştiririz.
- Gelişim için geri bildirim alırız ve yapıcı geri bildirim veririz.
- İç ve dış paydaşlarımızın gelişimine katkı sağlarız.

Mükemmellik

Mükemmellik değerimizin ASELSAN kültüründeki karşılığı:

- Süreçlere uygun çalışır, süreçlerin etkinliğini sürekli izler ve iyileştirme önerileri sunarız.
- Kaynaklarımızı verimli kullanırız.
- Daha iyisi için bir işin nasıl yapılmayacağını değil nasıl yapılabileceğini konuşuruz.
- İşimizin izlenebilir, tekrar edilebilir olmasını sağlarız.
- Paydaşlarımızın ihtiyaç ve beklentilerini doğru analiz ve tespit eder, karşılıklı teyit ederiz.

Yenilik

Yenilik değerimizin ASELSAN kültüründeki karşılığı:

- Rutini sorgular, yeni fikirler üretir, yaratıcı çözümler deneriz.
- Değişim ihtiyacını anlar, destekler ve değişime öncülük ederiz.
- Hata yapmaktan korkmayız ve hataları bir öğrenme fırsatı olarak görürüz.
- Bireylerin farklı fikirlerini ifade etmelerini destekleriz.
- Dünyadaki yenilikçi yaklaşımları takip eder, proaktif bir anlayışla işlerimize yansıtırız.

GÜCÜMÜZ DEĞERLERİMİZ

aselsan

Denizin derinliklerinden
Uzayın derinliklerine
www.aselsan.com
aselsan
50 yıl

SİBER SAHADA ÇAĞI YAKALIYORUZ

ASELSAN olarak milli güvenliğin en önemli unsurlarından sayılan siber sahamızın korunması için yerli teknolojiler geliştirmenin kaçınılmaz bir zorunluluk olduğunu biliyoruz.

İnternetin doğuşuyla birlikte hayatımıza giren siber güvenlik meselesi, ASELSAN'ın en kritik öncelikleri arasında bulunuyor. Günümüzde yapay zekâ ve otonom sistemlerin yaygınlaşmasıyla siber güvenliğin ne kadar hayati bir mesele olduğunu daha fazla idrak ediyoruz. Bu nedenle siber dünyadaki verileri çok iyi muhafaza etmemiz gerektiğini biliyoruz.

Geliştirdiğimiz sistemlerin hafızasını artık tamamen dijital ortamda saklıyoruz. Adeta mahremiyetimizi oluşturan bu altyapıları Siber Zırh Programı ile koruyoruz.

Geleceğin yıkıcı teknolojileri arasında ilk sıralarda bulunan siber saldırılara geçit vermemek adına önemli çalışmalara imza atıyoruz. Siber güvenlik alanında her gün değişen tehditlere karşı, yetkinliklerimizi de günün şartlarına uygun olarak geliştiriyoruz. Geleceğin sistemlerini geliştirirken, kritik düzeydeki teknolojilerimizi, milli siber güçlerimizle koruyoruz.

Ahmet AKYOL
Genel Müdür

ASELSAN'da geliştirdiğimiz Siber Zırh Programı ile kurumların güvenlik altyapılarını oluşturan yapıtaşlarının risk tabanlı bakış açısı ile değerlendirilmesini, eksikliklerin ortaya çıkartılmasını ve kurumsal siber direncin artırılmasını hedefliyoruz.

Uzun yıllar boyunca teknik bir sorun olarak ele alınan siber güvenlikle ilgili çözümler hep teknolojik

ürünlerde arandı. Günümüzde ise siber güvenlik stratejik seviyede risk temelli düşünülmesi gereken bir olgu haline geldi. Siber Zırh Programı ile modern güvenlik yaklaşımları kurguladık.

Bu program sayesinde siber güvenliğin kompleks ve karmaşık sorunlara sistematik yöntemlerle çözümler üretebiliyoruz.

Savunma sanayi gibi kritik bir alanda siber güvenliğin sağlanmasının, bağımsızlığımızın teminatı olduğunu biliyoruz. Bu nedenle hayati önem taşıyan büyük verileri, olası siber saldırılara karşı korumak için çağın da ötesine geçecek önlemleri alıyoruz. Kuantum çalışmalarımıza da uzun yıllardır yatırım yapıyoruz. Bu kapsamda TOBB Ekonomi ve Teknoloji Üniversitesinde Türkiye'nin ilk kuantum bilgisayarını devreye aldık. Kuantum bilgisayarları, klasik bilgisayarların işlem gücünü aşarak, karmaşık problemleri çözme kapasitesiyle, yapay zekâ, şifreleme, optimizasyon ve biyoteknoloji gibi alanlarda gerçek anlamda bir devrim yaratma potansiyeline sahip. Böylece savunma teknolojilerinde devrim yaratacak oyun değiştirici kuantum çözümleri ile geleceği inşa ediyoruz.

Ülkemizin ve ASELSAN'ın bilişim altyapısının olası saldırılara karşı dirençli hale getirilmesinin ne kadar zaruri olduğunu yakın coğrafyamızda yaşanan son olaylarla bir kez daha gördük. Bu hadiselerin etkisiyle, siber saldırılara karşı en güvenli çözümlerin sadece yerli ve milli siber sistemlerle sağlanacağını düşünüyoruz.

Siber Vatan'daki tehditlere karşı oluşturduğumuz siber güvenlik çözümlerimizle hem erken safhada saldırıları engelliyor hem de önceden tedbir alıyoruz.

Savunma sektöründe de dijital bir güç olma yolunda ilerleyen ülkemizin siber kalkanlarını güçlendirmek ve ASELSAN'ı bir dünya markası yapmak için çalışmayı sürdüreceğiz. aselsaneXT 2030 vizyonu doğrultusunda dünyanın dört bir yanına imzamızı atarken, siber saldırılara karşı savunmamızı da güçlendireceğiz.

Tartışmasız en önemli önceliklerimiz arasında bulunan siber güvenliğin tüm yönlerini işlediğimiz, ufuk açacağına inandığım dergimizi keyifle okumanızı diliyorum.

aselsan DERGİ

ISSN 1300-2473
YIL: 37,ARALIK 2024, SAYI: 121

ASELSAN Elektronik Sanayi ve Ticaret Anonim Şirketi Adına Yayın Sahibi
Ahmet AKYOL

Genel Yayın Yönetmeni
Mehmet ARTAR

Sorumlu Yazı İşleri Müdürü
İbrahim BİLEKLİ

Yayın Kurulu
Hüseyin Ada ACUN
Kadir Emre AKCİ
Melih BABAGİL
Yunus Emre ÇOLAK
Sevcan DAŞDAN
Esra ERKAN
Mustafa ERKEK
Rana ERMİŞ
Ecem GÖZDE KARABULUT
Tülay KARADENİZ
Serkan KEKEÇ
Fuat Taner ÖZDEMİR
Övünç ÖZDEMİR
Mehmet Burak SAAT
Mustafa SAYIN
Aybüke TUFAN
Aybeniz YİĞİT

Haber Merkezi
Erdinç ÇELİKKAN
Hatice Miray VURMAY GÜZEL
Simge KALKAN

Fotoğraf
Evren BARIŞIK
İbrahim ÖZTÜRK
Cem TAŞKIN

Dağıtım
Osman ARDOĞAN

Tasarım
ARMAPRGROUP
100. YIL MAHALLESİ HATIR SOKAK 27/5 Gaziosmanpaşa Ankara
06700 ÇANKAYA / ANKARA
www.armaprgroup.com

Yayın Tarihi
Sayı 121 - 18 ARALIK 2024

Yayın İdare Adresi
ASELSAN Elektronik Sanayi ve Ticaret Anonim Şirketi
Mehmet Akif Ersoy Mahallesi
İstiklal Marşı Caddesi, No: 16
Yenimahalle 06200, Ankara

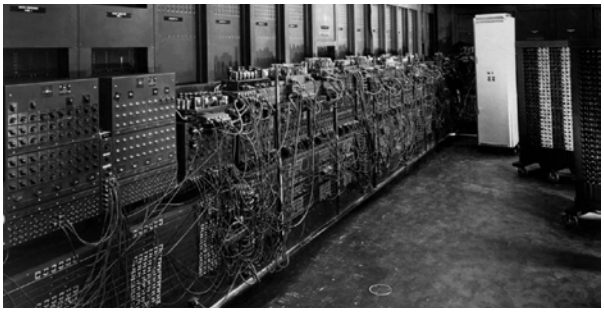
Baskı Cilt
18 ARALIK 2024
ELMA TEKNİK BASIM Matbacılık ve Tan. Hiz. Teks. Tur. İnş.
İth. İhr. San ve Tic. Ltd. Şti.
İvedik O.S.B. Matbaacılar Sitesi 1516/1 Sokak
No:35 Yenimahalle/Ankara +90 312 229 92 65, Sertifika No: 49617

Yayının Türü
Yerel Süreli Yayın

Dergide yayımlanan yazılardan, kaynak adı gösterilerek alıntı yapılabilir. Dergide yayımlanan yazılar yazarların kişisel görüşüdür. ASELSAN Elektronik Sanayi ve Ticaret Anonim Şirketini sorumlu kılmaz. ASELSAN Dergisi, Basın Ahlak Yasasına uymayı taahhüt eder.

TÜRK SİLAHLI KUVVETLERİNİ GÜÇLENDİRME VAKFI

ASELSANA .Ş
Türk Silahlı Kuvvetlerini Güçlen dirme Vakfı kurulu şudur.



SİBER GÜVENLİĞİN TARİHÇESİ
S/**12**

KÜRESEL DÖNÜŞÜMÜN ÖNEMİ: SİBER DAYANIKLILIK
S/**56**

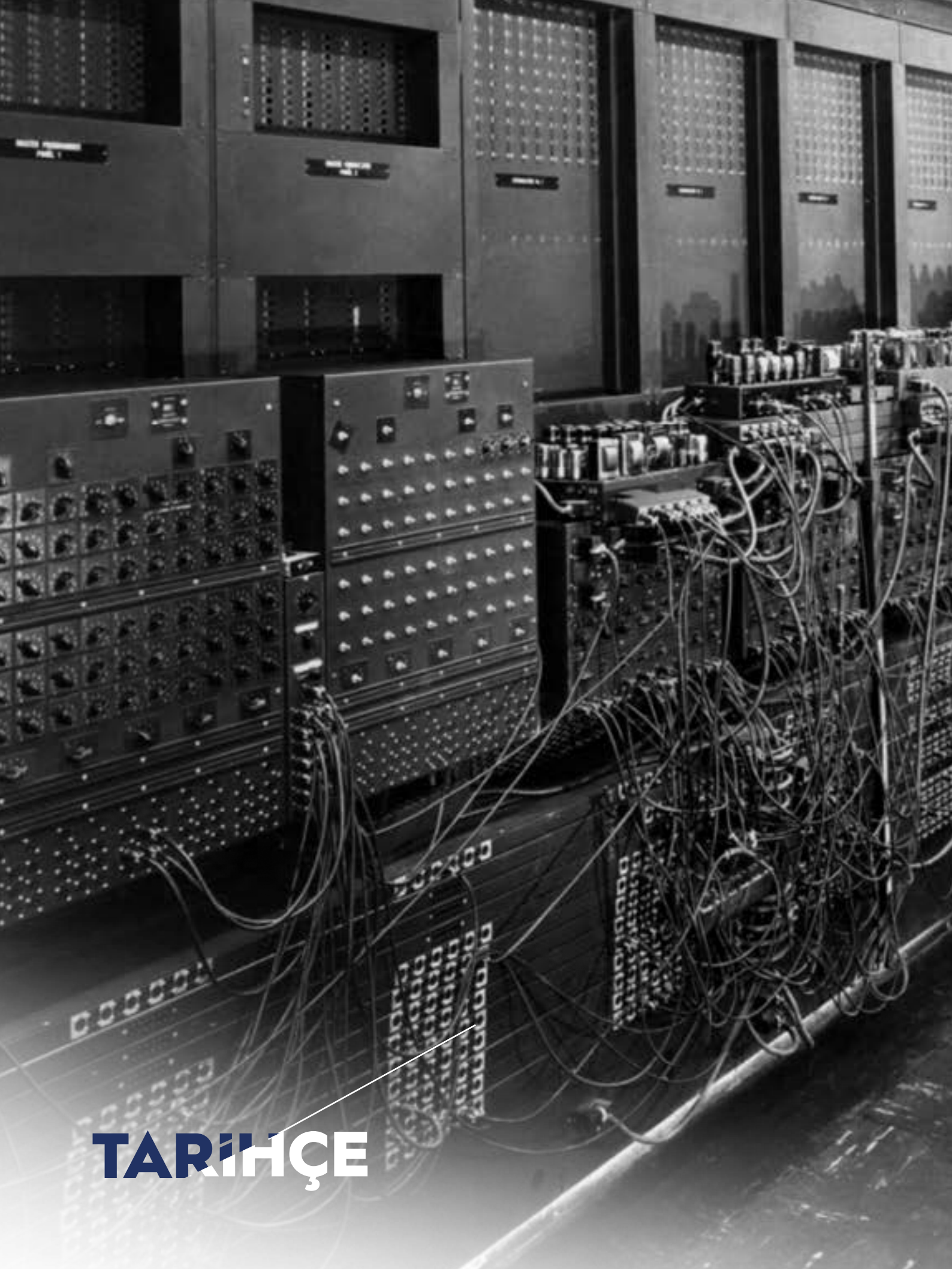
GÜNCEL SİBER GÜVENLİK KONULARI
S/**154**

İÇİNDEKİLER

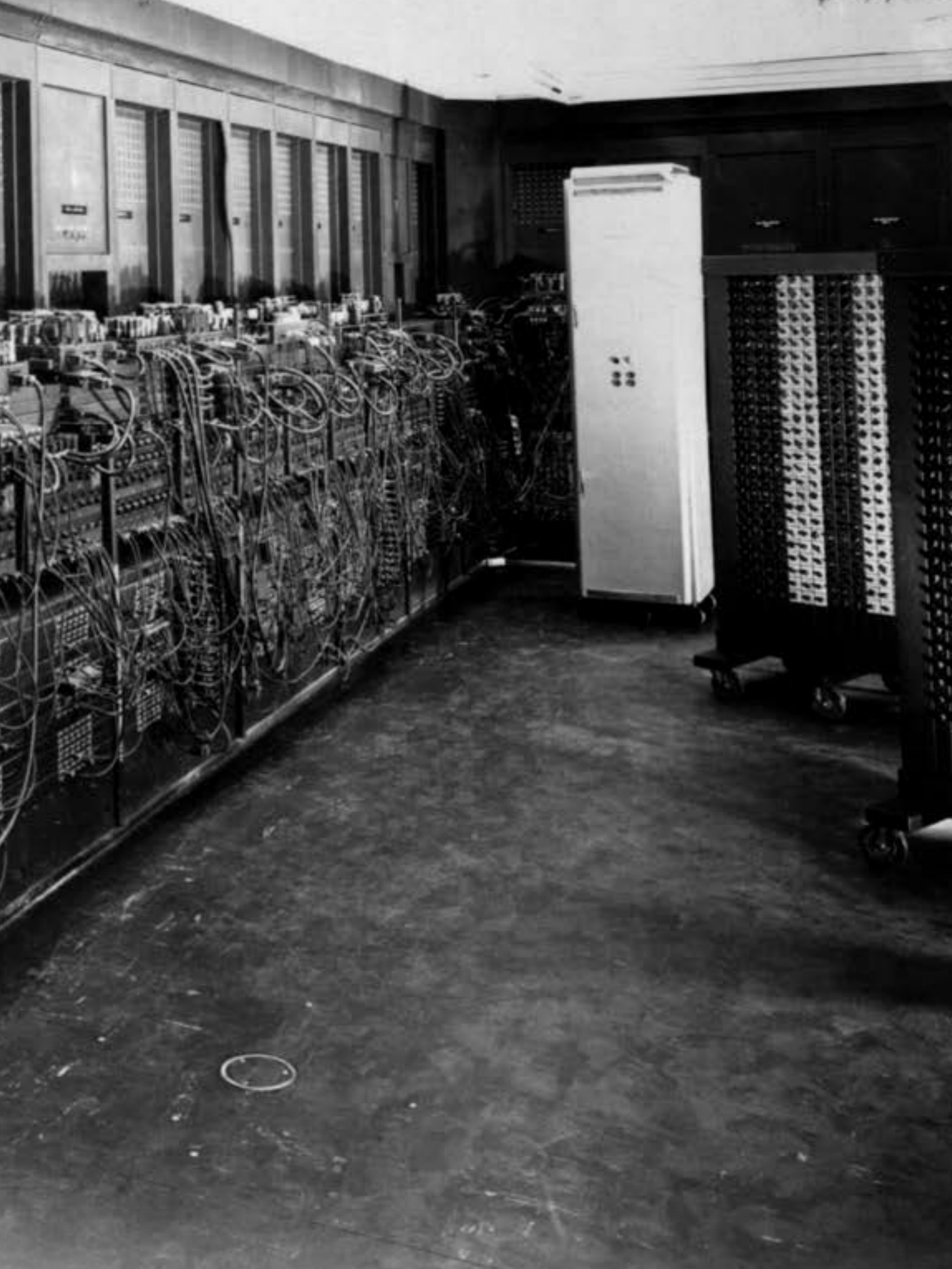
TARİHÇE	**10**
SİBER GÜVENLİĞİN TARİHÇESİ	12
TÜRKİYE'DE SİBER GÜVENLİK	18
KRİPTOLOJİ TARİHÇESİ	26
TARİHTEKİ ÖNEMLİ SİBER OLAYLAR	30
SİSTEM GÜVENLİĞİ MÜHENDİSLİĞİ	**40**
TASARIMIYLA GÜVENLİ SİSTEMLERE GENEL BAKIŞ	42
SİBER DİRENÇLİ SİSTEMLER	56
KRİPTOLOJİ VE BİLGİ GÜVENLİĞİ	**58**
KUANTUM SONRASI KRİPTOGRAFİ	60
TAKTİK SAHADA KRİPTOLU HABERLEŞME	64
YÜKSEK HIZLI KRİPTOLAMA YETENEKLERİ	70
KRİPTO YÖNETİMİ (ANAHTAR YÖNETİMİ VE UZAKTAN YÖNETİM)	72
YAN KANAL ANALİZİ VE KRİPTO ANALİZ	76
ÖZEL SİSTEMLERDE SİBER GÜVENLİK	**78**
TAKTİK SAHADA SİBER GÜVENLİK UYGULAMALARI	80
ELEKTRONİK HARP VE SİBER GÜVENLİK	84
KABLOSUZ İLETİŞİM AĞLARINDA GÜVENLİK	94
BAĞLI ARAÇLAR VE SİBER GÜVENLİK	102
NESNELERİN İNTERNETİ GÜVENLİĞİ	110
BULUT BİLİŞİMDE GÜVENLİK	114
KUBERNETES ALTYAPILARINDA GÜVENLİK DENETİMİ VE İZLEME	120
FİNANSAL SİSTEMLERDE BLOKZİNCİR GÜVENLİĞİ	130
AVİYONİK SİSTEMLERDE SİBER GÜVENLİK	142
GÜNCEL SİBER GÜVENLİK KONULARI	**154**
SİBER GÜVENLİK FARKINDALIĞI	156
SİBER CAYDIRICILIK	162
SİBER SALDIRI METODOLOJİSİ	166
GÜVENLİ YAZILIM GELİŞTİRME VE İDEAL DEVSECOPS KURGUSU	176
YAZILIM TEDARİK ZİNCİRİ GÜVENLİĞİ	190
YAPAY ZEKÂ VE MAKİNE ÖĞRENMESİ: SİBER GÜVENLİKTEKİ FIRSATLAR VE ZORLUKLAR	196
SIFIR GÜVEN YAKLAŞIMI İLE AĞ GÜVENLİĞİNİ ANLAMAK	206
PAROLANIN HİKAYESİ VE KİMLİK DOĞRULAMA	214

“İlim ve fen ve ihtisas nerede varsa, sanat nerede varsa gidip öğrenmeye mecburuz. Çok çalışmaya mecburuz. Çalışmak demek ise boşuna yorulmak terlemek değildir. Zamanın gereklerine göre bilim ve teknik ve her türlü medeni buluşlardan azami derecede yararlanmak zorunludur.”

Mustafa Kemal ATATÜRK



TARİHÇE



SİBER GÜVENLİĞİN TARİHÇESİ

Ali IŞIKLI

Teknolojinin hızla ilerlemesiyle birlikte, dijital dünya artık yaşamımızın merkezinde yer alıyor. Her geçen gün daha fazla işlemi ve etkileşimi dijital platformlar üzerinden gerçekleştiriyoruz. Ancak bu dijital dönüşüm, beraberinde yeni ve karmaşık güvenlik sorunlarını da getiriyor. İşte tam da bu noktada, siber güvenlik kavramı önem kazanıyor.

Bu sayının ana teması olan siber güvenlik tarihi, bizleri geçmişten günümüze kadar uzanan bir yolculuğa davet ediyor. Siber güvenlik, internetin doğuşundan bu yana dramatik bir şekilde evrim geçirmiş teknoloji ve uygulamalarının değişen manzarasını yansıtmaktadır. Basit ağ savunmalarının ilk günlerinden bugünün sofistike sistemlerine kadar, siber güvenliğin tarihi, dijital varlıkları ve altyapıyı kötü niyetli aktörlerden koruma konusundaki insanlık mücadelesinin devam eden bir göstergesidir. Sayısı giderek artan ve daha sofistike hale gelen siber tehditlerle mücadele etmek için insanlık, inovasyon ve dayanışma ruhu ile birlikte hareket etmek durumundadır.

Internet'in doğduğu gün siber güvenliğin de dünyaya geldiğini söyleyebiliriz. Sadece bunun farkına varmamız biraz süre aldı. Başlangıçta araştırma kurumları arasında iletişim aracı olarak geliştirilen ARPANET'in (İleri Araştırma Projeleri Ajansı Ağı), kısa sürede dünya çapındaki işletmeler, hükümetler ve bireyler için hayati bir araç haline geleceği İnternet olacağı bu ağı geliştirenler tarafından da öngörülmedi. İlk bilgisayar solucanları ve virüsleri, bu ağlar üzerinden yayılarak ciddi zararlara neden oldu ve siber güvenlik endüstrisinin doğuşuna zemin hazırladı.

1980'lerde, kişisel bilgisayarların yaygınlaşmasıyla birlikte bilgisayar virüsleri ve kötü amaçlı yazılımların tehdidi de arttı. Bilinen ilk bilgisayar virüsü olan Elk Cloner, 1982'de keşfedildi ve siber güvenliğin yeni bir döneminin başlangıcını işaret etti. On yıl boyunca, 1988'deki Morris Worm dahil bir dizi yüksek profilli siber saldırı, daha güçlü güvenlik önlemlerine olan ihtiyacı vurguladı.

1990'larda, World Wide Web'in ortaya çıkması ve e-ticaret ile online bankacılığın hızla yayılmasıyla birlikte, güçlü bir siber güvenliğe duyulan ihtiyaç giderek daha da belirgin hale geldi. Bu dönemde, şifreleme teknolojileri, çevrimiçi iletişim ve işlemleri güvence altına almak için geliştirildi.

2000'lerin başlarında, İnternet'in bireysel kullanımının yaygınlaşması ile birlikte siber suçluların hükümet kurumlarına, şirketlere, kritik altyapılara ve bireysel kullanıcılara yönelik gerçekleştirdikleri siber saldırıların sayısı da arttı. Bunun üzerine, dünya çapında hükümetler siber tehditlerle mücadele etmek için büyük yatırımlar yapmaya başladılar; ulusal ve uluslararası mevzuat ve standartları hayata geçirerek önlem almaya çalıştılar.

Ancak siber güvenlik sadece bilgisayar sistemleri özelinde değil, aynı zamanda ulusal güvenlik açısından da kritik önem taşıyor. 2009'da Amerika Birleşik Devletleri Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC) gibi kuruluşların kurulması, siber güvenliğin ulusal güvenlikte öncelikli bir konu olarak tanınmasının işaretini verdi. Stuxnet solucanı gibi örnekler, siber saldırıların fiziksel altyapıları da hedef alabileceğini gösteriyor. Stuxnet, İran'ın nükleer tesislerine yönelik karmaşık bir siber saldırıydı ve bu, siber saldırıların artık sadece bilgisayar sistemlerini değil, aynı zamanda gerçek dünyadaki tesisleri ve altyapıyı da etkileyebileceğini gösterdi.

NATO ve diğer birçok ulus, siber alanı yeni bir savaş alanı olarak kabul etti. Bu, siber güvenlikle ilgili tehditlerin artık sadece birkaç bilgisayar korsanının etkinlik alanı olmadığını, aynı zamanda devletler arası çatışmaların da bir parçası haline geldiğini gösteriyor. Bu durum, uluslararası iş birliğinin ve güçlü siber savunma stratejilerinin önemini vurguluyor.

Günümüzde, siber güvenlik giderek karmaşık hale geliyor. İnternetin yaygınlaşmasıyla birlikte, mobil cihazlar, bulut bilişim ve nesnelerin interneti gibi yeni teknolojiler ortaya çıktı. Bu da yeni güvenlik zafiyetlerinin ortaya çıkmasına neden oldu. Siber güvenlik uzmanları, sürekli olarak yeni tehditlere karşı önlemler geliştiriyor ve savunma stratejilerini güçlendiriyor.

Bugün, siber güvenlik bireyleri, işletmeleri ve hükümetleri etkileyen küresel bir endişedir. İşletmelerin operasyonlarını aksatan fidye yazılımı saldırılarından devlet destekli siber casusluk kampanyalarına kadar tehditler çeşitlilik göstermektedir ve sürekli olarak değişmektedir. Modern toplumun dayandığı dijital altyapıyı korumak için teknolojinin ilerlemesiyle birlikte, teknolojik ve stratejik siber güvenlik savunmalarımızın da yeni tehditlere ve zafiyetlere uyum sağlayarak sürekli olarak gelişmesi ve iyileştirilmesi gerekmektedir.

Ancak siber güvenlik sadece teknik bir konu değil, aynı zamanda insan davranışlarına da bağlıdır. Güvenlik açıklarını kapatmanın yanı sıra, bilinçli kullanıcılar ve eğitimli personel de güvenliği sağlamak için kritik öneme sahiptir. Bu nedenle, siber güvenlik kültürünün kurulması ve sürdürülmesi büyük bir önem taşımaktadır.

Bu sayıda, siber güvenlik dünyasının ülkemiz ve ASELSAN'daki gelişimine ve geleceğine daha yakından bakacağız. Ayrıca, güvenlik uzmanlarının görüşlerine hazırladıkları makaleler ile yer vereceğiz. Umarız ki, bu makaleler siber güvenlik konusunda farkındalığınızı artırır ve dijital dünyada daha güvenli bir gelecek için ilham verir.

Keyifli okumalar dileriz.

Hayatı
Yenileyen
Teknoloji
Yenilenebilir Enerji Sistemleri
ASELSAN köklü mühendislik birikimi ile Yenilenebilir Enerji Sistemlerinde lider yerli teknoloji tedarikçisi olma yolunda çalışmalarını sürdürüyor.
www.aselsan.com
aselsan

TÜRKİYE'DE SİBER GÜVENLİK

Ali IŞIKLI

Günümüzde, askeri stratejiler artık sadece geleneksel cephelerde değil, aynı zamanda siber alanda da şekillenmektedir. Askeri güç, artık dijital dünyanın savunulmasında da kritik bir rol oynamaktadır. Türkiye, siber güvenliği ulusal savunma stratejisinin merkezine yerleştirerek, siber tehditlere karşı etkili bir şekilde mücadele etmektedir.

Türkiye'nin siber güvenlik alanındaki tarihi, bilgi teknolojilerinin ülkeye girişiyle başlar. İnternet kullanımının artmasıyla birlikte, bilgisayar korsanlığı, veri sızıntıları ve dijital casusluk gibi tehditler de Türkiye için ciddi birer risk haline gelmiştir. Türkiye, bu tehditlere karşı etkili bir şekilde mücadele edebilmek ve dijital altyapısını güçlendirebilmek için çeşitli önlemler almıştır.

Türkiye, siber güvenlik alanında uluslararası iş birliğine de önem vermektedir. Türkiye, NATO'nun siber savunma stratejilerine aktif bir şekilde katkıda bulunmakta ve uluslararası platformlarda siber güvenlik konusunda iş birliği yapmaktadır. Ayrıca, başta startuplar, teknokent firmaları ve Türkiye Siber Kümelenme üyesi firmaların siber güvenlik alanında başarılı projelere imza atması, Türkiye'nin bu alandaki potansiyelini göstermektedir.

Türkiye'nin siber güvenlik konusundaki kararlılığı, özellikle askeri alanı etkilemektedir. Askeri sistemlerin ve iletişim altyapısının siber saldırılara karşı korunması, ulusal savunma stratejisinin temel unsurlarından biridir. Bu nedenle, Türkiye'nin siber güvenlikteki başarısını artırmak için, özellikle askeri alanda siber güvenlik bilincini ve kapasitesini artırmak önemlidir. Bu nedenle, Türk Silahlı Kuvvetleri siber güvenlik alanında sürekli olarak güçlü bir şekilde yatırım yapmakta ve yeteneklerini geliştirmektedir.

Siber güvenliğin Türkiye'deki kronolojik gelişimine hızlıca bir göz atacak olursak :

Tüm dünyada olduğu gibi 90'ların sonlarına doğru ağ teknolojilerinin ve internetin yaygınlaşması, bu ortamları hedefleyen ve bu ortamlardan kaynaklı tehditlerin de yaygınlaşması sonucunu doğurdu. Devlet kaynaklarını, vatandaşları hedef alan saldırıların maddi ve manevi sonuçları baş ağrıtmaya başladı. Bu durum bireylerin ve organizasyonların aldıkları önlemlerle çözülemeyecek seviyeye geldi. Siber ortamda varlıkların korunması ve siber güvenliğinin sağlanması artık ulusal güvenliğin bir parçası olarak ülkelerin politika ve stratejilerinde yer bulmaya başladı.

Türkiye'nin siber güvenlik yolculuğu 1991 yılında 765 sayılı Türk Ceza Kanununa Bilişim Suçlarının dâhil edilmesi ile başlamıştır.

1999 yılında Ulaştırma Bakanlığı koordinatörlüğünde yürütülen çalışmalarla Güven Çalışma Grubu tarafından getirilen Ulusal Bilgi Güvenliği Üst Kurulu ve Bilgi Güvenliği Kurumu oluşturulması önerisi bilgi altyapısına yönelik bir yapılanmanın bulunmadığı ortamda fazla iddialı bulunmuş, Bilgi Toplumu Kurumu altında bilgi güvenliğinin ele alınması şekline çevrilmiştir. Ulusal bilgi güvenliğinin sağlanması amacıyla bilgi güvenlik duvarının oluşturulması ve kişisel bilgi güvenliği sağlanması, veri aktarma ve saklama güvenliği, e-ticaret güvenliği, güvenlik teknolojilerinin önceliklendirilmesi öne çıkan hususlardandır.

Milli Savunma Bakanlığı tarafından hazırlanan Ulusal Bilgi Güvenliği Teşkilatı ve Görevleri Hakkında Kanun Tasarısı Türkiye ulusal bilgi güvenliğini tek elden koordine etmeyi amaçlayan ilk çalışma sayılır.

Sekizinci Beş Yıllık Kalkınma Planı (2001–2005), Ulusal Bilgi Güvenliği ile ilgili yasal düzenleme tedbirlerinin yer verildiği ilk kalkınma planıdır.

9 Ekim 2001 tarihli Başbakanlık Genelgesi ile başlatılan e-Türkiye girişimi kapsamında 13 ana çalışma grubu oluşturulmuştur.

Genelkurmay Başkanlığı tarafından koordine edilen ve 1996 yılında oluşturulmuş Güvenlik Çalışma Grubu çalışmalarını e-Türkiye Girişimi ile koordineli yürüterek Ulusal Bilgi Güvenliği Kanun Taslağı'nı hazırlanmıştır.

Türkiye'nin bilgi toplumuna geçiş faaliyetlerinin bir bütünlük içinde yürütülmesi, bu yönde politika ve stratejilerin oluşturulmasını sağlamak üzere 3 Ocak 2003 tarihli 58. Hükümet Acil Eylem Planı içinde e-dönüşüm Türkiye Projesine yer verilmiştir. 27 Şubat 2003 tarihli ve 2003/12 sayılı Başbakanlık genelgesi ile Devlet Planlama Teşkilatı koordinasyon ile görevlendirilmiş ve Bilgi Toplumu Dairesi kurulmuştur.

2003-2004 döneminde hazırlanan kısa dönem eylem planında ağ güvenliğin test edilmesi ve sağlanmasına ilişkin pilot uygulamaların geliştirilmesi konusunda TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsüne (UEKAE) , kişisel verilerin korunması hakkında kanun çıkarılması ve ceza kanununda bilişim suçlarının revizyonu çalışmaları için Adalet Bakanlığına, Ulusal Bilgi Güvenliği Kanunu'nun çıkarılması konusunda Milli Savunma Bakanlığı'na görev verilmiştir.

2004 yılında yürürlüğe giren 5237 Sayılı Yeni Türk Ceza Kanununun Bilişim Alanında Suçlar başlığı altında bilişim suçu oluşturacak eylemler ve bunlara uygulanacak cezalar detaylı olarak belirlenmiştir.

2006 yılında Bilgi Toplumu Stratejisi ve Eylem Planında yer alan eylem maddesi uyarınca bilgisayar etkinlikleri ve kamu kurumlarının bilgi güvenliğini sağlamaya yönelik faaliyetler için Bilgisayar Olayları Müdahale Ekibi (TR-BOME), TÜBİTAK Bilgi ve Bilgi Güvenliği İleri Teknolojileri Araştırma Merkezi (BİLGEM) kurulmuştur.

TÜBİTAK

BİLGEM

2008 yılında yürürlüğe giren Elektronik Haberleşme Kanunu ile elektronik haberleşme sektörünün çalışma usul ve esaslarını düzenleyen kanun denetleme, yeni yatırımların teşvik edilmesi, tüketici haklarının gözetilmesi vb. sektörün gelişimine odaklanan birçok hususu ele almıştır. Telekomünikasyon sektörünün düzenleme ve denetleme fonksiyonunun bağımsız bir idari otorite tarafından yürütülmesi amacıyla 2000 yılında kurulan Telekomünikasyon Kurumu, bu kanun ile Bilgi Teknolojileri ve İletişim Kurumu (BTK) olarak isim değiştirmiş ve Ulaştırma Bakanlığına bağlanmıştır. BTK elektronik ve haberleşme sektörünün ana düzenleyicisi olarak ilgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak

düzenlemelerde bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi ilkesi (4. madde (l) bendi) ve kişisel verilerin ve gizliliğinin korunması, elektronik haberleşme şebekelerinin bütünlüğünün idame ettirilmesi, izinsiz erişime karşı şebeke güvenliğinin sağlanması yönünde kendi sektörünün sahasında güvenlik faaliyetlerini de düzenleyebileceği yönünde görevlerini bu kanunla yüklenmiştir.

Türkiye'de devletin tüm kurumları düzeyinde siber güvenlik konusu ilk kez 27 Ekim 2010'da toplanan Milli Güvenlik Kurulunda tartışılmıştır. Ulusal güvenlik politikası bağlamında siber güvenliğe daha fazla önem verileceği aşağıdaki ifadelerle net olarak belirtilmiştir. Siber tehdit ifadesi kamuoyunda Kırmızı Kitap olarak bilinen Milli Güvenlik Siyaset Belgesine girmiştir. Hükümet, Genelkurmay'ın önerisi doğrultusunda siber terörizmi, Türkiye'nin tehdit algılamaları arasına almıştır. "Siber tehdidin global düzeyde ulaştığı boyut ve bu tehdidin ulusal güvenliğine etkileri kapsamlı surette ele alınmıştır. Bu bağlamda, siber tehdidin engellenebilmesi açısından milli düzeyde yürütülen çalışmalar değerlendirilmiştir."

2012 tarihli, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar ile Ulaştırma, Denizcilik ve Haberleşme Bakanlığına kamu kurumları ve kritik altyapı işletmelerince uyulması gereken tedbirler, bu kurumların verdiği hizmetlerde güvenliğin ve gizliliğin sağlanması, ulusal politika ve stratejilerin hazırlanması, eylem planlarının hazırlanması, kurumlar arası uyumu sağlama ve koordinasyonu temin etme, Siber Güvenlik Kurulunun sekretaryasını yürütme, gerektiğinde uluslararası kuruluşlarla iş birliğine gitme, toplumsal farkındalığı artırmaya yönelik eğitim faaliyetlerini yürütme, siber saldırılara karşı milli savunma mekanizmalarını geliştirme görevleri verildi. Aynı kararda bakanlığın icracı kurumlarından biri de BTK olarak belirlendi. (Madde 5/h/3)

2012, Siber Güvenlik Kurulunun teşkil edilmesi: Bakanlar kurulu kararının 20 Ekim 2012 tarihinde Resmi Gazete'de yayımlanmasının ardından Siber Güvenlik Kurulu, Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında Dışişleri, İçişleri, Millî Savunma, Ulaştırma, Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Millî İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı gibi bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşacak şekilde teşkîl edildi. Ulaştırma Bakanlığı tarafından belirlenen politika, strateji ve eylem planlarının nihai onay makamı ve bunların ülkede etkin şekilde uygulanması ile yükümlü ana mercî yapılan bu düzenleme ile Siber Güvenlik Kurulu olarak

belirlenmiştir. Kurul, ilk toplantısını 20/12/2012 tarihinde gerçekleştirmiş ve 'Ulusal Siber Güvenlik Stratejisi ve 2013–2014 Eylem Planı'nı uygulamaya karar vermiştir. İkinci toplantı 20/06/2013 tarihinde, üçüncü toplantı 19/12/2013 tarihinde yapılmıştır. Kurul dördüncü toplantısını 10 Şubat 2016 tarihinde gerçekleştirmiştir. 2014–2015 yıllarında kurul toplanmamıştır.

2012, TÜBİTAK Siber Güvenlik Enstitüsünün Kurulması: 1997 yılında Bilişim Sistemleri Güvenliği (BSG) Birimi adıyla TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) çatısı altında faaliyetlerine başlayan birim, 2012 yılı itibarıyla ayrışmış ve TÜBİTAK BİLGEM bünyesinde ayrı bir enstitü olarak teşkil edilmiştir. Siber Güvenlik Enstitüsü Türkiye bilgi güvenliği ve siber güvenliğine ilişkin hazırlanmış birçok rehber, mevzuat, esas dokümanları vb. çalışmalarını gerçekleştirmiştir.

2013, 2013–2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: 16 Ocak 2013 tarihinde yürürlüğe girmiştir. Hazırlık çalışmaları 2012 yılında başlamış, Bilim Sanayi ve Teknoloji Bakanlığı ve Bilgi ve İletişim Teknolojileri Kurumu (BTK) koordinasyonunda Türkiye'de siber suçla mücadele sivil toplum kuruluşları ve kurumları ile birlikte yürütülmüştür. Türkiye'nin ilk siber güvenlik strateji dokümanıdır. Strateji ekindeki eylem planında toplam 29 eylem maddesi yer almıştır.

2013, USOM'un Kuruluşu: 27.05.2013 tarihli Bakanlar Kurulu kararıyla siber saldırın etkilerini azaltmak veya ortadan kaldırmak üzere BTK'ya bağlı olarak Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur.

2013, SOME Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği: 11 Kasım 2013 tarihli ve 28818 sayılı Resmi Gazete'de yayımlanan tebliğ ile SOME'ler (Siber Olaylara Müdahale Ekipleri) kurulması kararlaştırılmış ve bu birimlerin görevleri belirtilmiştir. Kurumsal SOME ve Sektörel SOME'ler oluşturulmaya başlanmıştır.

2013, Siber Savunma Komutanlığı Kuruluşu: Türkiye'nin askeri alandaki ilk siber güvenlik yapılanması Siber Savunma Komutanlığı olarak bilinen ilk siber ordusu, Savunma Bakanlığı, TÜBİTAK ve ODTÜ iş birliği ile Genelkurmay Başkanlığı bünyesinde 2010 yılında kurulmuştur. 2013 yılında Ulusal Siber Güvenlik Stratejisinin yayınlanmasıyla resmileşerek görevleri tanımlanmıştır.

2013, Emniyet Siber Suçlarla Mücadele Daire Başkanlığının kurulması: Emniyet Genel Müdürlüğü tarafından siber suçlarla mücadelede yetkin personelden oluşan bir uzmanlık birimi olarak 2011/2025 sayılı Bakanlar Kurulu kararı ile Bilişim Suçlarıyla Mücadele Daire Başkanlığı kurulmuştur. Bu birimin ismi 2013 yılı içinde Siber Suçlarla Mücadele Daire Başkanlığı olarak değiştirilmiştir.

Bilgi Toplumu Stratejisi ve Eylem Planı ile Bilgi Güvenliği ve Kullanıcı Güveni ekseninde siber güvenlik hususları müstakil olarak ele alınmıştır. Siber güvenlik kanununun çıkarılması, kişisel verilerin korunması mevzuat çalışmaları ve bilişim suçları ihtisas mahkemelerinin kurulması konusu Adalet Bakanlığına, Ulusal siber suç stratejisinin çalışılması Emniyet Genel Müdürlüğüne, internetin güvenli kullanımı konusunda farkındalığın artırılması konusu ise TİB'e, görev olarak atanmıştır. Bir önceki dönemden farklı olarak bu stratejinin ara izleme ve sonuç raporları paylaşılmamıştır. Bilgi Toplumu ve Stratejisi eylem planında yer alan eylem maddesinden Adalet Bakanlığı uhdesinde yürütülen Ulusal Bilişim Güvenliği Kanunu çalışmalarının bir kez daha isim değiştirerek Siber Güvenlik Kanunu adı altında devam ettiğini anlıyoruz. 2015 sonunda tamamlanmak üzere koyulan hedef gerçekleştirilememiştir.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığına bağlı Siber Güvenlik Kurulu koordinesinde 2015 yılı içerisinde sorumlu veya ilgili kurumlarla birlikte 7 adet değerlendirme toplantısı yapılmış, toplantıların ardından kritik altyapı işletmecileri, bilişim sektörü, üniversiteler, kamu kurumları ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir. Bu çalışmalar sonrası strateji hazırlanmış ve 9 Eylül 2016 tarihinde kamuoyu ile paylaşılmıştır. Beş stratejik amaç doğrultusunda 41 eylemin hayata geçirilmesi öngörülmüştür.

Yerli ve milli siber güvenlik teknolojilerinin ve siber güvenlik ekosisteminin geliştirilmesi temel amacı ile Cumhurbaşkanlığı Savunma Sanayii Başkanlığı koordinesinde Türkiye Siber Güvenlik Kümelenmesi Projesi 2017 yılında hayata geçirilmiştir. Proje, Dijital Dönüşüm Ofisi ve Savunma Sanayii Başkanlığı arasında 1 Şubat 2021 tarihinde imzalanan protokol sonrası resmi olarak birlikte yürütülmeye başlanmıştır.

Kişisel Verileri Koruma Kurulu atamaları tamamlanarak 2017 yılında faaliyetlerine başlamıştır.

Yeni hükümet sistemine geçiş ile birlikte 2 Temmuz 2018 tarihli ve 703 sayılı KHK ile Siber Güvenlik Kurulu kaldırıldı. Kurulun görev ve yetkilerinin Cumhurbaşkanınca belirlenen kurul veya merciye devredileceği bildirilmiştir. Bu görev ve yetkilere ilişkin kısmî atamalar mevcut olsa da, tamamı bugüne kadar herhangi bir kurula veya merciye devredilmemiştir.

9 Temmuz 2018 tarihinden itibaren uygulanmaya başlanan Cumhurbaşkanlığı Hükûmet Sisteminin 1 sayılı Cumhurbaşkanlığı Kararnamesi ile Dijital Dönüşüm Ofisi kurulmuştur. Ofise «Bilgi güvenliğini ve siber güvenliği artırıcı projeler geliştirmek» üst görevi atanmıştır.

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından kamu kurumları ve kritik altyapı hizmeti veren işletmelerce uyulması gereken Bilgi ve İletişim Güvenliği tedbirlerini içeren 06.07.2019 tarih ve 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi yayınlanmıştır.

29 Aralık 2020 tarih ve 31349 sayılı Resmi Gazetede yayımlanan 2020/15 sayılı Genelge ile Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020–2023) yürürlüğe girmiştir. 40 eylem ve 75 uygulama adımından oluşan eylem planı sorumlu ve ilgili kurumlara resmi yazı ile gönderilmiştir.

2023 yılında MİT Elektronik ve Teknik İstihbarat Başkanlığı altında devam eden siber istihbarat faaliyetlerini yürütmek üzere, MİT Siber İstihbarat Başkanlığı kuruldu.

Son yıllarda Türkiye, siber güvenlik konusunda önemli adımlar atmıştır. Siber Güvenlik Kanununun kabul edilmesi, ülkenin siber güvenlik politikalarını daha etkili bir şekilde yönetmesine yardımcı olmuştur. Ayrıca, kamu kurumları ve özel sektör firmaları arasında siber güvenlik bilincini artırmak için çeşitli eğitim ve farkındalık kampanyaları düzenlenmektedir.

Gelecekte, Türkiye'nin siber güvenlik alanındaki rolü daha da önem kazanacaktır. Dijitalleşme sürecinin hızlanmasıyla birlikte, Türkiye savunma alanında da dijital bir güç olma yolunda ilerlemektedir. Ülkenin siber güvenlik alanındaki potansiyeli, askeri stratejilerin belirlenmesinde ve savunma kapasitesinin güçlendirilmesinde kritik bir rol oynamaktadır.

Sonuç olarak, Türkiye'nin siber güvenlik alanındaki yaklaşımı, ülkenin savunma stratejilerinin merkezine yerleştirilmiş etkili bir siber güvenlik politikasıdır. Ulusal savunma gücünün sadece geleneksel cephelerle sınırlı olmadığını, aynı zamanda siber alanda da güçlü bir şekilde korunması gerektiğini göstermektedir. Türkiye'nin siber güvenlikteki başarısı, ülkenin askeri kapasitesini ve ulusal güvenliğini güçlendirecektir.

KRİPTOLOJİYE GİRİŞ

Erkan USLU, Dr. Murat Burhan İLTER,

Dr. Neşe KOÇAK

Kriptoloji güvenli iletişimi inceleyen bilim dalıdır. Kriptografi ve kriptanaliz olarak iki ayrı dala ayrılmaktadır. Kriptografi teriminin kökeni Antik Yunancaya dayanmaktadır. Kriptografi kelimesi, gizli anlamına gelen kryptós ve yazmak anlamına gelen graphein kelimelerinin birleşiminden oluşmaktadır. Kriptografi kapsamında güvenli yöntemler tasarlanırken kriptanalizde tasarlanan yöntemlerin güvenliği incelenmektedir.

Kriptolojide temel olarak gizlilik, bütünlük ve erişilebilirlik gibi servisler hedeflenmektedir. Gizlilik ile özel veya gizli bilgilerin yetkisiz kişilere açıklanmadığı veya ifşa edilmediği şekilde garantilenmesi amaçlanır. Bütünlük, verilerin oluşturulduktan, güncellendikten, depolandıktan veya iletildikten sonra içeriğinin bozulmasının veya yetkisiz kişiler tarafından değiştirilmesinin anlaşılabilmesini hedefleyen bir özelliktir. Erişilebilirlik, varlık içeriğinin veya hizmetlerinin yetkili kullanıcıları tarafından kullanılabilir durumda olduğu bir özelliktir.

Kriptografide sık kullanılan tanımlar aşağıda verilmiştir.

Açık Metin: Şifreleme işlemi yapılacak verilerdir.

Kapalı Metin: Şifreleme işlemi sonrası elde edilen verilerdir.

Anahtar: Şifreleme ve deşifreleme algoritmaları tarafından kullanılan ve genellikle gizli tutulması gereken bir parametredir.

Şifreleme (Kripto) Algoritması: Açık metin ve anahtar bilgilerini kullanarak kapalı metin elde edilmesinde kullanılan algoritmadır.

Deşifreleme (Kripto Çözme) Algoritması: Kapalı metin ve anahtar bilgilerini kullanarak açık metin elde edilmesinde kullanılan algoritmadır.

Asimetrik (Açık Anahtarlı) Kriptografi: Anahtar paylaşımı, şifreleme ve dijital imzalama amaçlarıyla kullanılan bu sistemlerde açık ve gizli olmak üzere iki anahtar kullanılır. Bu anahtarlar birbirleriyle matematiksel olarak ilişkilidir. Açık anahtar herkes tarafından bilinebilirken gizli anahtar sadece kullanıcıda olmalıdır.

Simetrik Kriptografi: Veriyi şifrelemek ve şifreli veriyi çözmek için tek bir anahtar kullanılır. Bu anahtar, veri gönderilmeden önce alıcı ve gönderici arasında güvenli kanaldan paylaşılmalıdır.

Kriptoloji yaklaşık olarak 4000 yıldır kullanılmaktadır. Uzunca bir süre sadece askeri sistemlerde kullanılmıştır. 1950'li yıllardan sonra modern anlamda bilgisayarların gelişmesi ve finans sektörü gibi alanlarda ihtiyaç duyulması sebebiyle endüstride kriptoloji kullanılmaya başlanmıştır. İnternet bankacılığı, sosyal medya ve online mesajlaşma gibi sıklıkla kullandığımız platformların güvenliği kriptoloji kullanılarak sağlanmaktadır.

Klasik ve modern kriptoloji olarak ikiye ayrılan bu sürecin kısa bir tarihçesi sonraki başlıkta verilmiştir.

Klasik Kriptoloji

Kriptolojinin kullanıldığına dair ilk bulgu M.Ö. 1900'lü yıllara kadar uzanmaktadır. Antik Mısır'da, hiyerogliflerin, yazıların yetkisi olmayan kişilerden saklanılması amacıyla kullanıldığı düşünülmektedir. Antik Yunan'da M.Ö. 500'lü yıllarda şifreleme amacıyla silindirler geliştirilmiştir.

Roma'da, günümüzde Sezar şifreleme yöntemi olarak bilinen yöntem geliştirilmiştir. Milattan önce 60'lı yıllarda Julius Caesar generalleriyle şifreli iletişim kurabilmek için kelimelerde bulunan harfleri, alfabedeki yerlerinden 3'er sıra kaydırarak yazmıştır. Generaller de harfleri 3 sıra tersine kaydırarak bu şifreyi çözebilmişlerdir.

1500'lü yıllarda Blaise de Vigenere tarafından Sezar şifrelemesinin iyileştirilmesiyle Vigenere şifreleme yöntemi geliştirilmiştir. 1700'lü yılların sonlarında Thomas Jefferson tarafından disk şifreleme yöntemi mekanik şifreleme yöntemlerinin ilk örneği olarak gösterilmektedir. Enigma makinası, 1. Dünya Savaşı sırasında icat edilmiş ve 2. Dünya Savaşı sırasında geliştirmeleri yapılmıştır. Vernam şifreleme yöntemi 1917'de Gilbert Vernam tarafından geliştirilmiş olup literatürde tek kullanımlık şifre (One Time Pad) olarak adlandırılmıştır. Bu yöntem hala güvenli olarak kabul edilmektedir.

Kullanılan kriptografik algoritmaların güvenlikleri zamanla incelenmiş ve içerdikleri zafiyetler sebebiyle yeni kripto algoritmalarının geliştirilmesi ihtiyacı doğmuştur. 2. Dünya Savaşı'nda Enigma'nın kırılması hem savaşın seyrini değiştirmiş hem de günümüz bilgisayarlarının temelini atmıştır. Bu durum savaşın müttefik devletler tarafından kazanılmasına yardım etmesiyle birlikte bilgi güvenliğinde bilgisayarların işlem güçlerine dayanıklı kriptografik algoritmalar tasarlanması gerekliliğini de beraberinde getirmiştir.

Modern Kriptoloji

1950'li yıllarda bilgisayarların icadı ve Shannon'un enformasyon teorisi alanında yaptığı çalışmalar modern kriptolojinin ortaya çıkmasında önemli rol oynamışlardır. Modern kriptoloji ile birlikte sağlanması gereken güvenlik kriterlerinin birçoğu bu dönemde tanımlanmış ve çözümler üretilmeye çalışılmıştır.

Modern kriptografi simetrik ve asimetrik kriptosistemler olarak iki alt başlık altında incelenmektedir. Simetrik kriptosistemlerde şifreleme ve deşifreleme işlemi aynı gizli anahtarla yapılmaktadır. Blok tipi şifreleme algoritmalarında 1950-2000 yılı arasında önemli gelişmeler aşağıda özetlenmiştir.

1970'lerde, IBM Lucifer şifresini geliştirmiş ve bu şifreleme standardı 1976'da Veri Şifreleme Standardı (Data Encryption Standard) haline gelmiştir. Bu standart 2000'li yıllara kadar kullanılmıştır. Modern kriptanaliz yöntemleri bu dönemde ortaya çıkmış ve DES algoritmasının incelemeleri yapılmıştır. 1998'de, Joan Daemen ve Vincent Rijmen, Rijndael adlı simetrik şifreleme algoritmasını geliştirmiş ve bu algoritma 2001'de Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından Gelişmiş Şifreleme Standardı (AES) olarak seçilmiştir. Günümüzde AES algoritması hala güvenli olarak kabul edilmektedir.

Asimetrik kriptosistemler kavramı 1970'li yıllarda ortaya çıkmıştır. Bu algoritmalar kullanılarak şifreleme, anahtar paylaşımı ve sayısal imzalama yapılabilmektedir. Asimetrik algoritmaların performansı göz önünde bulundurulduğunda genellikle anahtar değişimi ve sayısal imza işlemlerinde kullanılırlar. Asimetrik kriptosistemlerde işlemler birbirlerine bağımlı açık ve gizli anahtar çiftiyle yapılmaktadır. Bir veri şifrelenmek istendiği zaman kullanıcının gizli olmayan, herkes tarafından bilinebilen, açık anahtarıyla şifreleme yapılır. Deşifreleme işlemi ise sadece kullanıcıya ait gizli anahtarla yapılabilmektedir. Sayısal imzalarda imzalanacak veri gizli anahtar kullanılarak imzalanmaktadır. İmza doğrulama işlemi ise açık anahtar kullanılarak yapılmaktadır. İmzalanan veri açık anahtara sahip herkes tarafından doğrulanabilirken, imzalama işlemi sadece gizli anahtara sahip kişiler tarafından yapılabilmektedir.

Kronolojik olarak bakıldığında bu yapıların ilk örneği, 1976'da, Whitfield Diffie ve Martin Hellman tarafından geliştirilmiştir. Diffie-Hellman anahtar değişimi olarak bilinen bu yöntemle güvensiz olan kanallarda güvenli bir şekilde anahtar paylaşımı mümkün olmaktadır. 1977'de, Ronald Rivest, Adi Shamir ve Leonard Adleman RSA algoritmasını geliştirmişlerdir. 1987'de, Neal Koblitz, açık anahtarlı kriptosistemlerde kullanılmak üzere eliptik eğrileri önermiştir.

Milenyum sonrasında, kriptolojinin kullanıldığı alanlar gün geçtikçe artmaya başlamıştır. İletişimin ve internet kullanımının artmasıyla her geçen gün güvenlik daha önemli bir ihtiyaç haline gelmektedir. Günümüzde kriptolojinin kullanım alanlarına örnekler aşağıda verilmiştir.

Blok Zincir

Blok zincir teknolojisi sunduğu merkeziyetsiz yapı esnekliğiyle finans sistemi başta olmak üzere birçok uygulama alanında kullanılmaktadır. Blok zincir teknolojilerinde özet alma fonksiyonları, kimlik doğrulama ve dijital imzalama başta olmak üzere kriptografik yapılar kullanılmaktadır.

Kaynak Kısıtlı (Lightweight) Kriptografi

Kaynak kısıtlı kriptografi, sınırlı kaynaklara sahip olan cihazlarda güvenliği sağlamak ve verimli bir şekilde çalışmak üzere özel olarak tasarlanmış kriptografik mekanizmaları ifade eder. Bu cihazlar genellikle düşük işlemci gücü, düşük bellek kapasitesi ve sınırlı enerji kaynaklarına sahiptir. Kaynak kısıtlı kriptografi, bu tür cihazlar için optimize edilmiş kriptolama algoritmaları, kimlik doğrulama protokolleri ve anahtar yönetimi teknikleri geliştirme amacını taşır. Bu yaklaşım, mobil cihazlar, akıllı kartlar, IoT (Nesnelerin İnterneti) cihazları, giyilebilir teknolojiler ve diğer gömülü sistemler gibi çeşitli uygulama alanlarında kullanılmaktadır. Bu alanda yapılan araştırmalar, güvenlik standartlarını korurken kaynak kullanımını minimize etmeyi ve cihazların performansını artırmayı hedefler. NIST, 2023 yılında Ascon algoritmasını standart olarak seçmiştir.

Kuantum Sonrası Kriptografi

Günümüzde kullanılan açık anahtarlı kripto algoritmaları kuantum bilgisayarlar yeterli seviyede işlem yapabildiğinde güvensiz hale gelecektir. Bu sebeple kuantum bilgisayarlar kullanılarak yapılacak ataklara karşı güvenli algoritmalar tasarlanmaktadır. NIST, 2023 yılında anahtar kapsülleme algoritması olarak CRYSTALS-Kyber'i, imzalama algoritması olarak CRYSTALS-Dilithium, Falcon ve SPHINCS+ algoritmaları standart olarak belirlemiştir.

Homomorfik Şifreleme

Homomorfik şifreleme, bir kullanıcının şifrelenmiş verisi üzerinden herhangi bir deşifreleme yapmadan anlamlı işlem yapmasını sağlayan kriptografik bir yapıdır. Finans ve sağlık sektörü gibi önemli uygulama alanlarına kullanılması hedeflenmektedir. Homomorfik şifreleme algoritmalarının yavaş çalışması ve bellek ihtiyacının fazla olması aktif kullanımını sınırlamaktadır. Buna rağmen, bu algoritmaların şifreli veriler üzerinde anlamlı işlem yapabilme yeteneği nedeniyle akademik ve sektörel alanda yoğun ilgi görmektedir ve bu algoritmaları verimli hale getirmek için çalışmalar yapılmaktadır.

TARİHTEKİ ÖNEMLİ SİBER SUÇLAR

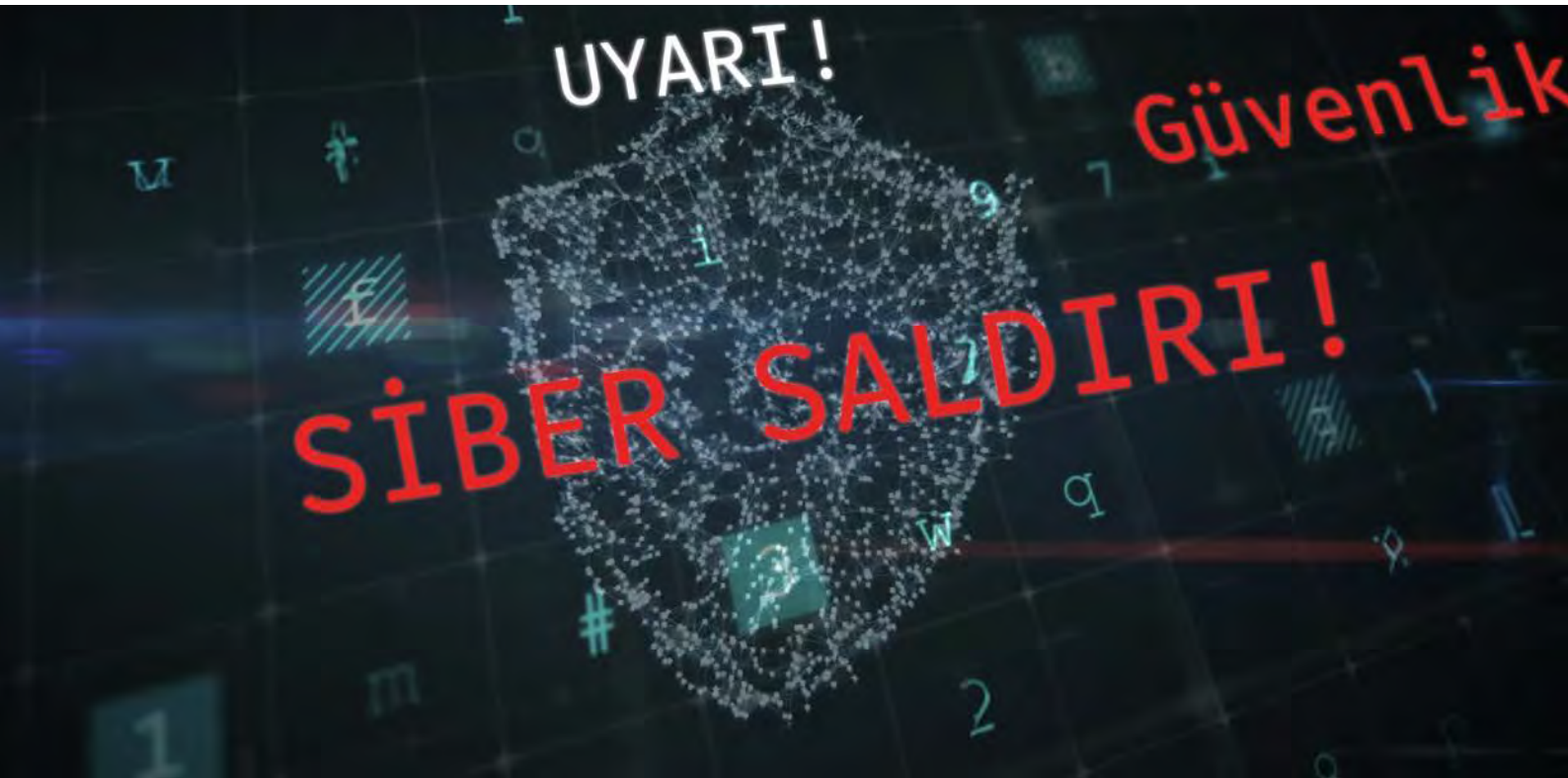
İdil KARAGÖZ

Siber güvenlik, dijital çağın en kritik konularından biri haline gelmiş durumda. Bilgi teknolojilerinin hızla geliştiği ve dijitalleşmenin yaygınlaştığı günümüzde, siber saldırılar hem bireylerin hem de kurumların günlük hayatını etkileyen önemli bir tehdit oluşturuyor. Bu tehditlerin kökeni oldukça eski olsa da modern anlamda siber suçlar tarihinin kilometre taşlarını oluşturan ilk saldırılar da mevcut.

Siber suçlar tarihinin ilk önemli saldırıları:

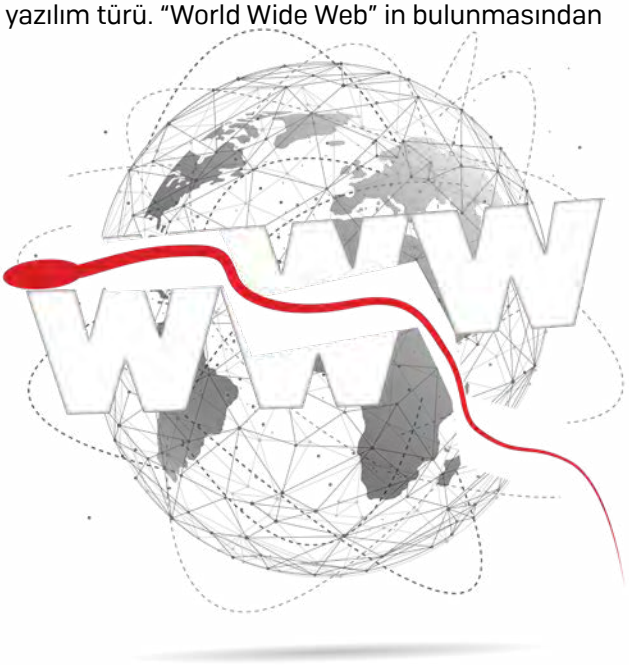
Blue Box

Modern siber saldırıların ilk örneklerinden biri, "Captain Chrunch" olarak da bilinen John Draper tarafından gerçekleştirilen telefon hırsızlığı. 1960'lar ve 1970'lerin başında yaygınlaşan telefon hırsızlığındaki amaç, kullanıcıların para ödemeden dünyadaki diğer kullanıcıları arayabilmesini sağlayacak bir yöntem bulmaktı. Draper da "Captain Chrunch" adlı kahvaltılık gevreğin içinden çıkan düdüğün sesinin, AT&T firmasının uzun mesafe aramasının bitişini bildiren uyarı sesi ile aynı frekansta, 2600Hz, olduğunu keşfetti ve bununla tüm dünyaya ücretsiz arama yapabilmenin mümkün olduğunu gösterdi. Sonrasında, Apple'ın kurucu ortağı olan Steve Wozniak ile tanışan Draper onunla birlikte bunu bir cihaza dönüştürme çalışmalarına başladı ve 1972'de "Blue Box" isimli cihazı yapmayı başardılar. Bu cihaz ile telefon firmaları tarafından kullanılan bildirim seslerini taklit ederek bedava arama yapabiliyorlardı.



Morris Solucanı

İnternet üzerinde yapılan ilk önemli saldırı ise 1988 yılında Cornell Üniversitesinde Yüksek lisans öğrencisi olan Robert Tappan Morris tarafından geliştirilen "Morris Solucanı". Solucan ağlar üzerinden yayılabilen ve kullanıcı etkileşimi gerektirmeden diğer sistemlere bulaşabilen zararlı bir yazılım türü. "World Wide Web" in bulunmasından



bir sene önce yayınlanan bu solucan, UNIX işletim sisteminin spesifik bir sürümünde bulunan güvenlik açıklarını kullanarak sisteme sızıp, kontrolü ele geçirmekteydi. Morris, solucanı tasarlarken asıl amacının, internetin güvenlik zayıflıklarını göstermek ve bilgisayar sistemlerinin savunmasız noktalarını vurgulamak olduğunu belirtmişti. Ancak solucan beklenenden daha hızlı yayıldı ve internetin o dönemdeki altyapısını ciddi şekilde etkiledi. Morris solucanı, bilgisayara ve bilgisayar içindeki dosyalara zarar vermemesine rağmen, internet trafiğinde ciddi sorunlara yol açarak Berkeley, Harvard, Princeton, Stanford, Johns Hopkins, NASA gibi kurumları etkiledi.

AIDS Trojan'ı

İlk fidye yazılımı AIDS Trojan'ı, 1989 yılında Joseph Popp tarafından geliştirildi. Fidye yazılımları bilgisayardaki dosyaları şifreleyerek kullanıcılardan, şifrelerin açılması için fidye talep eden zararlı yazılımlardır. Kurumsal ve bireysel internetin pek yaygın olmadığı bu dönemde "AIDS Trojan"ın yayılmasındaki temel metot, Popp' un Dünya Sağlık Örgütünün AIDS konferansına katılan 20,000 katılımcıya yazılımı disket olarak göndermesiydi. Popp tarafından dağıtılan diskler "AIDS Bilgi-Tanıtım Diskleri" olarak etiketlenmişti ve ek bir broşür içeriyordu. Disk takıldığında, metin tabanlı bir grafik görüntüleniyor ve bilgisayar yeniden başlatıldığında tekrar ortaya çıkıyordu. Program bilgisayarın kaç kere başlatıldığını takip edip, bu sayı 90'a ulaştığında dosya dizinlerini gizliyor ya da dosyaları şifrelenip kilitliyordu. Erişimi geri kazanmak için Panama'daki bir posta kutusuna PC Cyborg Corporation'a 189 dolar gönderilmesi gerekmekteydi. AIDS Trojanının riski minimaldi çünkü simetrik şifreleme kullanıyordu ve kısa sürede ödemeden dosyaları çözebilen araçlar ortaya çıktı.

90'larda telekomünikasyonda yaşanan gelişmeler sonucunda, telekomünikasyon ağları dünya çapında insanları birbirine bağladı. Bu gelişmeler siber saldırı sayısında ve yöntemlerinde artışı da yanında getirdi. Bilgisayar korsanları ve kötü niyetli aktörler, bu yeni teknolojiler geliştirilirken ve inşa edilirken güvenlik kontrollerinin başlangıçta göz ardı edilmesinden faydalandılar. O zamanlarda popüler internet servis sağlayıcıları, saldırganların kullanıcı bilgilerini çalması, oltalama saldırıları yapması ve servis kullanıcılarına spam mesaj ve eposta göndermesi sonucu saldırılarda bir vektör haline geldi.

Bu dönemdeki bazı önemli siber güvenlik olayları:

Kevin Mitnick

Kevin Mitnick 90'lar ünlü bir hacker olarak tanındı ve sosyal mühendislik becerilerini kullanarak çeşitli siber güvenlik saldırıları gerçekleştirdi. Mitnick, telefon hatlarını ve bilgisayar ağlarını manipüle ederek, kurbanlarından gizli bilgiler elde ediyordu. Özellikle bir şirketin çalışanlarını sosyal mühendislik yöntemleri ile kandırarak onlardan kullanıcı adı ve parola gibi bilgiler alıyordu. Bu bilgileri kullanarak birçok bilgisayar sistemine izinsiz erişim sağlayarak büyük çapta veri hırsızlıkları gerçekleştirdi. Motorola, Nokia ve Fujitsu gibi büyük teknoloji şirketlerinin sistemlerine sızarak ticari sırlar ve bilgiler çaldı. Mitnick'in bu etkili sosyal mühendislik saldırılarının arkasında dört aşamadan oluşan bir sistem bulunmaktaydı. İlk adımda hedef seçimi yaparak, saldıracağı sistem ve kişiler hakkında bilgi topluyordu. İkinci adımda, bu bilgileri kullanarak kendini güvenilir bir kaynak gibi gösterip, hedef kişilere yaklaşarak onların güvenini kazanıyordu. Üçüncü adımda, bu hedef kişilerden parola, kullanıcı adı veya sistem bilgileri gibi hassas bilgileri elde ediyor ve dördüncü adımda bu bilgileri kullanarak hedef sistemlere izinsiz erişim sağlıyor ve verileri çalıyordu. Mitnick'in saldırıları ve yakalanması, bilgisayar güvenliği ve sosyal mühendislik konularında bir dönüm noktası oldu.

ILOVEYOU virüsü

ILOVEYOU virüsü, 4 Mayıs 2000'de Filipinler'den yayılan ve tarihteki en yıkıcı bilgisayar solucanlarından biri olarak bilinir. Virüs, "I LOVE YOU" başlıklı bir epostada "LOVE-LETTER-FOR-YOU.txt.vbs" adlı bir ekte gönderiliyordu. Windows makinalarda .vbs dosya eklerinin görüntülenememesi sebebiyle kullanıcıların zararsız bir .txt dosyası zannederek açtığı ek ile virüs bilgisayarlarına bulaşıyor ve cihazlardaki .jpeg, .mp3, .js, .jse, .css gibi dosyaları tahrip ediyordu. Aynı zamanda virüs, etkilenen bilgisayarın Microsoft Outlook adres defterinde bulunan tüm kişilere kendini yeniden gönderiyordu, dolayısıyla oldukça hızlı yayıldı. Birkaç saat içinde

dünya genelinde milyonlarca bilgisayar bu virüsten etkilendi. Yedeklenmemiş olan bütün dosyalar kalıcı olarak silindi. Aynı zamanda ILOVEYOU, alıcının Internet Explorer ana sayfasını ve bazı Windows kayıt ayarlarını değiştiriyordu. ILOVEYOU, dünya çapında yaklaşık 10 milyar dolarlık zarara sebebiyet verdi, özellikle büyük şirketler, hükümet kurumları ve hatta askeri ağlar gibi kritik sistemleri etkiledi. Bu olay eposta güvenliği ve sosyal mühendislik saldırılarına karşı farkındalığı arttırdı ve dünya çapında bilgisayar suçlarına yönelik düzenlemelerin gözden geçirilmesine yol açtı.

2007 Estonya Siber Saldırıları

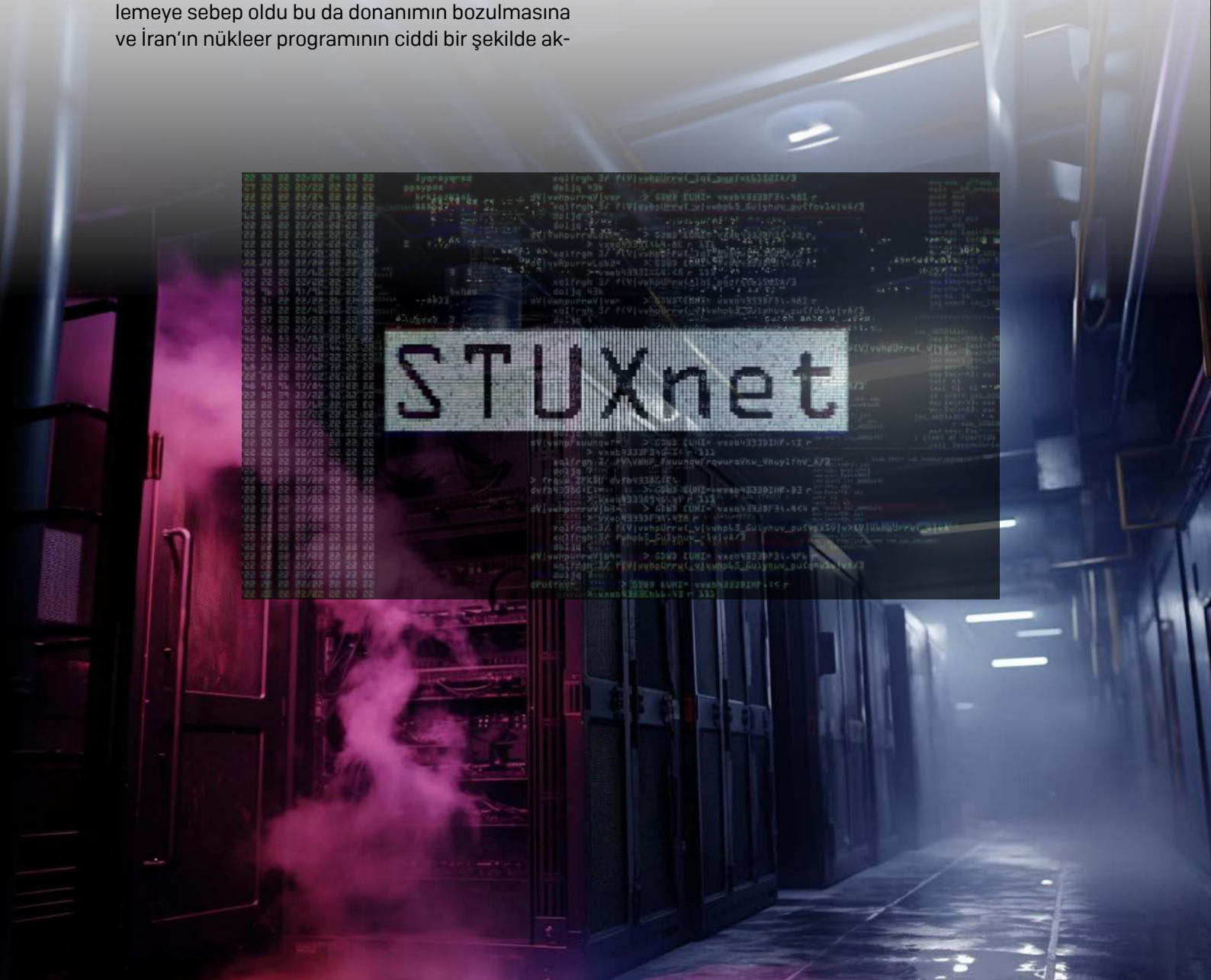
2007 yılında Estonya, dünya çapında yankı uyandıran büyük çaplı bir siber saldırıya maruz kaldı. Saldırıların sebebi olarak, Tallinn'de bulunan Sovyet dönemine ait "Bronz Asker" heykelinin başka bir yere taşınması ön görülüyordu. Bu saldırılar, 26 Nisan günü başladı ve üç hafta kadar sürdü. Özellikle, Estonya'nın kritik altyapılarına yönelik yoğun bir DDoS saldırısı başladı. DDoS (Dağıtılmış Hizmet Reddi) saldırıları, birçok arklı kaynaktan gelen yoğun bir trafik akışıyla bir hizmeti veya web sitesini erişilemez hale getirmeyi amaçlar. Saldırılar, Estonya'nın hükümet kurumlarının, medya kuruluşlarının, bankalarının ve birçok özel şirketin web sitelerini hedef alarak bu siteleri devre dışı bıraktı. Bu saldırılar Estonya'nın internet bağlantısını neredeyse tamamen durdurdu ve internet bağlantısı ile çalışan sistemlerini ciddi anlamda etkiledi. Özellikle finansal işlemler ve devlet hizmetlerinde büyük sorunlara yol açtı. Estonya, saldırıları yönetip etkilerini azaltabilmek için NATO ve Avrupa Birliği'nden yardım istedi. Saldırılardan sonra Estonya hükümeti ve NATO, siber güvenlik konusunda daha güçlü savunma mekanizmaları geliştirmek için adımlar attı. Bu olay siber güvenliğin önemi konusunda küresel bir farkındalık yarattı.

2010-2020 arası siber suçlarda büyük bir patlama yaşandı ve bir zamanlar daha küçük bir sektör olan bu alan, küresel bir iş haline geldi. Saldırganlar, siber suçları ve günlük saldırı sayısını arttıran yeni kötü amaçlı yazılımlar ve teknikler geliştirdi. Trilyonlarca dolar kaybedildi. Bu on yıl, fidye yazılımlarının yükselişine de tanıklık etti. Bitcoin gibi dijital para birimlerinin popülerleşmesi, kurumların dijitalleşmesi, mobil cihazların yaygınlaşması, yeni işletim sistemleri ve karanlık ağ, tehdit aktörlerine saldırılar için yeni yollar ve kaynaklar sundu. Siber suçlardaki bu yükseliş aynı zamanda siber güvenlik sektörüne de yansıdı. Kurumlar, siber tehdit riskine karşı koymak için daha fazla siber güvenlik uzmanı istihdam etmeye başladı.

Bu on yılın bazı önemli saldırıları:

Stuxnet

Stuxnet dijital dünyada devrim yaratan, gelişmiş bir siber silah olarak tarihe geçti. İlk olarak 2007'de faaliyete geçen Stuxnet solucanı, özellikle İran'ın nükleer programını hedef aldı ve 2010'dakı keşfinden sonra siber savaşın en çarpıcı örneklerinden biri olarak büyük yankı uyandırdı. Stuxnet, Siemens'in endüstriyel kontrol sitemleri (SCADA) üzerinde çalışan bilgisayarları hedef aldı ve sadece bu makineleri etkileyerek, Natanz'daki uranyum zenginleştirme tesisinde kullanılan santrifüjleri sabote etti. Bu sofistike zararlı yazılım, santrifüjlerin hızını kontrol ederek, aşırı yüklemeye sebep oldu bu da donanımın bozulmasına ve İran'ın nükleer programının ciddi bir şekilde aksamasına neden oldu. Stuxnet siber güvenlikte bir dönüm noktası oldu çünkü amacı sadece yazılımsal sistemlere değil aynı zamanda fiziksel hasara da sebebiyet vermekti. Saldırının arkasında ise ABD ve İsrail olduğu düşünülüyor, bu da Stuxnet'i devlet destekli bit siber savaş aracı olarak sınıflandırıyor. Yazılım, dört farklı "zero-day" açığından yararlanıyordu ve dört ana bileşenden oluşuyordu: bulaşma, saklanma, kontrol, sabotaj. Özellikle bulaşma aşamasında, Stuxnet kendini USB bellekler aracılığıyla yayarak, internet bağlantısı olmayan sistemlere dahi sızabiliyordu.



CryptoLocker Trojan'ı

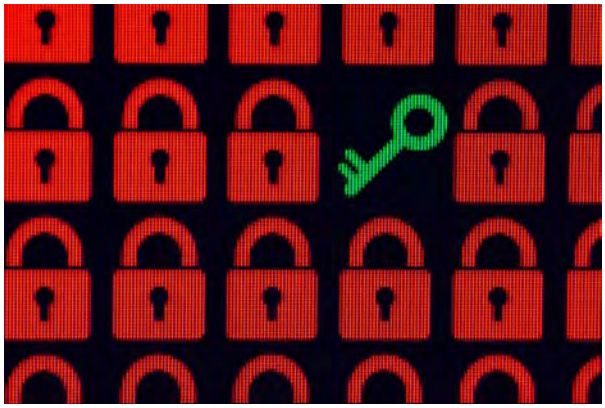
CryptoLocker fidye yazılımı saldırısı, 5 Eylül 2013'te gerçekleşti ve Mayıs 2014'ün sonuna kadar sürdü. Bu saldırı, çeşitli Windows işletim sistemi sürümlerini hedef alan bir Trojan olarak tanımlandı. CryptoLocker'ı asıl yayılış yöntemi eposta üzerinden oltalamaydı. Hedef bilgisayara meşru işletmelerin görünümünü taklit eden sahte bir eposta veya sahte bir FedEx ya da UPS takip bildirimleri aracılığıyla erişim sağlıyordu. Hedef bilgisayar enfekte olduktan sonra, CryptoLocker'ı bilgisayardan kaldırmak oldukça zor bir hale geliyordu çünkü virüs, paylaşılan ağ sürücüleri, USB sürücüleri, harici sabit diskler, ağ dosya paylaşım alanları ve hatta bazı bulut depolama sürücüleri içinde bulunan dosyaları, özgün bir anahtar ile şifreliyordu. 4 ay içinde, enfekte olan bilgisayar sayısı 250,000'e çıkmıştı. Dosyaları geri alabilmek için fidyeyi Bitcoin olarak ödemeniz gerekiyordu. Bu saldırganların kimliklerini korumalarına yardımcı oldu. Fidye mesajı, fidyenin nasıl temin edilip gönderileceğine dair talimatlar içeriyordu ve kullanıcıya talimatları tamamlaması için belli bir süre veriliyordu. Mayıs 2014'te, dünya çapında farklı siber güvenlik şirketleri ve emniyet teşkilatlarının çabalarıyla yapılan Tover operasyonu ile virüsün dağıtımında kullanılan Gameover Zeus botnet'i ele geçirildi ve elde edilen anahtarlar, hedef bilgisayarların kriptolarının çözümlenmesinde kullanıldı ve CryptoLocker etkisiz hale getirildi.

Türkiye DNS Saldırısı

14 Aralık 2015'te ülkemizdeki ns1.nic.tr ve ns5.nic.tr DNS sunucuları DDoS saldırısına uğradı. Bu saldırıdan dolayı 400,000'den fazla web sitesi erişim dışı kaldı ve DNS sunucuları kilitlendi. Saldırıyı hafifletip durdurabilmek için Türkiye'ye olan bütün internet trafiği durduruldu. Saldırıların menşeini gizlemek için sahte adresler kullanılarak yapıldığı tespit edildi.

Github'a DDoS Saldırısı

Şubat 2018'de Github, o dönemde kaydedilen en büyük DDoS saldırısına maruz kaldı ve bu saldırı 1.35 terabit/saniye (Tbps) ile zirveye ulaştı. Saldırı "memcached amplification attack" olarak bilinen bir yöntem kullanıldı. Bu teknik küçük sorgular göndererek büyük yanıtlar alınmasını sağlayan ve genellikle ağları ve veri tabanlarını hızlandırmak için kullanılan halka açık "memcached" sunucu-

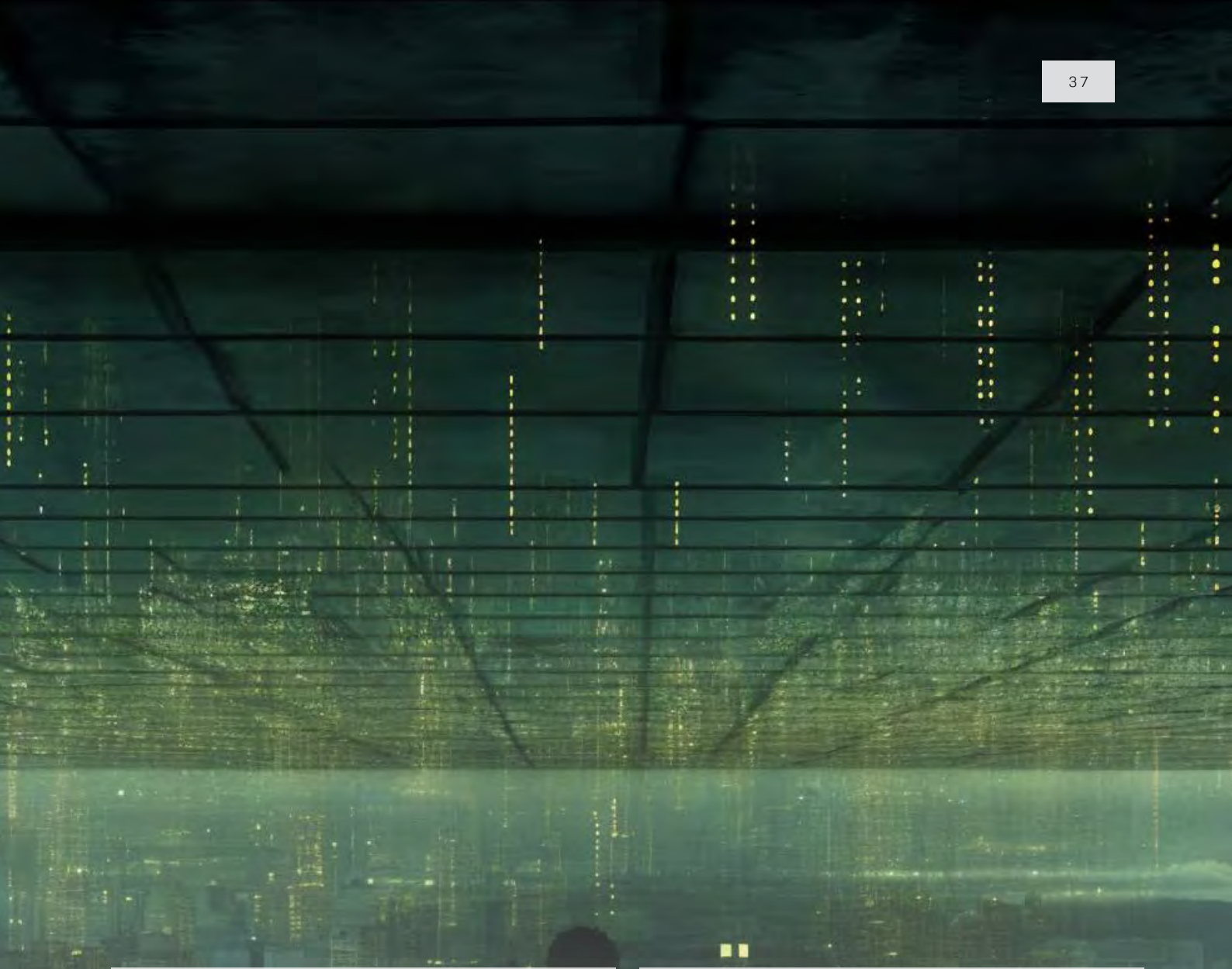


ların kötüye kullanılmasını içeriyor, bu da hedef sunucuya gönderilen veri miktarını önemli ölçüde arttırıyor. Github hızlı bir şekilde yanıt vererek Akamai Prolexic adlı DDoS önleme hizmetini devreye soktu. Bu hizmet trafiği kendi ağına yönlendirerek zararlı verileri filtreledi ve saldırının etkisini hafifletti. Github'ın hizmetler yaklaşık 10 dakikalık bir kesintiye uğradı. Bu olay, DDoS saldırılarının artan ölçeğini gösterdi ve etkili siber güvenlik önlemlerinin önemini vurguladı.

Petya, WannaCry ve NotPetya

Petya ilk olarak 2016 yılında tespit edilen bir fidye yazılımı türü. Diğer fidye yazılımlarında olduğu gibi Petya da hedef bilgisayardaki dosyaları ve verileri şifreliyor ve dosyaların tekrar kullanılabilir hale gelmesi için fidye talep ediyordu. Petya'yı benzerlerinden ayıran şey, diğer fidye yazılımlarının aksine, sadece önemli dosyaları şifrelemek yerine, bilgisayarın tüm depolama alanlarındaki bilgisayarın Ana Dosya Tablosunu (MFT) kullanarak şifreleyek kilitleyip, bilgisayardaki hiçbir dosyaya erişilememesine neden olmasıydı. Petya yalnızca Windows işletim sistemini kullanan bilgisayarları hedef aldı ve diğer fidye yazılımları gibi çoğunlukla eposta eki olarak yayıldı. Saldırganlar, insan kaynakları departmanlarına sahte iş başvuruları içeren e postalar gönderdiler. Bu epostalarda bulunan eklentiler ya bulaşıcı bir Dropbox bağlantısı ya da PDF olarak gizlenmiş çalıştırabilir dosyalar içeriyordu. Petya özellikle Ukrayna'yı etkiledi ve dünyanın geri kalanına yayıldı.

Petya'nın ortaya çıkışından bir sene sonra, Mayıs 2017'de, WannaCry ortaya çıktı. WannaCry'da Petya gibi bir fidye yazılımı saldırısıydı. Bu yazılım, Windows işletim sistemlerindeki SMB (Server Message Block) protokolünde bulunan bir güvenlik açığı olan "EternalBlue" adlı bir açıklık üzerinden yayıldı. Petya gibi WannaCry da dosyaları şifreleyip, kullanıcılardan Bitcoin olarak ödenecek bir fidye talep ediyordu. Saldırı 150'den



fazla ülkede 200,00'den fazla bilgisayarı etkileyerek büyük bir kaosa neden oldu. Bu kadar hızlı yayılmasının sebebi, Microsoft'un mart ayında yayınladığı, "Eternal Blue" açıklığını kapatan güncellemenin bilgisayarlara yüklenmemiş olmasıydı. Etkilenen kuruluşlar arasında İngiltere Ulusal Sağlık Servisi (NHS), İspanyol telekomünikasyon devi Telefonica, Renault gibi büyük kurumlar bulunuyordu. İngiltere'de hastaneler ve sağlık hizmetleri aksadı. Bir araştırmacı, WannaCry'ın "kill switch" (ölüm anahtarı) olarak bilinen mekanizmasını keşfetti ve yayılımını durdurdu fakat etkilenmiş olan bilgisayarlar şifrelenmiş bir şekilde kaldı.

WannaCry'ın başarısından sonra, Haziran 2017'de yeni bir fidye yazılımı olan NotPetya ortaya çıktı. Petya'ya birçok açıdan benzeyen NotPetya dünyadaki farklı kurumları etkiledi. 28 Haziran 2017'ye kadar 200 kurum bu yazılımdan etkilenmişti. NotPetya da Petya gibi bilgisayarın depolama alanındaki bütün dosyaları şifreliyordu fakat bunu ana Dosya Tablosunu kullanarak değil, doğrudan sabit diskleri şifreleyerek yapıyordu. NotPetya'nın yayılımında WannaCry'a benzer olarak "EternalBlue" önemli bir faktör olmuştu. Böylece insanların eposta eklerine tıklamasıyla değil, bağlandığı ağlarda doğrudan bir solucan olarak çalışabiliyordu. NotPetya, etkilediği bilgisayarlarda bir fidye mesajı gösterse de amacı tamamen zarar vermek üzerineydi ve dosyaların hepsini siliyordu.

2010'larda hem siber suçlarda hem de siber güvenlik önlemlerinde görülen gelişmeleri takiben 2020'lerde de iki alanda da gelişmeler devam ediyor. Teknolojideki gelişmeler iki tarafa da hizmet ediyor. Artan bulut hizmetleri, sanallaşma ve yapay zekâ uygulamaları, daha farklı siber suçlar doğururken, aynı zamanda, yeni önlemler de geliştiriliyor.

2020'den bugüne gerçekleşmiş bazı önemli olaylar:

LockBit

LockBit fidye yazılımı, otomatik olarak uygun hedefler seçiyor ve ağda bulunan bütün erişilebilir bilgisayarlara yayılıyor ve genelde spesifik hedef kurum ve kuruluşlara saldırılar yapmak için kullanılıyor. LockBit saldırganları şirketleri ve kurumları, operasyonlarını bozmak, zorla para almak ve hassas bilgilerini çalıp yayınlamakla tehdit ediyor. Faaliyetlerine Eylül 2019'ta başlayan LockBit, kendi kendisine yayılabilmesi, spesifik hedef kurumlarının olması ve kullanılan yazılım araçlarının benzerliğiyle "LockerGoga & MegaCortex" ailesine mensup bir virüs sayılıyor. LockBit benzerlerinden farklı olarak "hizmet olarak fidye yazılımı" modeliyle de çalışıyor. Üçüncü kişiler bir depozito ile istedikleri kuruma saldırı yaptırabiliyor. Buradan alınan fidyenin dörtte üçü LockBit yazılım ekibine, kalanı ise saldırı isteğinde bulunan üçüncü partiye gidiyor. Şimdiye kadar dünyanın her yanında birçok kurum ve kuruluş saldırıya uğramış. LockBit çalışma prensibi üç farklı aşamadan oluşuyor: Ağda açık bulmak, Ağa sızmak ve Dağıtım yapmak. Öncelikle ağda açıklık bulan saldırganlar, bu açıklığı kullanarak ağa sızıyor ve bir bilgisayara virüsü bulaştırıyor. Sonrasında, virüs otomasyon içerdiği için ağdaki diğer bilgisayarlara kendi kendine yayılabiliyor. Virüs aktif olduktan sonra sistemdeki dosyalar şifreleniyor ve bu şifreler sadece LockBit tarafından üretilmiş anahtarlarla açılabiliyor. LockBit hala aktif ve şimdilerde ağdaki sunucu datalarının kopyasını da alıp, bu datalarla şantaj girişiminde bulunuyorlar ve fidyeyi ödemeyen kurbanların datalarını açık olarak paylaşıyorlar.

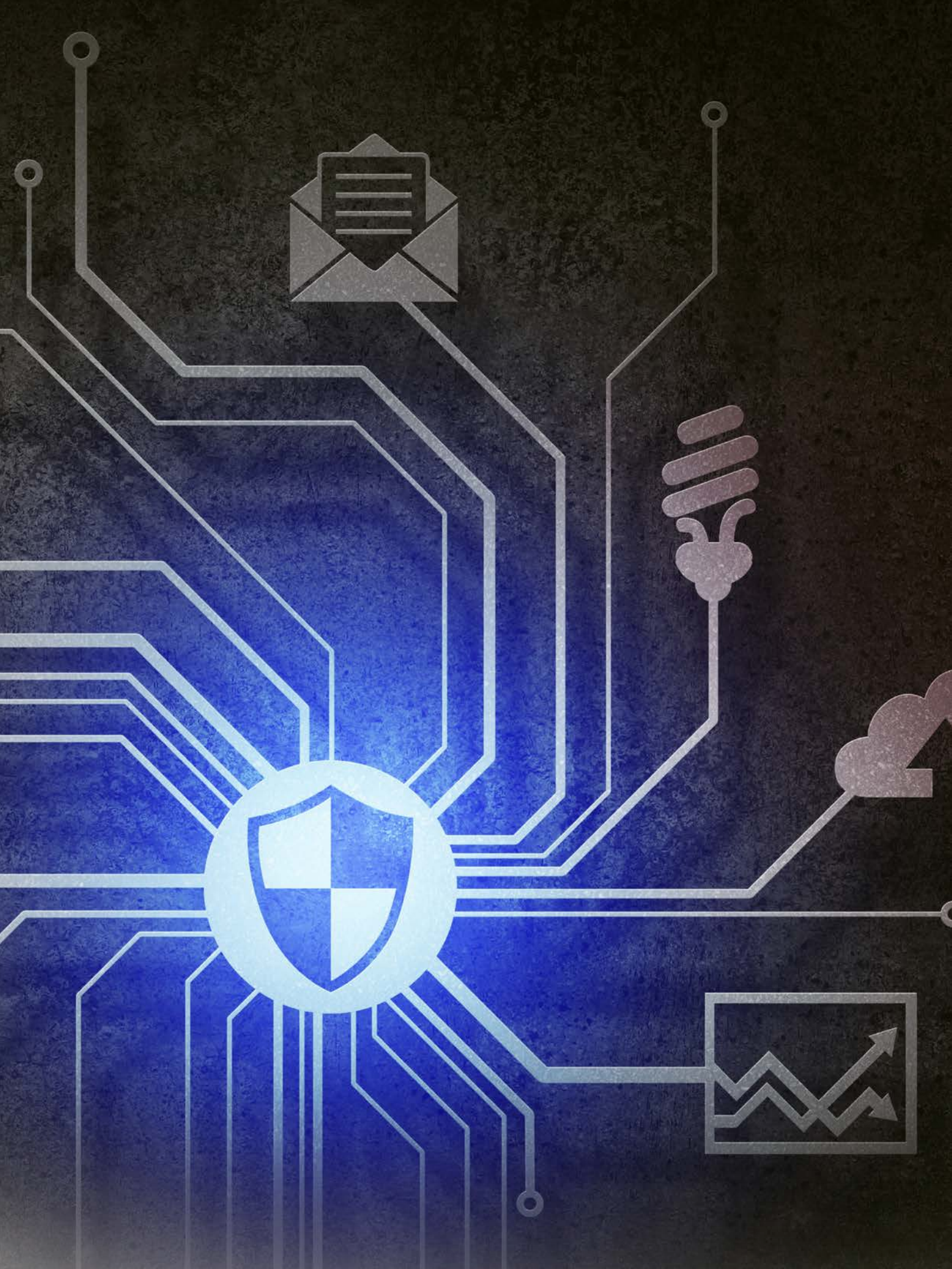
2022 Ukrayna Siber Saldırıları

2022 yılında, Rusya'nın Ukrayna'ya yönelik askeri saldırılarıyla birlikte, siber saldırılar da büyük bir artış gösterdi ve Ukrayna'nın kritik altyapılarına yönelik birçok tehdit ortaya çıktı. Ocak ve Şubat aylarında, Ukrayna'nın devlet kurumları ve bankacılık sistemlerine yönelik DDoS (Dağıtık Hizmet Reddi) saldırıları düzenlendi. Bu saldırılar, kamu hizmetlerini aksatarak panik ve kaos yaratmayı hedefliyordu. Örneğin, Ocak ayının sonunda, Ukrayna'nın dışişleri ve savunma bakanlıkları gibi önemli web siteleri hedef alındı ve bu siteler geçici olarak kullanılamaz hale geldi. Ayrıca, "HermeticWiper" adı verilen zararlı yazılım, Ukrayna'nın enerji ve iletişim altyapılarına sızarak veri silme işlemleri gerçekleştirdi ve bu da geniş çaplı hizmet kesintilerine neden oldu. Siber güvenlik uzmanları, bu tür saldırıları siber savaşın bir parçası olarak değerlendirerek, Rusya'nın bu yöntemleri askeri stratejilerinin bir uzantısı olarak kullandığını belirtti. NATO, Ukrayna'ya siber güvenlik desteği sağlarken, Avrupa ülkeleri de benzer saldırılara karşı kendi sistemlerini güçlendirmek için önlemler aldı. ABD, Ukrayna'ya siber saldırılara karşı koyabilmesi için teknik destek sağladı ve bu durum, siber tehditlerin modern savaşın ayrılmaz bir parçası haline geldiğini gözler önüne serdi. Ayrıca, siber saldırılar, yalnızca devlet kurumlarıyla sınırlı kalmayarak, enerji, iletişim ve finans sektörlerindeki özel şirketlere de yöneldi. 2022'de yaşanan bu siber saldırılar, siber güvenliğin günümüzdeki önemini ve siber savaşların fiziksel çatışmalarla nasıl iç içe geçtiğini gösterdi.

CrowdStrike

19 Temmuz 2024'te Amerikalı siber güvenlik şirketi CrowdStrike, Windows işletim sistemli bilgisayarları etkileyen hatalı bir güncelleme yayınladı. Bu güncelleme sonucunda 8,5 milyon sistem çöktü ve yeniden başlatılamadı. Bu kesinti dünya tarihinin en büyük kesintilerinden biri oldu. Kesinti oteller, havaalanları, borsalar hastaneler gibi binlerce kurumu, "Fortune 500"de bulunan şirketlerin %60'ı ve "Fortune 1000"de bulunan şirketlerin yarısını ve Microsoft Azure'da bulunan sanal makineleri etkiledi. Bu kesintiden dolayı yaşanan finansal zararın 10 milyar dolara yakın olduğu öngörülüyor. Olaydan birkaç saat sonra, hatanın kaynağının bir güvenlik açığı sensörü olan "Falcon Sensor"ün konfigürasyon güncellemesinde oluşan bir sorundan dolayı olduğu keşfedildi. Saat 04:09 UTC'de yayınlanan güncelleme, 05:27 UTC'de geri çekildi ve bu saatten sonra başlatılan bilgisayarlar sorundan etkilenmedi. Etkilenen bilgisayarlar için saat 09:45 UTC'de bir yama yayınlandı ve bu sorunun bir siber saldırı olmadığı belirtildi.

SİSTEM GÜVENLİĞİ MÜHENDİSLİĞİ



TASARIMIYLA GÜVENLİ SİSTEMLERE GENEL BAKIŞ: SİSTEM GÜVENLİĞİ MÜHENDİSLİĞİ VE TEHDİT MODELLEMESİ YOLUYLA SİSTEM GÜVENLİĞİNİ ARTIRMA

Dr. Murat DEMİRCİOĞLU
Berkan UFUK

Günümüzün dijitalleşen dünyasında donanım ve yazılım sistemlerinin güvenliği önemli bir rol oynamakta ve bu sistemleri hedef alan siber tehditler giderek daha karmaşık hale gelmektedir. Yüzde 100 güvenli veya sıfır zafiyetli bir güvenlik mimarisi oluşturmak pek mümkün görülmemektedir. Her ne kadar kesin güvenliği garanti edemiyor olsak da hassas dijital verilerin depolanması, işlenmesi ve iletilmesi için kullanılan teknolojilere yönelik siber güvenlik risklerini proaktif bir şekilde ele alarak güvenliği üst noktalara taşıyabiliriz. Bunun sonucunda, siber güvenliğin temel bir iş gereksinimi haline gelmesiyle birlikte güvenliğin sistem geliştirme yaşam döngüsünün her aşamasına dahil edilmesine vurgu yapan Tasarımıyla Güvenli adlı kapsamlı bir strateji oluşturulmuştur. Bu yazıda, Sistem Güvenliği Mühendisliği, Tasarımıyla Güvenli sistem geliştirme metodolojisi, Tehdit Modellemenin temel fikirleri anlatılmakta, her birinin güvenli ve siber dirençli sistemler oluşturmadaki önemi incelenmektedir.

Sızma Testi Yeterli Değil mi?

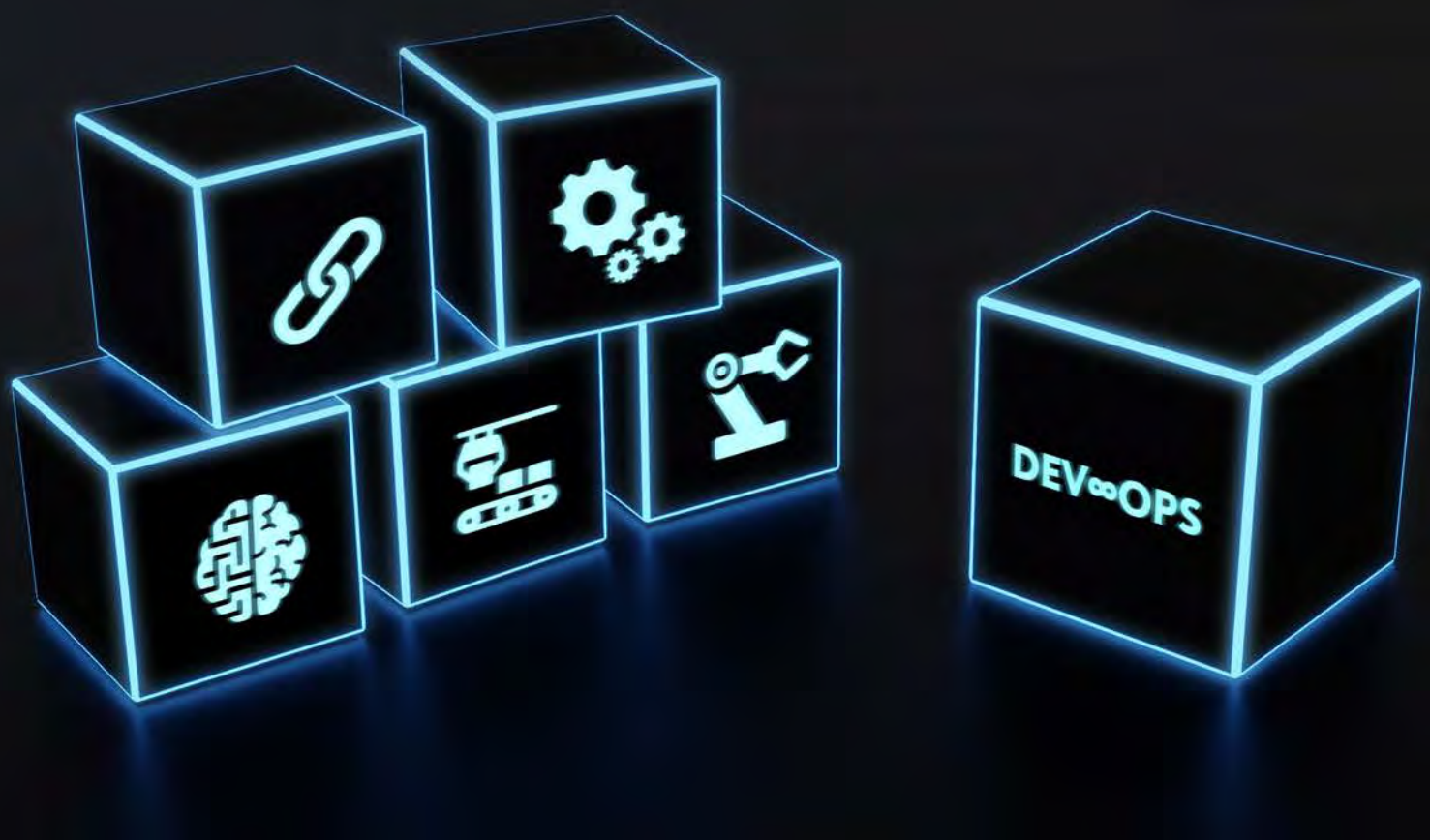
Güvenlikten bahsedince genel eğilim; bir sistem veya uygulama piyasaya çıkarılmadan önce siber saldırılara karşı değerlendirilmesine yönelik bir sızma testi yapılmasıdır. Tüm bilişim sistemlerinde işin doğası gereği çeşitli sıfırıncı gün açıklıkları ve tasarımsal zafiyetler bulunabilir. Herhangi bir güvenlik açığı ise sistemin gizlilik, bütünlük ve erişilebilirlik niteliklerine yönelik bir tehdidin gerçekleşmesine sebep olabilir. Bu güvenlik açıklarının kullanılması sonucunda veri, para, itibar kaybı ve hatta can kaybı meydana gelebilir. Yama yönetimi yalnızca sızma testi ile belirlenmiş olan güvenlik

açıklarını giderecektir. Eğer sistem tasarımının özünde bir güvenlik açığı varsa, uygulanacak çözümler son derece pahalı olabilir ve bazen düzeltilmesi imkânsız bile olabilir. Mevcut güvenlik açıklarını sızma testiyle ele almak ve güvenlik açıklarını buldukça yamamak, tesadüfi ve maliyetli bir süreç olmakla birlikte fazla efor gerektirmektedir. Sonuç olarak, siber güvenlikle ilgili sorunların mümkün olduğu kadar erken ele alınması her zamankinden daha önemli bir hal almıştır. Hiçbir şey, sistemleri başlangıçtan itibaren bir güvenlik bakış açısıyla tasarlamak kadar etkili olmayacaktır. Bu da bizi Tasarımıyla Güvenli sistemlerinin geliştirilmesi yönünde motive edecektir.

DevSecOps: Güvenliği Yazılım Geliştirme Sürecine Entegre Etmek

Tasarımıyla Güvenli, sistem geliştirme sürecinde güvenlik risklerini mümkün olduğu kadar erken tanımlamayı ve ele almayı amaçlayan proaktif bir yaklaşımdır. Kuruluşlar, güvenlik tanımlamalarını, iyi uygulama örneklerini ve gerekli kontrolleri projenin en başından itibaren ele alarak sistemlerinin güvenlik duruşunu önemli ölçüde iyileştirebilirler. Bu yöntem sayesinde, güvenlik sorunlarını ileride çözmek için gereken maliyet ve çaba azaltılırken aynı zamanda olası güvenlik açıkları ve tehdit riskleri de en aza indirilir.

Günümüzde güvenlik; yazılım, donanım ve IoT dahil olmak üzere birçok sistemin çok önemli bir bileşeni haline gelmiştir. Örneğin; yazılım geliştirme dünyasında Tasarımıyla Güvenli kavramı DevOps yazılım geliştirme metodolojisinde de yer almaya başlamıştır. Güvenlik testi ile birlikte statik ve dinamik kaynak kodu analizi faaliyetleri yazılım geliştirme hattına entegre edilerek tüm yaşam döngüsü boyunca devam eden bir güvenlik ekosistemi oluşturulmaktadır. Bu yaklaşım, geliştirme (development), güvenlik (security) ve operasyonlar (operations) anlamına gelen DevSecOps olarak tanımlanmakta ve güvenlik terminolojisinde "sola-kayma" (shift-left) olarak da bilinmektedir.



Peki Nedir Bu Sistem Güvenliği Mühendisliği?

Sistem, tanımlanmış bir ihtiyacı karşılamak ve belirlenmiş bir amaca ulaşmak için bir araya gelen unsurların bütünüdür. Ürünler (donanım, yazılım vb.), süreçler, insanlar, bilgiler, teknikler, yöntemler, tesisler, hizmetler gibi unsurlar bir sistemi oluşturabilir. Sistem tasarımında, genellikle performans ve maliyet gibi faktörler ön plandadır. Ancak güvenlik, sıklıkla ihmal edilen bir hususdur ve genellikle geliştirme sürecinin sonlarına doğru bırakılır. Sistemler tamamlandıktan sonra yapılan güvenlik kontrolleri veya sızma testleri ile güvenlik açıkları keşfedilir ve üçüncü taraf çözümlerle veya güvenlik yamalarıyla bulunan zafiyetler giderilmeye çalışılır. Ancak, güvenliği sistem geliştirme sürecinin her aşamasına entegre etmek, sistemlerin siber tehditlere karşı korunmasının en etkili yoludur. Bu sayede uygun maliyetli siber dirençli sistemlerin tasarlanması ve geliştirilmesi mümkün olur.

Sistem mühendisliği, beklenen sistem davranışını karşılayan, etkili sistem uygulaması ve işletimi ile sonuçlanan disiplinlerarası bir mühendislik alanıdır. Sistem güvenliği mühendisliği ise güvenli sistemler üretmek amacıyla güvenlikle ilgili konularla ilgilenen sistem mühendisliğinin bir dalıdır. Bu yaklaşım, risk analizleri yaparak, güvenlik önlemlerini değerlendirerek ve uyumluluğu sağlayarak sistem geliştirme yaşam döngüsünün her aşamasında güvenliği sağlamayı amaçlar. Tehditlerin ve güvenlik açıklarının tespit edilmesi, risk analizi ve azaltma tekniklerine karar verilmesi, tehdit modellemesinde sonuçların etkin bir şekilde iletilmesi gibi faaliyetler sistem güvenliği mühendisliği kapsamındadır. Bu disiplin, güvenilir ve emniyetli sistemler geliştirmeye yönelik yapılandırılmış, disiplinli bir yaklaşım sunar.

Tasarımıyla Güvenli Kültürünü Oluşturmak

Tasarımıyla Güvenli metodolojisi, sistem güvenliği mühendisliği ilkeleriyle hayata geçirilir. Sistem Güvenliği Mühendisliği, sistem mühendisliğinin önemli bir parçasıdır ve güvenli sistemlerin tasarımı, geliştirilmesi ve yönetimi için mühendislik fikirlerinin ve yöntemlerinin metodik kullanımını içerir. Sistem güvenliği mühendisliğinde gereksinim analizi, sistem mimarisi tasarımı, güvenli kod-

lama teknikleri, güvenlik testleri, sürekli izleme ve bakım gibi çok çeşitli faaliyetler yer alır. Mühendislik teknikleri ve güvenlik odaklı metodolojiler kullanılarak güvenlik hususlarının sistemin temellerine entegre edilmesini garanti etmeyi amaçlar.

Tasarımıyla Güvenli yaklaşımı, kuruluşların sistem mühendisliği süreci boyunca güvenlikle ilgili maliyetleri azaltmasına yardımcı olur. Güvenlik sorunlarına projenin başlangıcından itibaren dikkat edilmediğinde, sistemler siber tehditlere karşı savunmasız olabilir. Bu durum, fiziksel hasar, veri kaybı, mali kayıplar, itibar kaybı veya can kaybına yol açabilir. Ayrıca, siber olaylar ve sonrasında gerçekleştirilecek olan adli bilişim araştırmaları zaman alıcı ve maliyetlidir. Yasal düzenlemelere uyum sağlanmaması ise ciddi para cezalarına neden olabilir. Dahası, müşteriler kuruluşların veri koruma yeteneklerine olan güvenlerini kaybedebilir, bu da müşteri kaybına ve yeni müşteri bulmanın zorlaşmasına neden olabilir. Bu nedenle, Tasarımıyla Güvenli ilkelerinin herhangi bir proje veya sistemde uygulanmaması mali kayıplara, itibar kaybına ve hukuki sonuçlara yol açabilir.

Örnekler İhlaller: Tasarımıyla Güvenli'nin Önemi

- Equifax Veri İhlali (2017): Equifax, 147 milyondan fazla müşterinin kişisel bilgilerinin sızdırılmasına neden olan önemli bir veri ihlali yaşadı. Bu olay, Tasarımıyla Güvenli yönergeleri takip edilseydi önlenebilirdi.

- Mirai Botnet Saldırısı (2016): Savunmasız IoT cihazlarına bulaşarak geniş çaplı internet kesintilerine yol açan büyük bir DDoS saldırısı başlatıldı. Bu durum, güçlü kimlik doğrulama ve şifreleme gibi güvenlik kontrollerinin dikkatlice ele alınmasıyla önlenebilirdi.

- WannaCry Fidye Yazılımı Saldırısı (2017): Dünya çapında binlerce sistemin etkilendiği büyük bir fidye yazılımı saldırısı gerçekleşti. Kuruluşların saldırıya maruz kalmasının nedeni, yama yönetiminin gecikmesi ve Tasarımıyla Güvenli sistemlerde yapılan güncellemelerin ihmal edilmesiydi.

Bunlar gibi birçok örnek, Tasarımıyla Güvenli'nin önemini vurgulamakta ve kuruluşların güvenlik odaklı yaklaşımlar benimseyerek mali ve itibari kayıpları önlemelerinin ne kadar kritik olduğunu göstermektedir.

Sistem güvenliği mühendisliği ve sistem mühendisliği, birbirlerini tamamlayarak Tasarımıyla Güvenli kültürünü oluştururlar. Projelerin başlangıç aşaması, güvenlik sorunlarının ilk olarak ele alındığı ve belgelenmesi gereken bir dönem olmalıdır. Sistem mühendisliğinin her aşamasında güvenlik sorunlarıyla başa çıkmak için çeşitli stratejiler kullanılır. Güvenlik riskleri sürekli değiştiğinden, bunların etkili bir şekilde yönetilmesi için bir güvenlik riski yönetimi aracıyla belgelenmeli ve düzenli olarak güncellenmelidir.

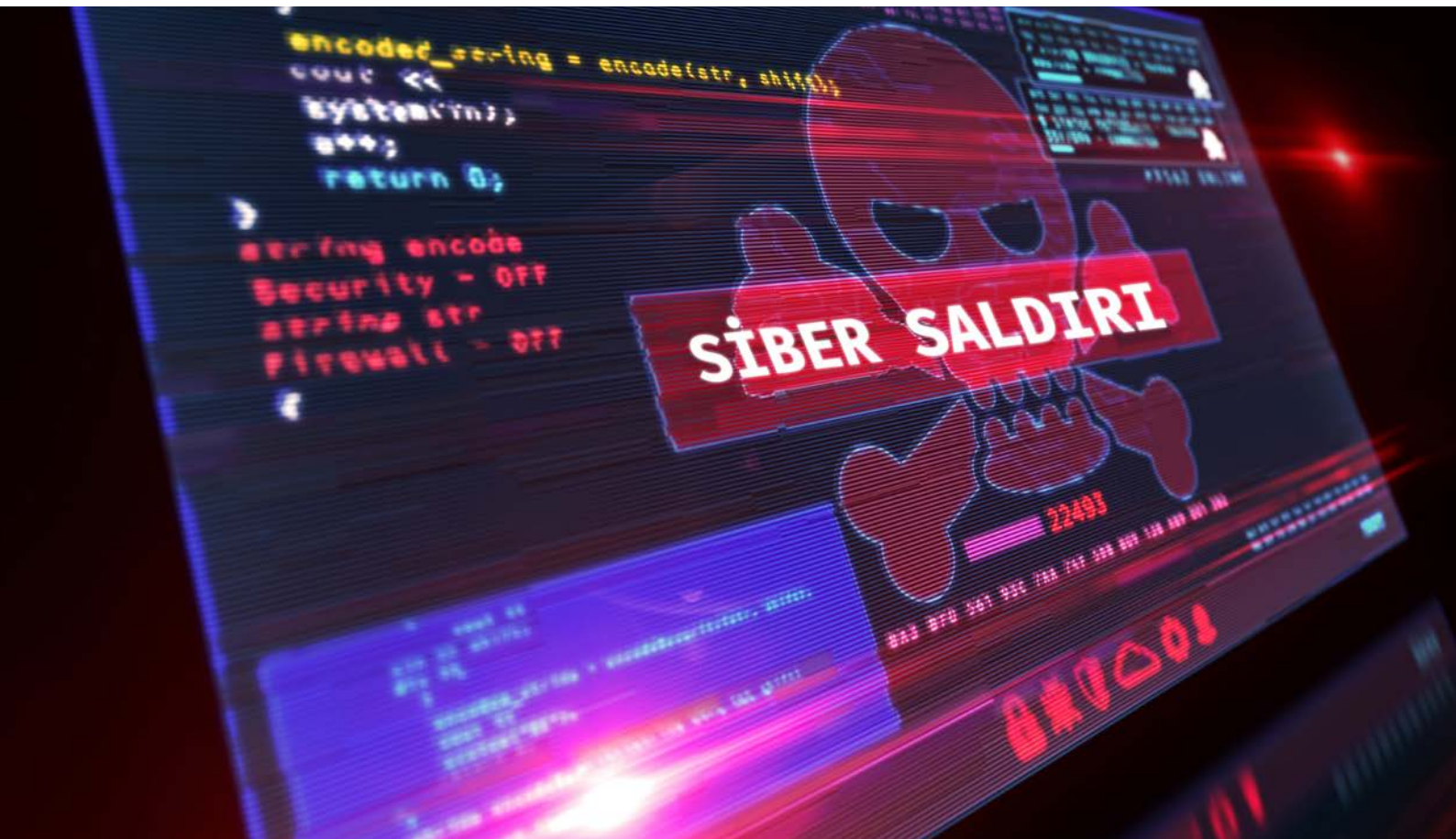
Güvenliğin sistem mühendisliğinin her aşamasında uygulanması, güvenlik risklerinin üst yönetim ve diğer paydaşlar tarafından açık ve net bir şekilde anlaşılmasını ve güvenlik riskinin kabul edilebilir bir düzeye indirilmesi için zamanında karar alınmasını sağlar. Microsoft, 2004 yılından bu yana ürünlerine güvenlik ve gizliliği entegre etmiş ve Microsoft Güvenli Geliştirme Yaşam Döngüsü (SDL – Secure Development Lifecycle) aracılığıyla bir güvenlik kültürü oluşturmuştur. SDL sürecinin beş aşaması, Tasarımıyla Güvenli zihniyetine ulaşmak için her türlü sistem mühendisliği faaliyetine uygulanabilir:

1. Gereksinimler: Güvenlik ve gizliliği artırmaya yönelik geliştirme ve destek maliyetlerinin, işin talepleri göz önüne alındığında makul olup olmadığının belirlendiği aşamadır.

2. Tasarım: En iyi uygulamaları belirlemek adına işlevsel ve tasarım spesifikasyonları kullanılırken, sistemdeki tehditleri ve zayıflıkları bulmak için risk analizi kullanılır.

3. Uygulama: Müşterinin sistemi güvenli bir şekilde dağıtması için ihtiyaç duyduğu kılavuzlar ve rehberlik araçları oluşturulur.

4.Doğrulama: Sistemin, doğrulama aşamasının önceki adımlarında tanımlanan güvenlik ve gizlilik gereksinimlerine uyduğu doğrulanır. Bunu başarmak için güvenlik testleri, tehdit modeli güncellemeleri, kod incelemesi ve belge kontrolleri kullanılır.



5. Yayınlama: Sistemin genel kullanıma hazır hale getirildiği aşamadır. Planlama, yayınlama aşamasındaki anahtar fikirlerden biridir. Herhangi bir güvenlik açığı bulunması durumunda karşı bir eylem planı hazırlanır ve yayınlanmadan önce son bir güvenlik incelemesi yapılır.

Tehdit Modellemesi: Güvenlikte Önleyici Bir Yaklaşım

Prof. Gene Spafford'un ifade ettiği gibi, "Gerçekten güvenli olan tek sistem, gücü kesilen, beton bir blok içine dökülen ve silahlı muhafızlarla kurşun kaplı bir odaya kapatılan sistemdir. Ve o zaman bile şüphelerim vardır."

Herhangi bir sistem, kararlı ve yetenekli düşmanlar, insan hataları, kazalar, bileşen arızaları, suiistimaller ve doğal felaketler gibi çeşitli potansiyel risklere maruz kalabilir. Bu nedenle, sistemlerde zafiyet ihtimalini göz önünde bulundurarak güvenlik tedbirlerimizi bu yönde almamız önemlidir. Bu noktada, etkili bir yöntem tehdit modellemesi veya diğer adıyla mimari risk analizidir.

Sistem güvenliği mühendisliğinin önemli bir unsuru olan Tehdit Modellemesi, güvenlik gereksinimlerini, potansiyel tehditleri ve güvenlik açıklarını belirlemek için sistematik bir yol sunarken, riskleri ölçer ve sistemdeki kritiklik düzeyine bağlı olarak gerekli iyileştirmeleri belirler. Kuruluşlar, potansiyel saldırı vektörleri ile birlikte potansiyel saldırganların niyetlerini ve yeteneklerini belirleyerek güvenlik kontrollerini etkili bir şekilde önceliklendirebilir ve gerekli kaynakları tahsis edebilir. Tehdit modelleme, güvenlik risklerine yeterli güvenlik önlemlerinin uygulanmasını sağlayarak işletmelerin tehditlerle nasıl başa çıkılacağı konusunda rasyonel kararlar almasını sağlar.

Tehdit modellemesi, sistemin saldırı yüzeyini doğru bir şekilde belirleyerek çeşitli tehditlere risk atanması ve güvenlik açıklarını azaltmaya yönelik bir süreçtir. Bu süreç, yazılımlardan donanımlara, sistemlerden ağlara ve Nesnelerin İnterneti (IoT) cihazlarına kadar geniş bir alanda uygulanabilir. Tehditleri belirleyerek ve ardından bu tehditlerin etkilerini azaltmak veya önlemek için karşı önlemleri tanımlayarak güvenliği artırmak için kullanılan bir faaliyetler silsilesidir.

Tehdit modellemesi, genellikle aşağıdaki dört soruyu içeren bir çerçeve üzerine kurulmuştur:

1. Ne üzerinde çalışıyoruz? Bu, bir sprint kadar küçük veya bir sistem kadar büyük olabilir.

2. Ne yanlış gidebilir? Bu, basit bir beyin fırtınası olabileceği gibi yapılandırılmış teknikler de kullanılabilir.

3. Bu konuda ne yapacağız? Her tehdit için risk azaltma stratejileri belirlenir ve risk yönetim yaklaşımları uygulanır.

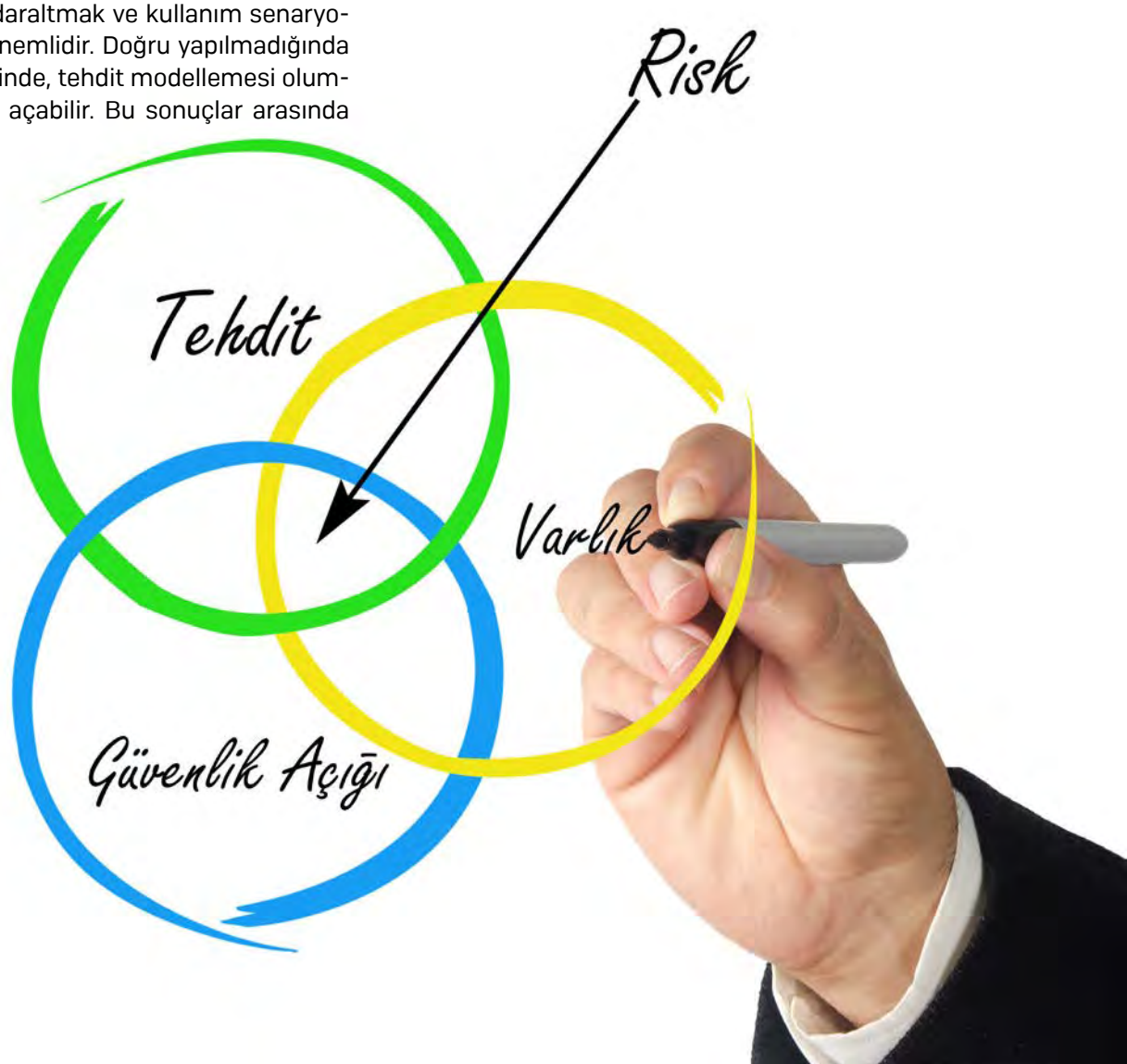
4. İyi bir iş mi yaptık? Sisteme yönelik güvenlik önlemlerinin yeterli olup olmadığı değerlendirilir.

Tehdit modellemesi, tüm potansiyel riskleri bulmak için zaman alıcı bir çalışma olabilir. Bu nedenle, arama alanını daraltmak ve kullanım senaryolarını belirlemek önemlidir. Doğru yapılmadığında veya ihmal edildiğinde, tehdit modellemesi olumsuz sonuçlara yol açabilir. Bu sonuçlar arasında fark edilmeyen güvenlik açıkları, yetersiz güvenlik önlemleri ve maliyetli reaktif güvenlik stratejileri bulunmaktadır.

Sonuç olarak, tehdit modellemesi, güvenlik açıklarını tespit etmek ve bunlara karşı korunma önlemlerini belirlemek için önemli bir araçtır. Bu yaklaşım, güvenlikte proaktif bir yaklaşımı teşvik eder ve reaktif stratejilerin maliyetli sonuçlarından kaçınmamıza yardımcı olur.

Tehdit modelleme süreci, sistemin güvenliğini sağlamak için kritik bir adımdır. İşte genellikle takip edilen adımlar:

1. Sistemi Tanımlama: Sistemin bileşenlerini, arayüzlerini, veri akışlarını ve bağımlılıklarını anlamak için başlangıç adımıdır. Bu, sistemin mimarisini ve tasarımını kavramanızı sağlar.



2. Varlıkları ve Veri Akışlarını Belirleme: Sistemde korunması gereken kritik varlıkları ve veri akışlarını tanımlamak önemlidir. Bu, veri toplama, işleme, depolama ve iletimini içeren süreçleri anlamanıza yardımcı olur.

3. Potansiyel Tehditlerin Belirlenmesi: Harici ve dahili tehditlerin yanı sıra kötü niyetli aktörlerin, bilgisayar korsanlarının ve içerideki kişilerin sistemi nasıl etkileyebileceğini belirlemek önemlidir.

4. Güvenlik Açıklarının Analizi: Belirlenen tehditlerin kullanabileceği güvenlik açıklarını değerlendirmek kritiktir. Bu, sistem mimarisi, tasarımı, kodu, yapılandırmaları ve uygulamasını analiz etmeyi içerir.

5. Risk Değerlendirmesi ve Azaltma: Her tehdide ilişkin riskleri analiz edin ve uygun risk derecelendirmesi atayın. Daha sonra, belirlenen riskleri azaltmak için uygun güvenlik kontrolleri ve karşı önlemleri geliştirin ve uygulayın.

6. Doğrulama ve İnceleme: Uygulanan güvenlik kontrollerinin etkinliğini doğrulayın ve sistemi düzenli olarak gözden geçirin. Sistem değiştikçe veya yeni tehditler ortaya çıktıkça tehdit modelini güncelleyin.

Bu adımların kullanılması, işletmelerin potansiyel tehditleri ve riskleri sistematik olarak tanımlamasına ve çözmesine yardımcı olur. Bu sayede daha dayanıklı ve güvenli sistemler oluşturulabilir.

Tehdit modelleme sürecinde, STRIDE yöntemi tehditlerin belirlenmesine ve sistemin güvenlik zafiyetlerinin analiz edilmesine yardımcı olur. Sisteme yönelik potansiyel tehditleri belirlemek için kullanılan bu yaklaşımda, tehditler altı farklı kategoriye ayrılmaktadır. Bu yöntem, sistemin ne tür tehlikelere maruz kalabileceğini anlamak için çok kullanışlıdır ve güvenlik uzmanları tarafından sıklıkla tercih edilir. İşte STRIDE'ın sorduğu sorular ve tehdit modelleme sürecindeki önemi:

1. Kimlik Sahtekarlığı (Spoofing): Bir saldırgan sahte kimlik kullanarak erişim sağlayabilir mi? Bu soru, kimlik doğrulama mekanizmalarının zayıflıklarını ve kimlik hırsızlığı risklerini değerlendirmeye yardımcı olur.

2. Kurcalama (Tampering): Bir saldırgan, uygulama boyunca akan verileri değiştirebilir mi? Bu soru, veri bütünlüğü ve veri değiştirme risklerini değerlendirmeye odaklanır.

3. Reddetme (Repudiation): Saldırgan bir şeyi yaptığını inkâr ederse, yaptığını kanıtlayabilir miyiz? Bu soru, kullanıcıların veya sistem bileşenlerinin eylemlerinin izlenebilirliği ve doğrulanabilirliği ile ilgilidir.

4. Bilgi İfşası (Information Disclosure): Bir saldırgan özel verilere erişebilir mi? Bu soru, gizlilik risklerini ve hassas verilerin korunmasını değerlendirir.

5. Hizmet Reddi (Denial of Service): Bir saldırgan sistemin çökmesine veya kullanılabilirliğinin azalmasına neden olabilir mi? Bu soru, sistem hizmetlerinin kesintiye uğrama risklerini ve hizmet reddi saldırılarını değerlendirir.

6. Ayrıcalığın Yükseltilmesi (Elevation of Privilege): Bir saldırgan ayrıcalıklı bir kullanıcının kimliğini üstlenebilir mi? Bu soru, yetkilendirme ve ayrıcalıkların doğru bir şekilde yönetilmesi gerekliliğini vurgular.

Veri Akış Şeması (DFD – Data Flow Diagram) gibi araçlar kullanılarak, sistem bileşenleri ve veri akışları ayrıntılı bir şekilde incelenir. Bu, sistemin farklı seviyelerindeki tehditleri ve riskleri tanımlamak için bir çerçeve sağlar. Bu süreç, sistemin güvenliğini artırmak için alınacak önlemleri belirlemeye ve doğrulamaya yönelik aksiyonları içerir.

Tehdit modellemesi için bir dizi araç ve yöntem bulunmaktadır. Veri akış diyagramları oluşturmak için genel araçlar kullanılabileceği gibi, tehdit modelleme için özel olarak tasarlanmış araçlar da mevcuttur. Bu araçlar, tehditleri tanımlamak, riskleri değerlendirmek ve güvenlik kontrolleri geliştirmek için kullanılır.

İşte bazı popüler tehdit modelleme araçları:

1. Microsoft Tehdit Modelleme Aracı: Microsoft tarafından geliştirilmiş ve tehdit modellemesi için bir çerçeve sağlar. Sistemlerin ve uygulamaların güvenlik açıklarını belirlemek ve ele almak için kullanılır.

2. OWASP Threat Dragon: OWASP (Açık Web Uygulaması Güvenliği Projesi) tarafından sağlanan açık kaynaklı bir tehdit modelleme aracıdır. Uygulamaların güvenlik risklerini değerlendirmek için kullanılır.

3. IriusRisk: Kurumsal düzeyde tehdit modelleme ve risk değerlendirmesi sağlayan bir platformdur. Özellikle büyük ölçekli projeler için uygun olan geniş bir özellik yelpazesine sahiptir.

4. ThreatModeler: Kullanıcı dostu bir arayüze sahip olan ThreatModeler, karmaşık sistemlerin tehdit modellemesini kolaylaştırır. Hem büyük hem de küçük ölçekli projeler için uygundur.

5. PyTM: Python tabanlı açık kaynaklı bir tehdit modelleme aracıdır. Esnekliği ve özelleştirilebilirliği sayesinde çeşitli ortamlarda kullanılabilir.

Başarılı bir tehdit modellemenin sonucunda, sistem için özel güvenlik gereksinimleri ve güvenlik kontrolleri belirlenir. Bu gereksinimler ve kontroller, çeşitli standartlar ve kontrol listeleri kul-

lanılarak belirlenebilir. Örneğin, NIST SP 800-53 ve Bulut Kontrol Matrisi gibi standartlar, geniş bir güvenlik kontrol yelpazesi sunar ve çeşitli sektörlerde uygulanabilir. Ayrıca, sistem mühendisliği sürecinde uyulması gereken ek standartlar, kanunlar, mevzuatlar veya düzenlemeler de dikkate alınmalıdır. Bu, sistemlerin belirli sektör gereksinimlerini karşılamasını ve yasal uyumluluğu sağlamasını sağlar.

Zorluklar

Güvenli sistemlerin tasarımı ve uygulanması bir dizi zorluk ve açık sorunlarla karşılaşabilir. Bu zorluklar ve açık sorunlara odaklanmak, güvenli sistemlerin geliştirilmesi ve güvenlik standartlarının iyileştirilmesi için önemlidir. İşte bazı temel zorluklar ve açık sorunlar:

1. Karmaşık Tasarım ve Uygulama: Güvenli sistemlerin tasarımı ve uygulanması, birçok bileşenin ve teknolojinin etkileşimi nedeniyle karmaşık olabilir. Ayrıca, diğer tasarım hedefleriyle çelişen güvenlik gereksinimleriyle başa çıkmak da zor olabilir.

2. Yetersiz Bilgi ve Kaynaklar: Birçok geliştirme ekibi, güvenli tasarım metodolojilerini etkin bir şekilde uygulamak için yeterli bilgi ve uzmanlığa sahip olmayabilir. Bu durum, güvenlik açıklarının gözden kaçırılmasına veya yanlış şekilde ele alınmasına neden olabilir.

3. Kullanılabilirlik ve Güvenlik Dengesi: Güvenlik önlemleri, kullanılabilirlik ve kullanıcı deneyimi üzerinde olumsuz etkilere sahip olabilir. Bu nedenle, güvenlik ve kullanılabilirlik arasında denge kurmak önemlidir ancak zorlu bir süreçtir.

Bu zorlukların üstesinden gelmek için çeşitli açık problemler ile ilgilenmek gerekmektedir:

1. Etkili Değerlendirme ve Ölçüm: Tasarım yoluyla güvenliğin etkinliğini değerlendirmek için standartlaştırılmış kriterlere dayanan ölçüm ve değerlendirme prosedürleri geliştirmek önemlidir.

2. Otomatik Araçlar ve Çerçeveler: Geliştiricilere güvenli tasarım metodolojilerini kullanmalarına yardımcı olacak evrensel kabul görmüş otomatik araçlar ve çerçeveler oluşturmak gerekmektedir.

3. Tehdit Modellemeyi Güvenlik Kontrolleriyle Entegre Etmek: Tehdit modellemesi sonuçlarının güvenlik kontrollerinin seçimi ve uygulanmasıyla entegre edilmesini sağlayacak rehberlik yöntemleri ve çerçeveler geliştirmek önemlidir.

Bu açık sorunların çözümü, güvenli sistemlerin tasarımı ve uygulanmasında önemli adımlar atılmasına yardımcı olabilir ve endüstrinin genel güvenlik seviyesini artırabilir.

Sonuç ve Öneriler

Toparlamak gerekirse, güvenliğin operasyon ve bakımın her yönünü kapsayan bütünsel bir yaklaşımla ele alınması önemlidir. Güvenliğin, statik bir unsur olarak değil, sürekli bir çaba gerektiren bir olgu olduğunu bilinmelidir. Kuruluşlar, değişen tehditleri ve güvenlik açıklarını sürekli olarak göz önünde bulundurmalı ve güvenlik önlemlerini buna göre uyarlamalıdır. Güvenlik, sistemi kurmak ve ardından güvence altına almanın değil, tasarım sürecinin merkezinde yer almalıdır. Bu nedenle, kuruluşlar güvenliği öncelik haline getirmeli ve uygulamalarını buna göre ayarlamalıdır.

Güvenlik, işi desteklemesi gereken temel bir iş gereksinimidir ve sistemin kullanılabilirliğini tehlikeye atmadan sağlanmalıdır. Ayrıca, güvenlik ile sistem maliyeti ve teknik performansı arasında bir denge bulunmalıdır. Bu denge noktasına Makul Olarak Uygulanabildiği Kadar Güvenli (ASARP - As Secure As Reasonably Practicable) denir. ASARP, güvenliği maksimum seviyede sağlamak için gereken önlemlerin, sistemin maliyet ve performansını makul bir şekilde etkileyecek seviyede olması anlamına gelir.

Bu ilkeleri benimseyen ve uygulayan kuruluşlar, güvenlik standartlarını yüksek tutabilir ve olası riskleri minimize ederek daha güvenli sistemler oluşturabilirler.

aselsan

SİBER ZIRH PROGRAMI

SİBER ZIRH PROGRAMI

Siber Zırh Programı kurumların güvenlik altyapılarını oluşturan in san, süreç ve teknoloji yapıtaşlarının risk tabanlı bütüncül bakış açısı ile değerlendirilmesi, eksikliklerin ortaya çıkartılması ve ku rumsal siber direncin artırılmasını hedeflemektedir.

Siber Güvenlik, uzun yıllar boyunca teknik bir sorun olarak ele alınmış, çözüm ise süreçler ve teknolojik ürünlerde aranmıştır. Günümüzde ise Siber Güvenlik stratejik seviyede risk temelli dü şünülmesi gereken bir olgu haline gelmiştir.

ASELSAN bünyesinde hayata geçirilen güvenlik programı Siber Zırh'ın temelinde modern güvenlik yaklaşımları ile insan, süreç, teknoloji ve yönetişim ilkeleri ile kurgulanmış iş odaklı bir mimari model yer almaktadır.

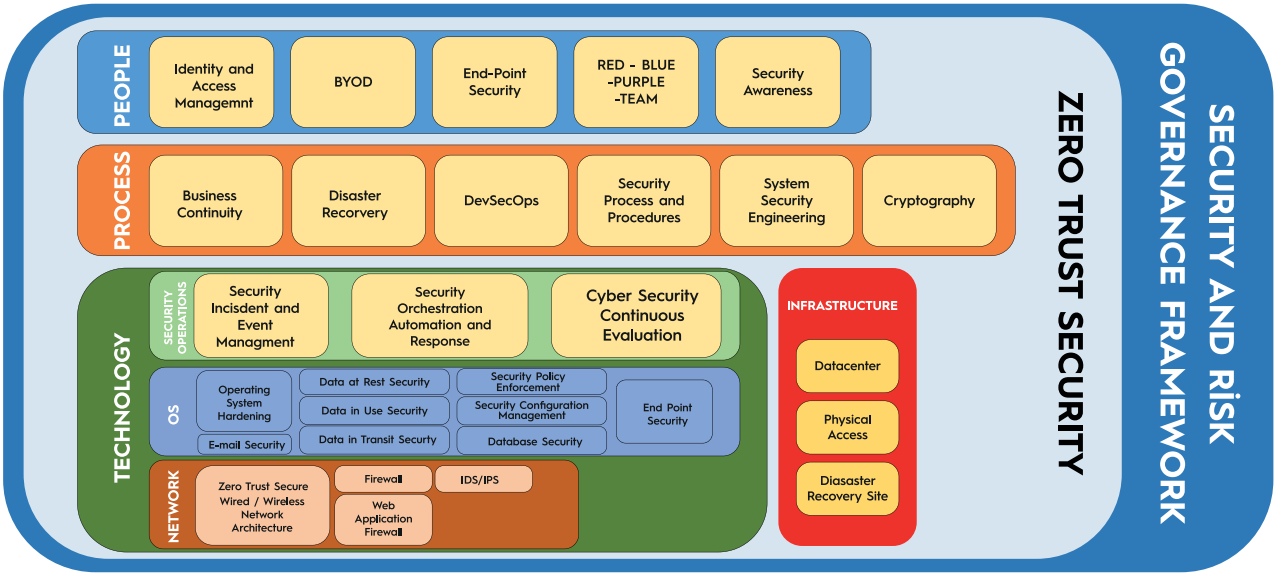
Gerçekçi ve dinamik bir model olarak tasarlanan Siber Zırh Prog ramı uygulanacak organizasyonun yapısal büyüklük ve faaliyet alanına bakılmaksızın kurumsal güvenlik anlayışının oluşturulma sı, güvenlik hizmetlerinin sürdürülebilir, gelişebilir ve genişleyebilir bir yapıya dönüştürülmesi hedeflenmektedir.

Siber Zırh Programı siber güvenliğin kompleks ve karmaşık se runlarına sistematik yöntemlerle çözümler üretmektedir. Ölçek lendirilebilir gerçekçi yapısı ile Siber Zırh'ın amacı insan, süreç ve teknoloji üçlemesini çevreleyen kurumsal bir güvenlik kültürünün oluşturulmasıdır.

Siber Zırh çerçeve programı 7 ana başlığı kapsamaktadır. Bunlar;

- Güvenlik Mimarileri
- Güvenlik Operasyonları
- Tehdit İstihbaratı
- Risk Değerlendirme
- Güvenlik Yönetişimi
- Siber Güvenlik Programları ve Standartlar
- Kişisel Gelişim ve son Kullanıcı Eğitimleri

Bu 7 ana başlık, veri odaklı güvenlik ve sıfır güven güvenlik tekno lojileri risk tabanlı bir yönetişim modeli ile ele alınmaktadır.



Özellikler önceden bildirilmeksizin değiştirilebilir. | Tüm değerlerin toleransı ±%10'dur.

KÜRESEL DÖNÜŞÜMÜN ÖNEMİ: SİBER DAYANIKLILIK

Ali IŞIKLI

Teknoloji, günümüz dünyasında hayati bir öneme sahiptir. Dijitalleşme, iş süreçlerinin verimliliğini artırırken, iletişimi kolaylaştırır ve küresel bağlantıları güçlendirir. Ancak, bu dijital dönüşüm aynı zamanda siber tehditlerin artmasına neden olmuştur. Siber saldırılar, kurumlar için ciddi mali ve itibari zararlara yol açmaktadır. İşte bu noktada, kurumlar siber saldırılara karşı dirençli olmak için güvenli tasarım prensiplerini benimseyerek siber dayanıklılığı artırabilirler. Bu makalede, güvenli tasarımın siber dayanıklılığı nasıl sağladığını inceleyeceğiz.

Siber dayanıklılık, bir kurumun veya organizasyonun, siber saldırılar veya diğer siber tehditler karşısında dirençli olma yeteneğidir. Bu, saldırıların önlenmesi, algılanması, yanıtlanması ve iyileştirilmesi süreçlerini içerir. Siber dayanıklılık, kurumun operasyonlarını kesintiye uğratmadan siber tehditlere karşı dirençli olmasını sağlar.

Tasarımı ile güvenlik veya güvenli tasarım ise, bir ürün veya sistem oluşturulurken güvenlik gereksinimlerinin ve önlemlerinin başlangıçtan itibaren dikkate alınması anlamına gelir. Bu, ürün veya sistem geliştirme sürecinin her aşamasında güvenlik risklerinin değerlendirilmesini, azaltılmasını ve yönetilmesini içerir.

Güvenli tasarımın önemi, siber tehditlerin artması ve daha da karmaşık hale gelmesi ile birlikte daha da artmıştır. Geleneksel olarak, siber güvenlik, bir ürün veya sistemin son aşamasında eklenen bir özellik olarak düşünülürdü. Ancak, bu yaklaşım artık yeterli gelmemekte hatta günümüzde hatalı bir uygulama olarak tanımlanmaktadır. Güvenli tasarım, siber güvenliği ürün veya sistemin temel bir parçası haline getirir. Bu sayede sistemler siber saldırılara karşı daha dirençli hale gelir ve etkili bir savunma sağlar.

Siber dayanıklılığı sağlamak için bir dizi temel unsur vardır:

- Bir kurumun siber tehditlere maruz kalma riskini değerlendirmesi gerekir. Bu, varlık envanteri, tehdit modellemesi ve risk analizi gibi süreçleri içerir.
- Kurumlar, güvenlik politikaları, güvenlik yazılımları ve eğitim programları gibi önleyici tedbirler almalıdır.
- Siber saldırıların hızlı bir şekilde algılanması ve etkili bir şekilde yanıtlanması hayati öneme sahiptir. Bu, güvenlik olaylarının izlenmesi, tehditlerin tespit edilmesi ve saldırılara karşı müdahale edilmesi süreçlerini içerir.
- Bir siber saldırı meydana geldiğinde, kurumun operasyonlarını en kısa sürede normale döndürebilmesi için iyileştirme ve geri kazanma süreçleri önemlidir.

Siber dayanıklılık, sadece teknolojik çözümlerle değil, aynı zamanda kurumsal kültürle de yakından ilişkilidir. Bir kurumun siber güvenlik bilinci yüksek bir kültür geliştirmesi, çalışanların eğitilmesi ve bilinçlendirilmesi önemlidir. Ayrıca, kurumların üst yönetimleri tarafından siber güvenliğe verilen önemin vurgulanması ve gerekli kaynakların sağlanması da kritik öneme sahiptir.

Güvenli tasarım, siber dayanıklılık ilkesinin en önemli temel taşlarından birisidir. Güvenli tasarım, ürün veya sistemlerde önleyici güvenlik önlemlerinin koşulsuz uygulanmasını sağlar. Bu, potansiyel saldırı vektörlerini azaltarak siber saldırıların

önlenmesine yardımcı olur. Buna ilave olarak güvenli tasarım ile ürün veya sistemlere siber saldırıları algılama ve bunlara yanıt verme yetenekleri kazandırılır. Güvenli tasarlanmış bir sistem, saldırıların erken aşamalarda tespit edilmesine ve etkili bir şekilde önlem alınmasına olanak tanır. Güvenli tasarım, sürekli olarak güncellenen ve iyileştirilen bir yapı sağlar. Bu, yeni tehditlere karşı daha hızlı bir şekilde adapte olmayı mümkün kılar.

Güvenli tasarımı benimseyen kurumlar, siber güvenlik bilincinin artmasına ve kurumsal kültürün güçlenmesine katkıda bulunur. Çalışanlar, güvenli tasarım ilkelerini benimseyerek güvenlik açıklarını azaltmaya yardımcı olabilirler.

Güvenli tasarımın temel prensipleri şu şekilde sıralanabilir:

- Ürün veya sistem, varsayılan olarak güvenli olmalıdır. Ürün veya sistemlerde bulunan güvenlik ayarları ve yapılandırmaları varsayılan olarak etkin olmalıdır. Kullanıcılar ek güvenlik önlemleri almadan da sistem veya ürünler yeterli güvenlik güvencesini sağlamalıdır.
- Ürün veya sistem, minimum sayıda ayrıcalık ve erişimle çalışmalıdır. Bu, sayede siber saldırı yüzeyi daraltılarak saldırganların işleri zorlaştırılmaktadır.
- Ürün veya sistem, birden fazla savunma katmanı ile korunmalıdır. Derinlemesine güvenlik (Defence in depth) olarak adlandırılan bu yöntem ile tek bir savunma hattının kırılması durumunda bile saldırı farklı katmanlarda durdurulabilir.
- Güvenlik, sistem tasarım, geliştirme ve idame süreçlerinin temel bir parçası olmalıdır. Bu, yazılım güvenliği, ağ güvenliği, veri güvenliği ve fiziksel güvenlik gibi çeşitli alanları içermelidir.

Türkiye, dijital dönüşümün hızla yaşandığı bir ülkedir ve bu nedenle siber tehditlere karşı dayanıklılık önemlidir ve güvenli tasarımın önemi giderek artmaktadır. Ülkemiz kurumları, kamu ve özel sektörde, siber güvenlik stratejilerini geliştirmekte ve uygulamaktadır. Siber saldırılara karşı koruma sağlamak, algılamak ve yanıtlamak için çeşitli kurumsal girişimler ve ulusal düzeyde politikalar bulunmaktadır.

Güvenli tasarım, siber dayanıklılığın sağlanmasında kritik bir rol oynar. Kurumlar, ürün ve sistemlerini güvenli tasarım ilkelerine göre oluşturarak siber tehditlere karşı daha dirençli hale gelebilirler. Güvenli tasarımın benimsenmesi, siber güvenlik kültürünün geliştirilmesi ve son kullanıcıların korunması için önemlidir. Türkiye'deki kurumlar, güvenli tasarımı birinci sınıf bir öncelik olarak kabul etmeli ve siber dayanıklılıklarını artırmak için bu ilkeleri uygulamalıdır.

Ancak, Türkiye'deki özel sektör ve kamu kurumlarının siber güvenlik olgunluk seviyeleri hala gelişmekte olan bir süreçtedir. Siber tehditlerin karmaşıklığı ve çeşitliliği göz önüne alındığında, sürekli olarak güncellenen ve geliştirilen bir siber güvenlik stratejisinin benimsenmesi önemlidir.

Siber dayanıklılık, günümüzün dijital dünyasında hayati bir öneme sahiptir. Kurumlar, siber tehditlere karşı dirençli olmak için siber güvenlik stratejilerini güçlendirmeli ve sürekli olarak iyileştirmelidirler. Ayrıca, siber güvenlik bilincinin artırılması ve kurumsal kültürün güçlendirilmesi de önemlidir. Türkiye'deki kurumlar hala güvenli tasarımın tam potansiyelini gerçekleştirmekte biraz geride kalmaktadır. Bu nedenle, Türkiye'deki kurumlar, güvenli tasarımı birinci sınıf bir öncelik olarak kabul etmeli ve siber dayanıklılıklarını artırmak için bu ilkeleri uygulamalıdır. Türkiye'de, siber güvenlik alanında ilerleme kaydedilmesine rağmen, daha fazla çaba ve yatırım gerekmektedir.

KRİPTOLOJİ VE BİLGİ GÜVENLİĞİ

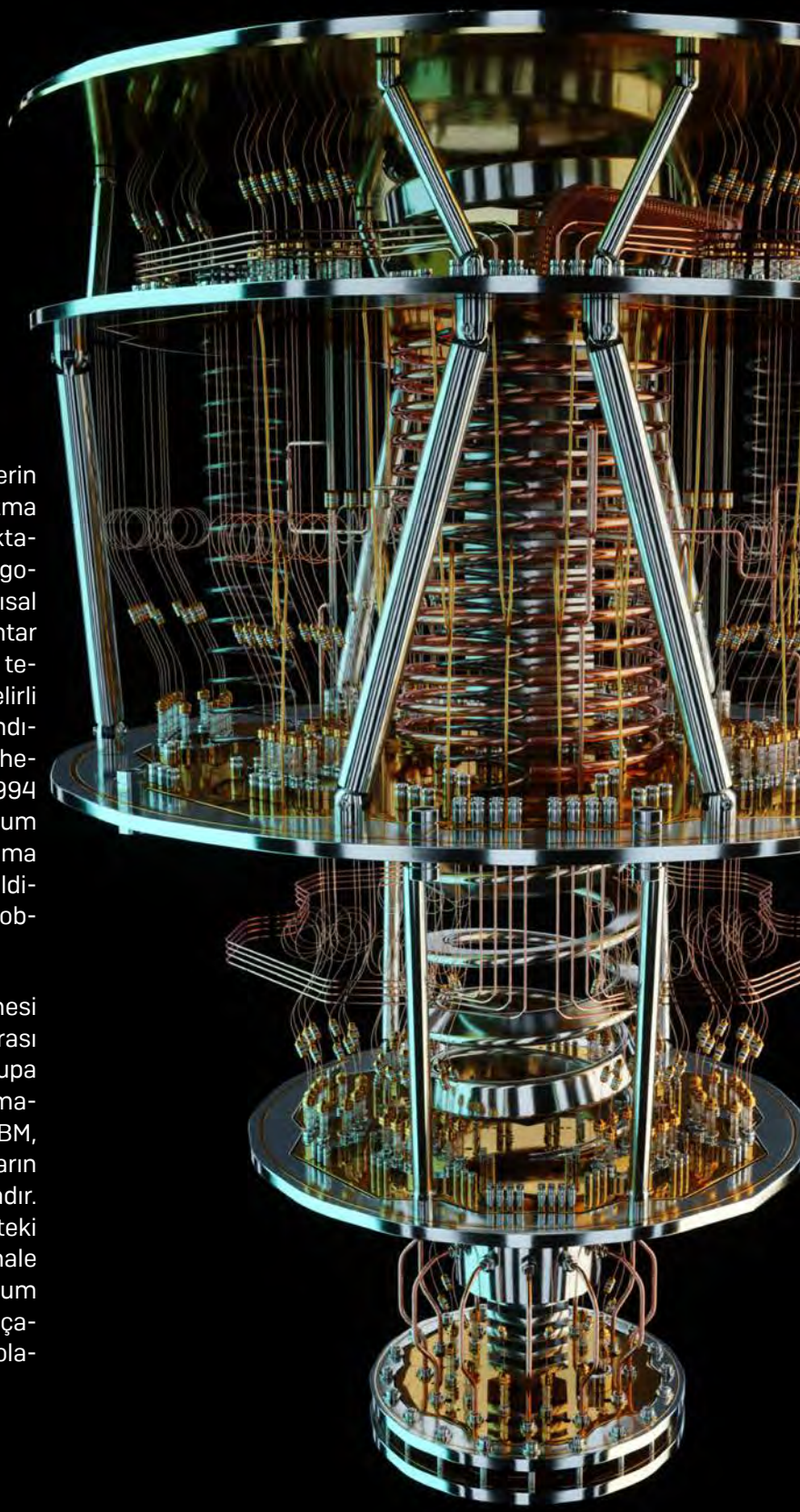
KUANTUM SONRASI KRİPTOGRAFİ

Erkan USLU, Dr. Murat Burhan İLTER, Dr. Neşe KOÇAK

Kuantum sonrası kriptografi nedir, neden ortaya çıkmıştır?

Günümüzde kullanılan asimetrik kriptosistemlerin güvenliği çarpanlara ayırma veya ayrık logaritma gibi matematiksel zor problemlere dayanmaktadır. Örneğin, RSA (Rivest-Shamir-Adleman) algoritması çarpanlara ayırma problemi, DSA sayısal imzalama algoritması ve Diffie-Hellman anahtar paylaşım algoritması ayrık logaritma problemi temel alınarak geliştirilmiştir. Bu problemler, belirli parametreler seçildiğinde, günümüzde kullandığımız bilgisayar sistemlerinin sahip olduğu hesaplama gücüyle çözülememektedir. Fakat, 1994 yılında Peter Shor tarafından önerilen kuantum algoritma (Shor Algoritması) ile yeterli hesaplama gücüne sahip kuantum bilgisayarlar geliştirildiğinde, çarpanlara ayırma ve ayrık logaritma problemleri çözülebilir hale gelmektedir.

Dünyada kuantum bilgisayarların geliştirilmesi ve kullanılabilir hale getirilmesi için uluslararası büyük bir yarış bulunmaktadır. Özellikle Avrupa ülkeleri, Amerika veya Çin gibi ülkeler bu çalışmalara büyük yatırımlar yapmaktadır. Bu alanda IBM, Google ve Microsoft gibi teknoloji devi firmaların geliştirmeleri ve Ar-ge projeleri bulunmaktadır. Yapılan çalışmalar, kriptosistemlerin gelecekteki kuantum hesaplama tehdidine karşı güvenli hale getirilmesi ihtiyacını ortaya çıkarmıştır. Kuantum hesaplama tehdidine karşı yapılan kriptografik çalışmaların tümü kuantum sonrası kriptografi olarak adlandırılmaktadır.



Aşağıdaki tabloda günümüzde kullanılan bazı kriptosistemlerin anahtar uzunlukları, bu anahtar uzunluklarına bağlı klasik ve kuantum hesaplamaya karşı varsayılan güvenlik seviyeleri bulunmaktadır.

ALGORİTMA	ANAHTAR UZUNLUĞU	GÜVENLİK	
		KLASİK	KUANTUM
RSA-1024	1024 bit	80 bit	0 bit
RSA-2048	2048 bit	112 bit	0 bit
ECDSA-256	258 bit	128 bit	0 bit
ECDSA-384	384 bit	192 bit	0 bit
AES-128	128 bit	128 bit	64 bit
AES-256	256 bit	256 bit	128 bit

Tablo 1: Kriptografik Algoritmaların Güvenlik Karşılaştırmaları

NIST Kuantum Sonrası Kriptografi Standardizasyon Süreci

Kuantum teknolojilerinin hızlı bir şekilde gelişmesi sebebiyle kuantum hesaplamaya dayanıklı asimetrik kriptosistemlerin de bir an önce ortaya çıkması ihtiyacı doğurmuştur. Bu ihtiyacı karşılamak için National Institute of Standards And Technology (NIST), 2016 yılında kuantum hesaplamaya dayanıklı algoritma belirleme sürecini başlatmıştır. Bu süreç kapsamında dünyada farklı akademik ve sektörel kurumlarda çalışan araştırmacılardan kuantum hesaplamaya dayanıklı zor problemlere dayanan anahtar paylaşım veya dijital imza algoritmaları tasarlayarak sürece dahil olmaları beklenmiştir. Ayıca NIST tarafından bu algoritmaların kuantum hesaplamaya bağlı saldırılarla birlikte klasik hesaplamaya bağlı saldırılara karşı da güvenli olması, verimli çalışması ve gerçekleme karakteristiklerinin kolay olması beklenmiştir. Çağrı sonrası 69 aday algoritma belirlenerek süreç başlamıştır. Bu sürece dahil olan algoritmalar;

- Kafes tabanlı,
- Kod tabanlı,
- İzojen tabanlı,
- Çok değişkenli,
- Özet fonksiyon tabanlı matematiksel problemlere dayanmaktadır.

Yaklaşık 6 yıl süren bu süreç 2022 yılı Temmuz ayında tamamlanmıştır. Süreç sonucunda standart anahtar paylaşım algoritması olarak kafes tabanlı CRYSTALS-Kyber algoritması, standart imzalama algoritması olarak da kafes tabanlı CRYSTALS-Dilithium, FALCON, özet fonksiyon tabanlı SPHINCS+ algoritmaları seçilmiştir.

Çarpanlara ayırma ve ayrık logaritma problemlerine dayanan algoritmalar çalışma performansları veya parametre boyları bakımından genellikle kuantum hesaplamaya dayanıklı algoritmalardan daha verimlidir. Bu sebeple kuantum hesaplamaya dayanıklı algoritmaların güncel sistemlere entegrasyonu bazı zorlukları da beraberinde getirmektedir. Bu sebeple NIST güvenlik varsayımlarıyla beraber standart olarak belirlediği algoritmaların verimlilik veya kolay gerçeklenebilirliğini de dikkate almıştır. Fakat algoritmaların birbirlerine karşı farklı avantajları olduğundan NIST çeşitlilik sağlanması açısından birden fazla algoritmayı standart haline getirmiştir. Örneğin, SPHINCS+ algoritması güvenlik ispatları bakımından CRYSTALS-Dilithium ve FALCON'dan daha olgundur. Fakat imza boyunun büyük olması veya çalışma hızının düşük olması gibi sebeplerden diğer iki algoritmadan geri kalmaktadır. Bu çeşitlilik sayesinde güvenli bir haberleşme protokolüne uygun algoritma seçimi yapılabilmekte, kullanıcılara çeşitlilik sağlanabilmektedir.

NIST Sürecindeki Anahtar Paylaşım Algoritmaları

NIST'in standart belirleme sürecinde CRYSTALS-KYBER algoritması standart olarak seçilmiştir. Algoritma kafes tabanlı hatalarla öğrenme problemine dayanmaktadır. Ayrıca NIST, kod tabanlı HQC, Classic McEliece, BIKE algoritmaları ile izojeni tabanlı SIKE algoritmasının daha fazla analiz edilmesi için süreci devam ettirmiştir. Böylelikle NIST farklı problemlere dayanan bir anahtar paylaşım algoritmasını daha standart haline getirmeyi amaçlamıştır. Süreç kod tabanlı bu algoritmalar için devam ederken, SIKE algoritması uygulanan kriptanaliz nedeniyle güvensiz hale gelerek süreçten elenmiştir.

KAFES TABANLI	CRYSTALS-KYBER	Parametre boyutları küçüktür.
		Performansı en iyi anahtar paylaşım algoritmasıdır.
		Güvenlik varsayımlarının daha fazla incelenmesi gerekmektedir.
KOD TABANLI	CLASSİC MCELİECE	Açık anahtar boyutu çok büyük, şifreli metin boyutu çok küçüktür.
		Performansı düşüktür.
		Güvenlik varsayımları kuvvetlidir.
	BIKE	Açık anahtar boyutu ortalama, şifreli metin boyutu büyüktür.
		Performansı düşüktür.
		Güvenlik varsayımlarının daha fazla incelenmesi gerekmektedir.
	HQC	Parametreleri büyüktür.
		Performansı düşüktür.
		Güvenlik varsayımları kuvvetlidir.

Tablo 2: Kuantum Sonrası Anahtar Paylaşım Algoritmalarının Özellikleri

NIST Sürecindeki İmzalama Algoritmaları

NIST'in standart belirleme süreci sonucunda CRYSTALS-Dilithium, FALCON ve SPHINCS+ sayısal imzalama algoritmaları standart olarak belirlenmiştir. Bu algoritmaların birbirlerine göre performans, açık/gizli anahtar boyutları ve imza boyutları açısından avantaj ve dezavantajları Tablo 3'te verilmiştir.

KAFES TABANLI	CRYSTALS- DİLİTHİUM	Performansı yüksektir.
		Açık anahtar ve imza boyutu küçüktür.
ÖZET TABANLI	FALCON	Anahtar üretim hızı düşük, imzalama ve doğrulama hızı yüksektir.
		Açık anahtar ve imza boyutu küçüktür.
	SPHINCS+	İmzalama ve imza doğrulama performansı düşüktür.
		Açık anahtar boyutu küçük, imza boyutu büyüktür.

Tablo 3: Kuantum Sonrası İmzalama Algoritmalarının Özellikleri

NIST'in standart belirleme sürecinde standart imza algoritmaları belirlenmiş ve diğer algoritmalar süreçten elenmiştir. Fakat bu süreçten sonra Ağustos 2022'de NIST tarafından yeni bir standart belirleme süreci duyurulmuştur. Bu süreçte asıl amaç ilk süreçteki imza algoritmalarına göre daha küçük imza boyutuna sahip ve daha hızlı doğrulama yapabilen yeni imzalama algoritmaları tasarlanması ve standart haline getirilmesidir. Ayrıca bu imza algoritmalarının yapısal kafes problemlerinden farklı problemlere dayanan algoritmalar olması beklenmektedir. Bu sayede NIST, imza algoritmaları arasında çeşitlilik sağlamayı, ihtiyaca uygun standart bir imzalama algoritması belirlemeyi amaçlamaktadır.

Temmuz 2023'te sürece 40 algoritma katılmıştır. Bu algoritmalar;

- Kafes tabanlı,
- Kod tabanlı,
- İzojen tabanlı,
- Çok değişkenli polinomlar tabanlı,
- Simetrik kriptosistemler tabanlı,
- Çoklu ortaklaşa hesaplama,
- Diğer matematiksel tabanlı problemler olarak sınıflandırılmıştır.

Süreç kapsamında algoritmaların değerlendirilmesi devam etmektedir. NIST tarafından bu sürecin bir önceki standart belirleme sürecine göre daha hızlı bitirileceği belirtilmiştir.

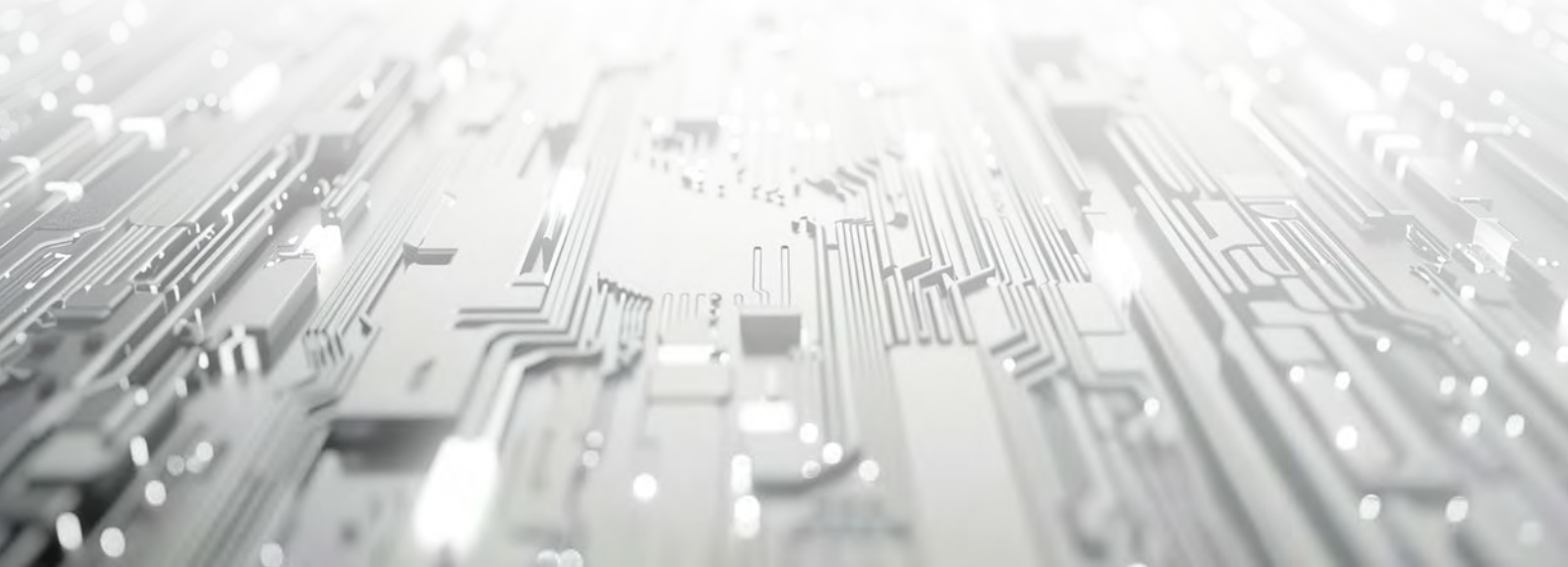
Yapılan Diğer Çalışmalar

NATO, 2019'da kuantum saldırı tehdidini yüksek riskli bir durum olarak belirlemiştir. NATO tarafından Anahtar paylaşımı, gizlilik, kaynak doğrulama ve inkâr edilemezlik gibi kriptografik kavramların, kuantum saldırılara karşı güvenliği sağlamak için gelecek yıllarda çalışmalar yapılması ve sistemlere entegre edilmesi hedeflenmektedir.

Almanya da kuantum sonrası kriptografiye büyük önem veren bir ülkedir. Almanya Federal Bilgi Güvenliği Kurumu (BSI), teknik öneri dokümanlarında kuantum saldırılara dayanıklı özet tabanlı imzalama algoritmalarının kullanımıyla ilgili detaylara yer vermiş ve bu algoritmaların kullanılmasını önermiştir. Ayrıca, kurumun yayınladığı başka bir öneri dokümanında, NIST tarafından standardize edilen 3. Tur alternatif anahtar paylaşım adaylarından FrodoKEM algoritmasının ilgili alanlarda kullanılması önerilmiştir.

Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), 2015'ten beri kuantum saldırılarına karşı güvenli uygulama alanlarını temel alan çalışma grupları düzenlemekte ve kuantum sonrası kriptografi konusunda çalıştaylar organize etmektedir.

Amerikan Ulusal Standartlar Enstitüsü (ANSI), Elektrik ve Elektronik Mühendisliği Enstitüsü (IEEE), İnternet Mühendisliği Görev Gücü (IETF), Uluslararası Standartlar Organizasyonu (ISO) gibi uluslararası kurumlar da kuantum sonrası kriptografi konusunda çalıştaylar düzenlemekte, çalışma grupları organize etmekte ve öneri dokümanları yayınlamaktadır.



TAKTİK SAHADA KRİPTOLU HABERLEŞME

Müge ERTEKİN, Oğuzhan ORAL, Berkin AKSOY, Bekir Buğra CÖMERT

Taktik Sahada Haberleşme

Taktik saha askeri operasyonların gerçekleştiği, stratejik öneme sahip saldırı ve savunma amaçlı kullanılan alanlardır. Askeri birliklerin koordinasyonu ile beraber taktik sahada hızlı, güvenli ve güvenilir haberleşme önem taşımaktadır. Taktik sahada haberleşme birlikler arası koordinasyonu sağlamak, durum bilgilerini paylaşmak ve hedeflere ulaşmak için kullanılmaktadır. Güvenli bir haberleşme ağı ile stratejik hedeflere ulaşılır ve operasyonlar başarıyla tamamlanır.

Taktik saha haberleşme ağında kriptolu haberleşme teknolojileri önemli rol oynamaktadır. Kriptolu haberleşmeyle askeri birlikler arasındaki bilgiler güvenli bir şekilde iletilmektedir ve kritik bilgilerin açığa çıkması engellenmektedir.

Taktik Sahada Güvenlik

Günümüzde bilgi teknolojilerinin yaygın olarak benimsenmesi siber saldırıların gerçekleşme sıklığını arttırmıştır. Siber saldırılar tüm haberleşme sistemleri için tehdit oluşturmaktadır. Taktik sahada kullanılan askeri haberleşme sistemleri de bu saldırıların hedefi haline gelmektedir.

Taktik sahadaki güvenli haberleşme, askeri operasyonların başarısı için kritik öneme sahiptir. Askeri birimler önemli görev ve operasyonlarını ancak güvenli haberleşme sayesinde başarıyla gerçekleştirebilirler. Taktik sahanının değişkenliği ve düşman tehditlerine karşı açıklığı göz önünde bulundurulduğunda doğru zamanda doğru bilgiye erişim askeri birimler açısından kritik önem taşımaktadır. Güvenli haberleşme sayesinde dinleme, bilgiyi manipüle etme, sinyal engelleme, aldatma gibi saldırılara karşı koruma sağlanmaktadır. Güvenli bir haberleşme sistemi ağda iletilen bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini garanti etmelidir.

Gizlilik, bilginin yetkisiz kişiler tarafından ele geçirilmesine karşı korunması,

bütünlük, bilginin yetkisiz kişiler tarafından değiştirilmesine karşı korunması,

erişilebilirlik ise bilginin yetkili kişiler tarafından ihtiyaç duyulduğunda erişiminin ve kullanımının zamanında ve güvenilir olmasının sağlanması olarak tanımlanmaktadır.

Haberleşme sisteminin Gizlilik, Bütünlük ve Erişilebilirlik özeliklerine sahip olması için tasarımı ile güvenli prensibiyle alınacak önlemlerin tasarım aşamasından itibaren uygulanması , geliştirme sürecinin her aşamasında siber güvenlik tehditlerinin belirlenmesi ve risklerin en aza indirilmesi hedeflenmelidir. ASELSAN tarafından geliştirilen taktik saha haberleşme cihazlarında güvenli kriptografik mekanizmalarının kullanımı, milli algoritmaların kullanımı, frekans atlamalı haberleşme desteği, özel tasarlanmış dalga şekillerinin kullanımı, cihazlarda kurcalamaya karşı önlem alınması gibi güvenlik önlemleri kullanılmaktadır. Bu güvenlik önlemleri sayesinde:

- Haberleşme ağına dışarıdan gelebilecek yanıltıcı mesajların sistem tarafından geçerli kabul edilmesi engellenmektedir.
- Haberleşme ağı içerisinde bulunan unsurlar arası gönderilen komut, konum ve hedef gibi kritik bilgilerin dinlenmesi, bilgi içeriklerinin değiştirilmesi, karşı istihbarat üretilmesi ve sistem aleyhinde kullanılması önlenmektedir.
- Haberleşme ağı içerisinde daha önceden yapılmış yayınların kaydedilerek tekrarlanması ile sistemde gerçekleşebilecek yanıltmalara karşı koruma sağlanmaktadır.
- Haberleşme ağına dahil olabilecek cihazlar karşılıklı kimlik doğrulama ve kriptografik kayıtlanma mekanizmalarıyla kontrollü bir şekilde belirlenmektedir.
- Kablosuz haberleşme sistemlerinde frekans atlamalı haberleşme yapılarak düşman unsurları tarafından gerçekleştirilebilecek sinyal karıştırma ve bastırma saldırılarına karşı haberleşme kanalının güvenilirliği sağlanmaktadır.
- Taktik sahada kaybolan ya da düşman tarafından ele geçirilen cihazların haberleşme sistemi genelinde tehdit yaratması kurcalama önlemleri ile engellenmektedir.
- Cihaz donanım ve yazılımlarında alınan TEMPEST önlemleri ile cihazın çalışma süresince yaydığı elektromanyetik radyasyonun, düşman unsurları tarafından analiz edilip kritik verilerin elde edilme riski engellenmektedir.

Kriptolu Ürünler ve ASELSAN Kripto Çözümleri

Taktik Saha Haberleşmesinde Kriptolu Ağ Haberleşme Cihazları

Güncel teknoloji doğrultusunda, taktik sahada kripto ve sistem güvenliği ihtiyaçlarına yönelik ASELSAN bünyesinde milli "GİZLİ" gizlilik seviyesinde onaylı ve kriptolu ağ haberleşme cihazları geliştirilmektedir. OSI modelinin ikinci katmanı olan link seviyesinde LKC (Link Kripto Cihazı) ve OSI modelinin üçüncü katmanı olan ağ seviyesinde IPKC (IP Kripto Cihazı) kullanılarak kriptolama ve kripto çözme işlemleri gerçekleştirilmektedir. ASELSAN kriptolu ağ haberleşme cihazları; sahip oldukları kripto algoritmaları ve mekanizmaları ile kullanıcı verilerini kriptolayarak verilerin dışarıdan izinsiz erişimini engeller, kullanıcı verilerinin bütünlüğünü korur ve iletilen verilerin inkâr edile-

memesini sağlar. Taktik sahada düşman unsurlar tarafından ele geçirilme tehdidine karşı ASELSAN kriptolu ağ haberleşme cihazlarında fiziksel kurcalamaya karşı önlemler bulunmaktadır. Elektromanyetik radyasyonun dışarıya sızmasını ve bu sızıntıların saldırgan tarafından incelenerek kriptografik hassas verilerin ele geçirilmesini engellemeye yönelik ASELSAN kriptolu ağ haberleşme cihazları TEMPEST önlemlerine sahiptir. Taktik saha haberleşmesinde, yüksek güvenlik gereksinimleri ile beraber düşük gecikme süreleri, askeri çevre koşullarına uyum, yüksek hareket kabiliyeti de önem arz etmektedir. ASELSAN kriptolu ağ haberleşme cihazlarının sahip olduğu donanımsal kripto yeteneği ile kriptolama kaynaklı gecikme süreleri milisaniyenin altında kalmaktadır. ASELSAN kriptolu ağ haberleşme cihazları, taktik sahanın askeri standartlarda (MIL-STD) ihtiyaç duyduğu yüksek/düşük sıcaklık, titreşim, nem ve basınç gibi zorlu şartlarda operasyon sahasında kullanıcıya kesintisiz hizmet verilebilmektedir. ASELSAN kriptolu ağ haberleşme cihazları, link seviyesinde ve IP seviyesinde uçtan uca güvenli haberleşebilmektedir. IP kripto cihazları tünel kurma için gerekli yönlendirme ayarları, statik olarak cihaza kullanıcı tarafından girilebilirken, Güvenli Tünel Bulma Protokolü (GTBP) ile dinamik olarak otomatik oluşturulabilmektedir. Bu sayede, taktik sahada tasarsız haberleşme ağlarına dinamik uyum sağlanarak kullanıcıya hareket esnekliği ve kullanım kolaylığı sağlanmaktadır.

GYM (Güvenlik Yönetim Merkezi) aracılığıyla ASELSAN kriptolu ağ haberleşme cihazları uzaktan "GİZLİ" gizlilik seviyesinde yönetilebilmektedir. GYM sayesinde taktik sahada yer alan haberleşme sisteminin izlenebilirliği ve yönetilebilirliği bir merkez tarafından sağlanmaktadır. Uzaktan yönetim ile taktik sahada bulunan kriptolu ağ haberleşme cihazlarına konfigürasyon gönderme ve izleme, anahtar güncelleme ve cihazlardan konfigürasyon getirme, alarm izleme, acil durumlarda devre dışı bırakma gibi işlemler yapılabilmektedir.

Taktik Saha Haberleşmesinde Kablosuz Haberleşme Cihazları

Taktik sahada ihtiyaç duyulan veri linki haberleşmesi ve telsiz haberleşmesi için ASELSAN tarafından kablosuz haberleşme çözümleri sunulmaktadır. Sunulan bu çözümler kapsamında güvenli ve hızlı veri haberleşmesini sağlamak amacıyla kablosuz haberleşme cihazları geliştirmektedir.

ASELSAN kablosuz haberleşme cihazları, haberleşme güvenliğini sağlamak amacıyla kriptografik mekanizmalar kullanarak COMSEC, NETSEC ve TRANSEC yeteneklerine sahiptir. Saldırganlar tarafından haberleşmenin dinlenebilmesi durumunda COMSEC yeteneği ile kritik verinin ele geçirilmesi engellenmektedir. TRANSEC ve NETSEC yeteneği ile ASELSAN kablosuz haber-

leşme cihazları, kriptografik algoritmaları kullanarak haberleşmenin yapıldığı frekans aralığında frekans atlamakta ve güvenli kontrol haberleşmesi gerçekleştirmektedir. Söz konusu yetenekler ile saldırganların dinleme yapmasının önüne geçilmekte, sinyalin bastırılması ve karıştırılması engellenmektedir.

ASELSAN kablosuz haberleşme cihazlarının sahip olduğu diğer bir kriptografik yetenek olan kimlik doğrulama mekanizması sayesinde yetkisiz cihazlarla haberleşme yapılmasının önüne geçilmektedir. Kriptografik imzalama ve bütünlük mekanizmaları kullanılarak alınan mesajların yetkili bir kaynaktan ve bozulmadan iletildiği kontrol edilebilmektedir.

ASELSAN kablosuz haberleşme cihazları; sakladığı kriptografik parametrelerin saldırgan tarafından elde edilmesini engellemek amacıyla kurcalama önlemleriyle donatılmış durumdadır.

Taktik sahada cihazlarının erişime zor alanlarda konuşlandırılma ihtimali de göz önüne alındığında uzaktan yönetim bu cihazlar için kritik öneme sahiptir. ASELSAN kablosuz haberleşme cihazları uzaktan yönetim yazılımları aracılığıyla operasyon merkezlerinden güvenli bir şekilde erişilip yönetilebilmektedir.

ASELSAN kablosuz haberleşme cihazları, taktik sahadaki kullanım konseptlerine göre ilgili MIL-STD standartları doğrultusunda çevre koşulları ve EMI/EMC uyumluluklarına sahiptir.

ASELSAN YÜKSEK HIZLI KRİPTOLAMA YETENEKLERİ

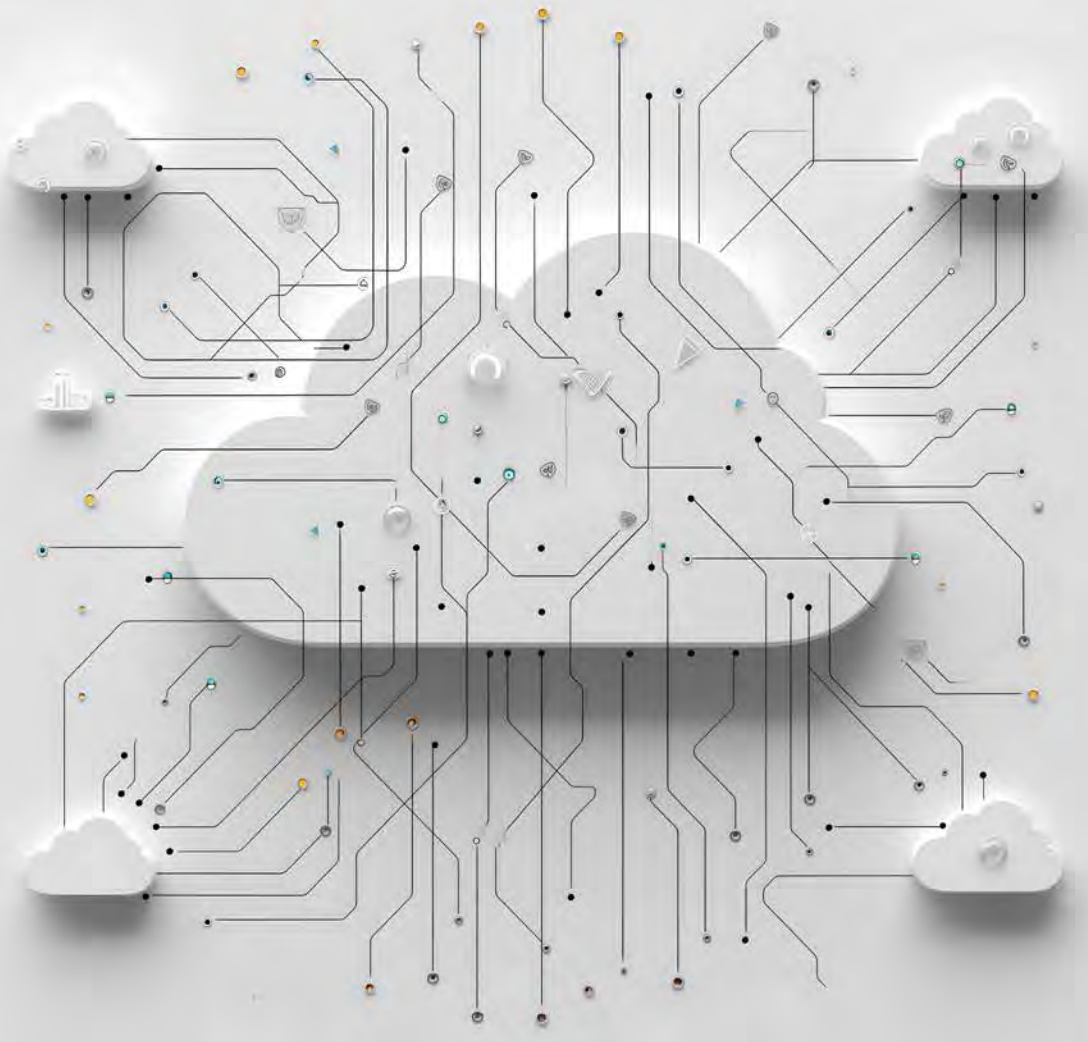
Bekir Buğra CÖMERT, Aybike Hilal BAYRAKTAR

1. Yüksek Hızlı Haberleşme İhtiyacı

Gelişen teknolojiyle beraber; hizmet, sağlık, endüstri, finans ve savunma sanayii gibi sektörlerin ihtiyaçları ve yetenekleri de çağın gerekliliklerine göre kendini güncellemektedir. Üretim bantlarından, tarım arazilerine, haberleşme cihazlarına ve tüketici elektroniğine kadar hayatın hemen her alanındaki ürünlerin; yapay zekâ ve nesnelerin interneti (IoT) gibi güncel teknolojilere sahip olması beklenmektedir. Bu beklentiler sonucu kazanılan yetenekler, veri üretimini de beraberinde arttırmaktadır. 2000'li yılların başında kullanılan cep telefonlarının depolama alanlarının "kilobayt" seviyelerinden güncel olarak "terabayt" seviyelerine çıkması bu durumun en net örneklerinden biridir.

Cep telefonlarının depolama alanlarında olduğu gibi yüksek hızlı haberleşme ihtiyacı da her geçen gün artmaktadır. Güncel mobil haberleşme teknolojisi olan "5G", "Gbps" mertebesinde hızlara ulaşabilmektedir. Bu hızlara erişilebilmesiyle birlikte cihaz tabanlı internet (IoT) teknolojisinin, günlük hayatta kullanılan birçok üründe kullanılabilmesinin önü açılmaktadır. Giyilebilir teknoloji ürünleri, akıllı arabalar, akıllı evler gibi birçok yenilikçi ürünün kullanımının "5G" ile daha işlevsel hale gelmesi beklenmektedir.

Kamu kurumları ve bankalar gibi büyük kuruluşların veri merkezleri ile bulut teknolojisi servisi sağlayan kurumların sunucularının da çok sayıda kullanıcıya hizmet vermesi sebebiyle "Gbps" mertebelerinde haberleşme bu kurumlar için gereklilik haline gelmiştir.



Teknoloji gündeminin merkezinde bulunan yapay zekâ çalışmaları, büyük verilerin işleneceği ve paralelizasyon metodunu gerçekleyebilen büyük veri merkezleri ile ilerleyebilmektedir. Bu veri merkezlerinin çok sayıda yapay zekâ geliştiricisine hizmet verdiği düşünüldüğünde yüksek hızlı haberleşme yapay zekâ geliştirmeleri için de kritik öneme sahiptir.

Yüksek hızlı haberleşme, günlük hayatta ve her sektörde kritik öneme sahip bir ihtiyaç olarak yerini korumakta ve gün geçtikçe daha da önem kazanmaktadır.

2. Yüksek Hızlı Haberleşmede Güvenlik İhtiyacı

Yüksek hızlı haberleşme ihtiyacı ile birlikte birim zamanda aktarılan verinin boyutu her geçen gün artmaktadır. Bu durum birçok kolaylık sağlıyor olsa da beraberinde bazı riskler getirmektedir. Bilgisayar, cep telefonu veya veri merkezi sunucusu gibi cihazlarda bulunan veriler; fiber kablolar, mobil şebekeler veya uydu haberleşmesi gibi araçlarla göndericiden alıcıya transfer edilmektedir. Bu transfer esnasında veri, göndericinin ve alıcının kontrolü dışındaki birçok lokasyondan ve noktadan geçmektedir. Hareket halindeki verinin kontrol edilmesinin imkansıza yakın olması sebebiyle verilerin transfer edilmeden önce kriptografik mekanizmalarla koruma altına alınması ve bu şekilde gönderilmesi kritik önem taşımaktadır.

Yüksek hızlı haberleşme yeteneği olan cihazlar, ilettikleri verinin gizlilik, bütünlük ve erişilebilirlik varlıklarını kriptografik mekanizmalar aracılığıyla koruyabilmektedirler. Mesajı ileten kaynağın güvenilirliği, iletim esnasında mesajın başkaları tarafından elde edilememesi ve göndericiye bozulmadan iletilmesi kriptografik mekanizmaların sağladığı temel hizmetler arasındadır. Bu hizmetler sayesinde bankalar, kamu kurumları, veri merkezleri, bulut teknolojisi sağlayıcıları ve kritik kurumlar yüksek hızlı haberleşme ihtiyaçlarını güvenli hale getirmektedir.

3. ASELSAN Yüksek Hızlı Kriptolama Çözümleri

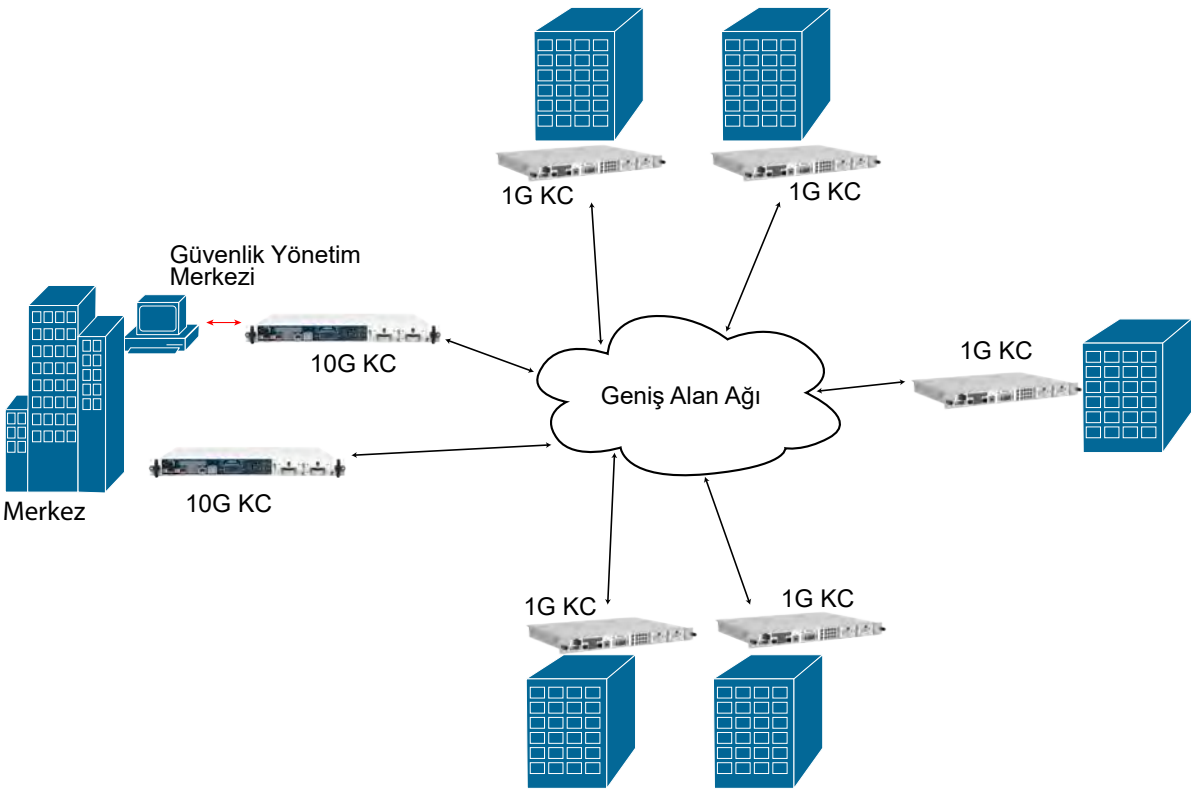
3.1 ASELSAN 2064 ÇETİN 10G Kripto Cihazı

ASELSAN'ın geliştirmiş olduğu 2064 ÇETİN 10G Kripto Cihazı, Katman-2 ve Katman-3 seviyesinde veri şifreleme ve şifre çözme yeteneğine sahiptir. 2064 ÇETİN 10G Kripto Cihazı, Katman-2 seviyesinde Ethernet haberleşmesini ve Katman-3 seviyesinde IP haberleşmesini protokol bağımsız olarak şifreleme ve şifre çözme yeteneğine sahiptir.

10 Gbps hızında olmasının yanı sıra, taktik sahadaki ASELSAN kripto cihazları ile güvenli haberleşme yeteneği yapabilmesi sayesinde 2064 ÇETİN 10G Kripto Cihazı, yüksek hızlı güvenli haberleşme ihtiyacı olan yıldız topolojilerin merkez cihazı olarak ya da üzerinden yoğun veri geçmesi beklenen veri merkezleri arasında kullanılmasına olanak sağlamaktadır. Kritik öneme sahip verilerin güvenli haberleşmesini sağlayan 2064 ÇETİN 10G Kripto Cihazı, veri kesintisi olmaması adına yedekli güç kaynağı ve fan mimarisine sahiptir.

2064 10G Ağ Kripto Cihazı, donanımsal olarak gerçeklenen milli onaylı algoritma ve AES-256 desteğine sahiptir. Anahtarlar, ASELSAN anahtar yükleme cihazı aracılığıyla cihazlara yakından yüklenebilmektedir. Ayrıca güvenlik yönetimi yazılımlarıyla anahtarlar güvenli şekilde ağ üzerinden de dağıtılabilmektedir. Anahtar dağıtımının yanısıra; cihaz alarmlarını izleme, cihaz konfigürasyon ayarlarını değiştirebilme ve cihazın haberleşme kurallarını belirleyen politika tablosunu güncelleyebilme özellikleri de güvenlik yönetim yazılımının yetenekleri arasındadır. Cihazlarda bulunan kritik parametreleri korumak amacıyla kurcalama önlemleri bulunmaktadır. Bu cihazlarda gerçekleşen veri haberleşmesindeki gecikme mikrosaniye mertebesini aşmamaktadır. 2064 ÇETİN 10G KC; jumbo paketler için de yüksek hızlı ve güvenli veri haberleşmesi desteğine sahiptir.

2064 ÇETİN 10G Kripto Cihazı, EMI/EMC için MIL-STD-461F standardına, çevre koşulları için MIL-STD-810G standardına ve TEMPEST önlemleri için SDIP-27A standardına uygun olarak geliştirilmiştir.



Şekil 1: ASELSAN Yüksek Hızlı ve Güvenli Haberleşme Çözümü

3.2 ASELSAN 2064 ÇETİN 1G Kripto Cihazı

ASELSAN 2064 ÇETİN 1G Kripto Cihazı, 2064 ÇETİN 10G Kripto Cihazı ve 2064 Mini IPKC ile 1Gbps hızında güvenli haberleşme yeteneğine sahiptir. ASELSAN 2064 ÇETİN 1G KC, 1Gbps hızında güvenli haberleşme ihtiyacı bulunan sistemlerde merkez cihazı olarak ya da merkezinde ASELSAN 2064 ÇETİN 10G KC bulunan sistemlerde uç birim cihazı olarak hizmet verebilmektedir.

ASELSAN 2064 ÇETİN 1G KC, ASELSAN 2064 ÇETİN 10G KC ile veri iletim hızı farklılığı haricinde aynı güvenlik önlemlerine, işlevselliğe ve standartlara sahiptir.

3.3 ASELSAN Yüksek Hızlı Haberleşme Cihazları Yol Haritası

Kuantum bilgisayarlarının önümüzdeki yıllarda işlevsel hale gelmesi beklenmektedir. Bu gelişmeyle birlikte güncel olarak kullanılan klasik asimetrik kriptografik mekanizmaların ileride geçerliliğini kaybetmesi beklenmektedir. 2064 10G Ağ Kripto Cihazı, kriptografik güvenliğin kuantum sonrası dönemde de sağlanması için ölçekli mimariye sahiptir. 2064 10G Ağ Kripto Cihazının kuantum sonrası döneme hazır olması için yapılan geliştirmelere devam edilmektedir.

Yüksek hızlı veri haberleşmesinin doğal gereği olarak, 40 Gbps ve 100 Gbps hızlarında kuantum sonrası döneme dayanıklı cihazların geliştirilmesi için de çalışmalara başlanmıştır.

KRİPTO YÖNETİMİ

Kutan FEYİZ, Sevgi Babacan ÇETİN, Dr. Neşe KOÇAK, Dr. Murat Burhan İLTER, Yeliz ERKEK, Aybike Hilal BAYRAKTAR

1. Anahtar Yönetimi

1.1. Tanım ve Önemi:

Anahtar yönetimi, kriptografi alanında kullanılan anahtarların rastgele bir şekilde üretilmesi, güvenli bir şekilde saklanması, dağıtılması, yenilenmesi, güncellenmesi ve güvenli bir şekilde yönetilmesini içeren kritik bir süreçtir. Bu süreç, siber güvenlik ve kripto güvenliği açısından son derece önemlidir; çünkü doğru bir anahtar yönetimi olmadan, haberleşmede kullanılan şifrelenmiş verilerin güvenliği tehlikeye girebilir. Modern kriptografinin temel prensiplerinden birisi olarak kabul edilen ve Kerckhoffs ilkesi olarak adlandırılan, 19. yüzyılda Auguste Kerckhoffs tarafından, bir kriptografik sistemin güvenliğinin, algoritmanın gizliliğine değil, anahtarın gizliliğine dayandırılması gerektiği ilkesi, anahtar yönetiminin ne kadar kritik olduğunu gösterir niteliktedir. Yetkisiz kişilerin eline geçen bir anahtar, hassas verilerin çalınması veya değiştirilmesi gibi ciddi güvenlik sorunlarına yol açabilir. Bu nedenle, kurumlar için doğru ve güvenilir anahtar yönetimi sistemleri, protokolleri ve stratejileri belirlemek ve uygulamak, hassas verilerini korumak ve güvenli bir haberleşme ortamı sağlamak için kritik bir öneme sahiptir. Bu anlamda, ASELSAN bünyesinde geliştirilen kriptografik cihazlara ait anahtar ve sertifika gibi kritik parametreler, ASELSAN Kripto Yönetim Merkezi'nde rassal olarak üretilmekte, üretilen bu kritik parametreler, veritabanlarında güvenli bir şekilde saklanmakta, ASELSAN ürünü olan anahtar taşıma cihazları ve farklı yetkilerde erişim denetimi modülleri ile manuel olarak veya ASELSAN Güvenlik Yönetim Merkezi aracılığıyla dağıtılmaktadır.

1.2 Anahtarların Üretimi, Güvenli Saklanması, Dağıtımı, Yenilenmesi ve Güncellenmesi:

Bir kriptosistemin güvenli olabilmesi için saklanması gereken parametreler kritik parametre olarak adlandırılmaktadır. Kriptografik anahtar, bu parametrelerden birisidir. Anahtarların ortaya çıkması durumunda kriptosistem tamamen güvensiz hale gelmektedir. Bu sebeple anahtarın gizli tutulması yüksek derecede önem arz etmektedir.

Anahtar güvenliğinde bir başka önemli konu, anahtarların rassal bir şekilde üretilmesidir. Bu amaçla kriptografide rassal sayı üreteçleri kullanılmaktadır. Bu üreteçler gerçek rassal sayı üreteçleri ve sözde rassal sayı üreteçleri olarak iki temel sınıfa ayrılmaktadır. Gerçek rassal sayı üreteçleri, deterministik olmayan fiziksel bir olaya dayalı çeşitli ölçümler yaparak rassal sayı dizileri üretirler. Bu fiziksel olaylara örnek olarak, radyoaktif ışıma, elektronun hareketleri, termal değişimler gibi örnekler verilebilir. Temel olarak bir rassal sayı üreteci, entropi kaynağı ve deterministik matematiksel bileşenlerinden oluşmaktadır.

Rassal sayı üreteçlerinin değerlendirilmesi için farklı bileşenlere farklı test ve değerlendirme yöntemleri uygulanmaktadır. Rassal sayı üreteçlerinin çıktıları istatistiksel testler ile değerlendirilmektedir. Bunun yanı sıra gürültü (entropi) işleme fonksiyonları da rassal anahtar üretiminde kullanılabilmektedir. Entropi havuzunda mevcut olan veriler entropi tahmin testleri ile test edilerek kaynağın fiziksel bileşenlerine dair değerlendirme yapılması mümkündür. Sağlık testleri ise kaynağın işleyişi sırasında oluşabilecek hataları veya problemleri gözlemlemek amacıyla uygulanmaktadır. Bu kapsamda üreteçlerin test ve değerlendirilmesi amacıyla Ulusal Standartlar ve Teknoloji Enstitüsü'nün (NIST) yayınladığı standartlar kullanılmaktadır.

Kullanıcıların kriptolu olarak haberleşebilmesi için kullanılacak anahtarların haberleşme öncesinde paylaşılması gerekmektedir. Anahtar dağıtım yöntemlerinden birisi anahtarın güvenli bir kanal üzerinden karşı tarafa gönderilmesidir. Anahtarların güvensiz bir kanal üzerinden paylaşılması için asimetrik kripto algoritmalarına ihtiyaç duyulmaktadır. Diffie-Hellman Anahtar değişim protokolü gibi bu amaçla tasarlanan protokoller, günümüzde internet iletişiminde kullanılan IPSEC ve TLS gibi protokollerin içerisinde yer almaktadır.

ASELSAN ürünlerinde, sistemlerin ihityaçlarına ve kullanım senaryolarına göre hem kriptografik anahtar değişim protokolleri hem de Önceden Paylaşılmış Anahtarlar ile anahtar dağıtımı yapılabilmektedir.

Siber Güvenlik'e dair önemli problemlerden birisi de kritik parametrelerin saklanması ve korunmasıdır. Kritik parametrelerin yetkisiz kişilerin eline geçmesi istenmediğinden bu konu öne çıkmaktadır. Kritik parametrelerin saklanması ve korunması amacıyla kullanılan en önemli araçlardan birisi olarak HSM (Hardware Security Module) cihazları gösterilebilir. HSM, donanımsal kriptolama yetenekleri olan bir cihazdır. Kriptolama işlemleri için kullanacağı kritik parametreleri kendi içinde üretir ve kendi içinde saklar, dışarıya çıktı olarak vermez. Ayrıca, üzerinde bulunan kurcalama önlemleri sayesinde bu kritik parametrelerin zorla alınmaya çalışılması durumunda bilgileri silerek saldırganların eline geçmesini engeller. Bu cihaz genellikle bir veritabanı ile birlikte kullanılır. Veritabanı, bu cihaz tarafından kriptolu bir şekilde tutulur. Bu şekilde, hem veritabanındaki kritik bilgilerin güvenli saklanması hem de sadece HSM'i kullanmaya yetkili kişilerin veritabanındaki kritik bilgilere erişimine izin verilmesi sağlanmış olur.

Kripto cihazlarına ve kriptolu telsizlere yüklenen anahtarların cihaz üzerinde saklanması, işlenmesi ve kullanılması sırasında, Haberleşme Güvenliği (Communication SECurity (COMSEC)) kriterlerine uyulması gerekmektedir. Bu sayede anahtarların her aşamada gizliliğinin ve bütünlüğünün sağlanması hedeflenmektedir.

Anahtar yenileme ve güncelleme, kriptografi alanında kullanılan anahtarların güvenliğini ve daha etkin olmalarını sağlamak amacıyla önem arz eder. Anahtarlar, belirli bir süre sonra güvenliklerini yitirebilir hale gelebilir. Bu nedenle, anahtarların periyodik olarak yenilenmesi ve güncellenmesi gerekmektedir. Anahtarların yenilenmesi ve güncellenmesinden kasıt anahtarların yeniden üretilmesidir. Anahtarların düzenli olarak belirli zamanlarda yeniden üretilmesi, potansiyel güvenlik açıklarını en aza indirerek ilgili sistemlerin ve haberleşmenin güvenliğini sağlamaya yardımcı olur. Bu süreç, genellikle bir anahtar yönetim politikasına ve prosedürüne dayanır ve belirli zamanlarda düzenli olarak veya belirli bir olay gerçekleştiğinde (örneğin, bir güvenlik ihlali tespiti) gerçekleştirilir. Anahtarların, yenilenmesi ve güncellenmesi ile eski anahtarların geçerliliği sonlanır. Bu sayede, sistemlerin sürekli olarak güncel ve güvenli kalmaları sağlanırken, verilerin bütünlüğü ve gizliliği de korunmuş olur.

2. Uzaktan Yönetim:

2.1. Uzaktan Erişim Güvenliği:

Uzaktan yönetim, kriptografik cihazların güvenli bir şekilde uzaktan yönetilebilmesine ve izlenebilmesine imkan tanır. Kriptografik cihazların bulunduğu bir sistemde uzaktan erişim ile kriptografik cihazların yönetim faaliyeti gerçekleştirilebilir. Uzaktan anahtar yüklenebilir, cihazın oluşturduğu alarmlar izlenebilir, cihaz durumları görüntülenebilir, konfigürasyon ayarı yapılabilir ve güvenli yazılım güncelleme işlemi gerçekleştirilebilir. Tehdit oluşturduğu düşünülen durumlarda cihaza yasaklama listeleri gönderilebilir veya uzaktan acil silme işlemi gerçekleştirilebilir. Uzaktan yönetim araçlarının kabiliyetleri göz önünde bulundurulduğunda güvensiz uzaktan yönetim sistemlerinde, yetkisiz kullanıcıların cihazlara erişmesi ve veri iletişimini kesintiye uğratması ya da verilerin yetkisiz kullanıcıların eline geçmesine sebep olması olasıdır. Güvenli uzaktan yönetim sistemleri oluşturmak, cihazlar yönetilirken ve izlenirken uzaktan yönetim yazılımının güvenliğini sağlamak önemlidir. Bu bağlamda güçlü şifreleme mekanizmaları, kaynak doğrulama, inkar edememezlik ve yetki seviyelerine göre ayrılmış kullanım konseptleri kullanılmaldır. Uzak yönetim ile güvenli bir şekilde yetkisiz erişimin önlenebilmesi ve verinin bütünlüğün kontrolü için sayısal imzalar kullanılabilir. Yönetilen cihazların uzaktan yönetim sistemiyle kimlik doğrulama mekanizmasının işletilmesi, cihazların tarih saatlerinin güncel tutulması güvenliği sağlamaya yönelik adımlardandır.

2.2. Uzaktan Erişim Yönetimi Araçları, Cihaz Güncellemeleri, Güvenlik Politikaları ve İzleme:

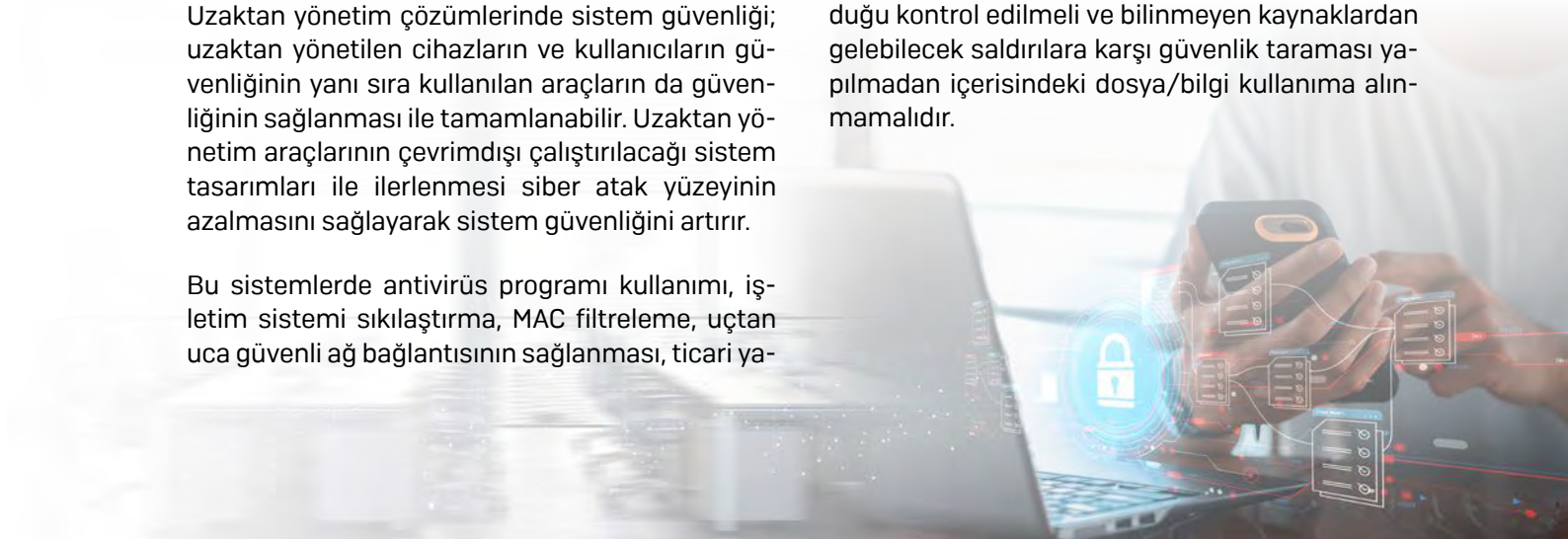
Uzaktan yönetim çözümlerinde sistem güvenliği; uzaktan yönetilen cihazların ve kullanıcıların güvenliğinin yanı sıra kullanılan araçların da güvenliğinin sağlanması ile tamamlanabilir. Uzaktan yönetim araçlarının çevrimdışı çalıştırılacağı sistem tasarımları ile ilerlenmesi siber atak yüzeyinin azalmasını sağlayarak sistem güvenliğini artırır.

Bu sistemlerde antivirüs programı kullanımı, işletim sistemi sıkılaştırma, MAC filtreleme, uçtan uca güvenli ağ bağlantısının sağlanması, ticari yazılımlar için gerekli güncellemelerin takip edilmesi ve zamanında yapılması önemli hale gelmektedir.

Uzaktan yönetim konseptinin doğası gereği sahip olduğu dinamik yapı, yüksek seviyede erişim kontrolünü zorunlu kılmaktadır. Uzaktan yönetim araçlarına erişimin rol tabanlı yapılması ve çok-faktörlü kimlik doğrulama içermesi bu platformların yetkisiz kullanımını kısıtlayarak güvenliği arttırmaktadır. Buna ek olarak, yapılan tüm işlemlerin kayıt altına alınması ve izlenmesi sayesinde yetkisiz kullanıcılar ve ağa yönelik sistematik saldırılar tespit edilebilmektedir. Ağ güvenliğinin sağlanması ve ağın izlenmesi uzaktan yönetim araçlarının güvenli yönetimi için önemli ölçütler olsalar da bu araçları kontrol eden kişilerden kaynaklanabilecek iç tehditlere yönelik önlemler de her zaman göz önünde bulundurulmalıdır. Uzaktan yönetim araçlarının güvenliğini sağlamaktan sorumlu personele belirli aralıklarla eğitim verilmesi ve böylece personelin siber güvenlik tehditlerine yönelik farkındalığının ve bilgisinin arttırılması insan kaynaklı tehditleri azaltma anlamında kritik öneme sahiptir.

2.3. Uzaktan Cihaz Güncellemeleri, Güvenlik Politikaları ve İzleme:

Yazılım ve firmware güncellenmesi ihtiyacı müşteri kullanımındaki cihazlar için önemli olmakla birlikte uzaktan yönetim yeteneği bulunan sistemlerde uzaktan güncellemeyi de içerdiği için daha karmaşık hale gelmektedir. Uzaktan yönetilen cihazlar için gerekli güncellemeler şifreli ve/veya sayısal imzalı gerçekleştirilebilir. İlgili güncellemenin bir donanım yardımıyla yapılabilmesi durumunda uzaktan yönetim cihazına bağlanacak donanımın (bilgisayar, USB bellek, vb.) güvenli olduğu kontrol edilmeli ve bilinmeyen kaynaklardan gelebilecek saldırılara karşı güvenlik taraması yapılmadan içerisindeki dosya/bilgi kullanıma alınmamalıdır.



YAN KANAL ANALİZİ

Berkin AKSOY, Kutan FEYİZ

Yan Kanal Analizi (YKA), bir sistem veya cihazın güvenliğini tehdit edebilecek yan kanal saldırılarını belirlemek ve önlemek için yapılan bir tür güvenlik analizidir. Cihazın fiziksel özellikleri veya elektriksel davranışı incelenerek Yan Kanal Analizi gerçekleştirilir. Yan kanal verisi, kriptografik algoritmaların gerçeklendiği donanımların istemli veya istemsiz ürettiği ve sistemin güvenliğini tehdit ettiği bilgileri ifade eder. Kriptografik anahtarlar ve cihaz güvenliği için kritik hassas bilgiler, cihaz çalışma sürecinde yan kanallardan sızabilir ve bu da sistemin güvenliğini riske atabilir. Yan kanal saldırıları ile bir cihazın güç tüketimi, zamana bağlı davranışı veya elektromanyetik radyasyonu analiz edilerek cihazın sahip olduğu kriptografik anahtarlar veya kritik bilgiler elde edilebilmektedir.

Yan Kanal Analizi; başlıca Güç analizi, Zamanlama analizi, Elektromanyetik analiz ve Akustik analiz yöntemleri kullanılarak gerçekleştirilmektedir. Cihazın kriptolama işlemi sırasında güç tüketimi, kullanılan algoritma anahtarına veya veriye göre değişebilmektedir. Cihazın güç tüketimi ile kriptografik işlem adımları arasındaki ilişki incelenerek yapılan analizler güç analizi olarak sınıflandırılmaktadır. Zamanlama analizinde bir kriptografik işlem sırasında kullanılan algoritmaların ve anahtarların işlenme süreleri baz alınarak, elektromanyetik analizde de cihazın çalışma sürecinde yaydığı elektromanyetik radyasyon incelenerek kriptografik anahtarlar veya cihaz için kritik bilgiler elde edilebilmektedir. Cihazın yaydığı ses dalgalarının frekansı, şiddeti, zamanlaması vb. gibi diğer özellikleri incelenerek de akustik analiz yapılabilmektedir.

Kriptografik işlemlerde rastgele zamanlama kullanılarak, kriptografik işlemlerin süreleri sabit tutularak, anahtarlar ve kritik bilgiler üzerinde maskeleme işlemleri yapılarak saldırganların zamanlama analizi yapması zorlaştırılabilir. Elektromanyetik radyasyonu azaltmak için cihaz tasarımında ekranlama ve filtreleme kullanılması, elektromanyetik radyasyonu karıştırmak için rastgele gürültü eklenmesi veya daha az elektroman-

yetik yayılım için düşük güç tüketimi hedeflenmesi elektromanyetik analiz ile kritik bilgi elde edilmesinin önüne geçebilir. Güç tüketimini düzenlemek için filtreleme yapmak veya gürültü eklemek, güç tüketimini gizlemek için işlemler arasına rastgele gecikmeler eklemek, güç tüketimini sabitlemek için kontrollü akım kaynakları kullanmak güç analizine karşı alınabilecek önlemler arasındadır. Akustik analize karşı ise hassas bilgilerin işlendiği ortamlara ses izolasyonu yapılarak veya beyaz gürültü eklenerek önlem alınabilmektedir. Bu önlemlere ek olarak, saldırgan tarafından cihazın ele geçirilmesi tehdidine karşı kurcalamaya yönelik fiziksel önlemler de yer almaktadır. Bu önlemler sayesinde olası bir yan kanal saldırısı anında analiz yapılmasının önüne geçilmektedir.

Geleneksel Yan Kanal Analizi yöntemleri, genellikle elde edilen verilerin analizine dayanmaktadır. Bu verilerin işlenmesi ve anlamlandırılması geleneksel yöntemler ile zaman alıcı olabilmektedir. Yapay zeka destekli yöntemler, verileri işleme ve anlamlandırma süreçlerini hızlandırması ve daha kesin sonuç sağlaması açısından ek bir Yan Kanal Analiz yöntemi olarak kullanılabilmektedir. Yapay zeka algoritmaları, veri anlamlandırma aşamasında veri kümelerinin analiz edilmesi ve verilerin arasındaki gizli karmaşık ilişkilerin belirlenmesini geleneksel yöntemlere nazaran daha kolaylaştırmaktadır. Yan Kanal Analizi için ilgili veriler, fiziksel ölçümler veya sensörler aracılığıyla elde edilir ve bir veri seti oluşturulur. İlk aşamada, verileri işleme amacıyla veri setinin boyutunun büyüklüğüne göre boyut indirgeme vb. gibi teknikler için ve sonrasında da birtakım özniteliklerin çıkartılması için seçilen bir yapay zeka algoritması kullanılabilmektedir. Veriler işlendikten sonra elde edilen bu özniteliklerin anlamlandırılması aşamasına geçilebilir. İlgili bir yapay zeka modeli, problemin karmaşıklığı da göz önünde bulundurularak seçilebilmekte ve eğitilebilmektedir. Sonrasında, eğitilen bu model ile Yan Kanal Analizi yapılabilmektedir. Yapay zeka ile yapılan analizlere karşı geleneksel yöntemler için alınan önlemlerin alınabileceği gibi, yapay zeka tabanlı karşı önlemler de geliştirilebilmektedir. Örneğin, analiz zorlaştırmaya yönelik yanıltıcı verilerin üretimi veya verilere gürültü eklenmesi yapay zeka desteği ile sağlanabilmektedir.

ÖZEL SİSTEMLERDE SİBER GÜVENLİK

SYSTEM

TAKTİK SAHA SİBER GÜVENLİK PAKETLERİ: ASKERİ OPERASYONLARIN DİJİTAL KALKANI

Dr. Murat DEMİRCİOĞLU

Taktik Saha Nedir ve Önemi Nedir?

Taktik saha, askeri operasyonların aktif olarak gerçekleştirildiği, hareketli ve dinamik alanları ifade eder. Bu alanlarda askeri birliklerin operasyonel görevlerini yerine getirirken hızlı ve güvenilir iletişim, veri paylaşımı ve koordinasyon sağlayabilmeleri büyük önem taşır. Taktik saha operasyonlarında, birliklerin başarıya ulaşması için teknolojik altyapının güvenliği kritik bir öneme sahiptir. Bu bağlamda, siber güvenlik, askeri bilgilerin ve iletişimin korunması açısından vazgeçilmezdir.

Taktik Saha Siber Güvenlik Paketleri Nelerden Oluşur?

1. Ağ Güvenliği

Siber güvenliğin bel kemiğini oluşturan ağ güvenliği, taktik saha operasyonlarında ilk savunma hattıdır. Güvenlik duvarları (firewall), saldırı tespit ve önleme sistemleri (IDS/IPS) ve VPN çözümleri, düşman siber saldırılarına karşı güçlü bir koruma sağlar. Ağ segmentasyonu ve mikrosegmentasyon, saldırıların yayılmasını önleyerek hasarı minimize eder.

2. Son Kullanıcı Cihaz Güvenliği

Sahadaki askeri personelin kullandığı cihazların güvenliği, operasyonel bilgilerin korunması açısından kritik öneme sahiptir. Anti-virüs ve anti-malware yazılımları, güvenli işletim sistemleri ve mobil cihaz yönetimi (MDM) çözümleri, bu cihazların güvenliğini sağlar. Bu sayede, cihazlara yönelik saldırılar engellenir ve hassas bilgiler korunur.

3. Veri Güvenliği

Veri, modern savaş alanlarında en değerli varlıklardan biridir. Veri şifreleme ve şifre çözme teknikleri, veri kaybı önleme (DLP) çözümleri ve güvenli veri saklama ve yedekleme sistemleri, verilerin güvenliğini temin eder. Böylece, kritik bilgilerin yetkisiz kişilerin eline geçmesi engellenir.

4. İletişim Güvenliği

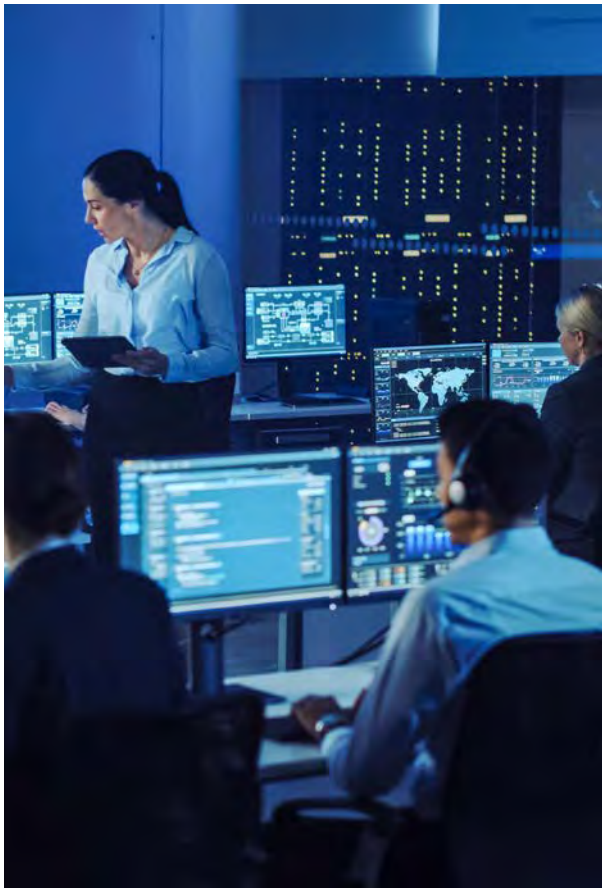
Güvenli iletişim, sahadaki koordinasyon ve operasyonel başarının anahtarıdır. Güvenli uydu iletişimi, şifreli telsiz ve telefon sistemleri ile güvenli e-posta ve mesajlaşma servisleri, iletişim güvenliğini sağlar. Bu sayede, düşman dinlemeleri ve bilgi sızdırmaları önlenir.

5. Durum İzleme ve Yönetim

Güvenlik bilgi ve olay yönetimi (SIEM) sistemleri, sürekli izleme ve log analizi, tehdit istihbaratı entegrasyonu, sahadaki siber güvenlik durumunu anlık olarak takip etmeyi ve hızlı müdahale etmeyi mümkün kılar. Olay müdahale ekipleri, olası tehditlere karşı hazırlıklı olur ve etkili bir şekilde yanıt verir.

6. Fiziksel Güvenlik

Siber güvenliğin yanı sıra, fiziksel güvenlik de büyük önem taşır. Güvenli veri merkezleri, saha ekipmanlarının güvenliği, fiziksel erişim kontrolleri ve çevre izleme sistemleri, operasyonel güvenliği tamamlayıcı unsurlar olarak karşımıza çıkar. Fiziksel güvenlik önlemleri, siber güvenlik önlemleriyle entegre çalışarak bütünsel bir güvenlik sağlar.



7. Siber Eğitim ve Farkındalık

Siber güvenliğin en zayıf halkası genellikle insan faktörüdür. Bu nedenle, askeri personelin siber farkındalığının artırılması ve düzenli eğitimlerle bilinçlendirilmesi kritik öneme sahiptir. Eğitim programları ve tatbikatlar, kullanıcı farkındalığını artırırken, olay müdahale ekiplerinin de yetkinliklerini geliştirir.

Gerçek Dünya Örnekleri ve Çözüm Önerileri

a. ABD Askeri İletişim Sistemleri

ABD ordusu, taktik saha operasyonlarında güvenli iletişim sağlamak için uydu tabanlı iletişim sistemleri ve şifreli telsiz ağları kullanmaktadır. Bu sistemler, düşman dinlemelerine karşı koruma sağlar ve operasyonel bilgilerin güvenliğini temin eder. İleri seviye şifreleme teknikleri kullanarak iletişim güvenliğinin artırılması ve uydu iletişim ağlarının yedekli ve esnek olması, acil durumlarda alternatif iletişim kanallarının devreye girebilmesi önerilebilir.

b. İsrail'in Demir Kubbe Savunma Sistemi

İsrail, Demir Kubbe füze savunma sistemiyle, sahadaki füze saldırılarına karşı etkin bir koruma sağlamaktadır. Bu sistem, gerçek zamanlı veri analizi ve tehdit tespiti yaparak saldırıları engeller. Yapay zekâ ve makine öğrenimi teknikleriyle tehdit tespit ve önleme sistemlerinin güçlendirilmesi, gerçek zamanlı veri işleme kapasitesinin artırılması ve veri güvenliğinin sağlanması, bu sistemlerin etkinliğini daha da artıracaktır.

c. NATO Siber Tatbikatları

NATO, düzenli olarak siber tatbikatlar gerçekleştirerek üye ülkelerin siber güvenlik yetkinliklerini test eder ve geliştirir. Bu tatbikatlar, gerçek dünya senaryoları üzerinden siber tehditlere karşı hazırlık yapmayı amaçlar. Düzenli siber tatbikatlarla personelin ve sistemlerin yetkinliklerinin sürekli olarak test edilmesi ve geliştirilmesi, tehdit istihbaratı paylaşımının artırılması ve iş birliği imkanlarının genişletilmesi, bu tür tatbikatların etkinliğini artıracaktır.

Karşılaşılabilecek Zorluklar

Siber tehditlerin sürekli evrilmesi ve yeni saldırı yöntemlerinin ortaya çıkması, bu dinamik ortamda savunma sistemlerinin güncel kalmasını zorlaştırır. Kaynak kısıtları, siber güvenlik çözümlerinin maliyetli olması ve askeri bütçelerin bu çözümleri finanse etmekte zorlanması, nitelikli siber güvenlik uzmanlarının bulunması ve istihdam edilmesi de önemli zorluklar arasında yer alır. Askeri sistemlerin genellikle karmaşık ve birbirine entegre yapıda olması, bir sistemdeki zafiyetin diğer sistemlere yayılma riskini artırır. Bu nedenle, tüm sistemlerin güvenliğinin entegre bir şekilde yönetilmesi gerekmektedir. İnsan faktörü ise en zayıf halka olarak karşımıza çıkmaktadır. Kullanıcı hataları ve sosyal mühendislik saldırıları gibi insan kaynaklı zafiyetler, siber güvenlik önlemlerini etkisiz hale getirebilir.

Sonuç

Taktik saha siber güvenlik paketleri, askeri operasyonların başarısı için vazgeçilmezdir. Bu paketler, sahadaki verilerin, iletişimin ve cihazların güvenliğini sağlayarak, operasyonel bütünlüğü ve başarısını korur. Askeri operasyonların dijital kalkanı olan bu çözümler, siber tehditlere karşı güçlü bir savunma sağlar ve askeri personelin güvenliğini temin eder.

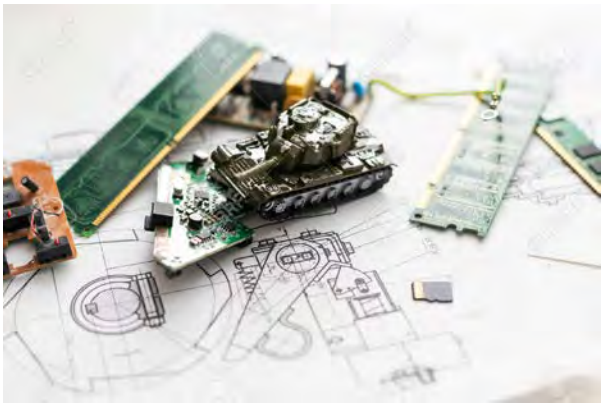
Siber güvenlik, modern savaş alanlarında başarının anahtarıdır ve bu alandaki gelişmeler, gelecekteki askeri operasyonların nasıl şekilleneceğini belirleyecektir. Taktik saha siber güvenlik paketleri, bu geleceğin temel yapı taşlarından biridir.

ELEKTRONİK HARP VE SİBER GÜVENLİK

Dr. Halil Kemal TAŞKIN

Giderek daha sık duymaya başladığımız dijital dönüşüm ile sahip olduğumuz dijital varlıklar da aynı hızda artmaya başladı. Bu da bilgi ve haberleşme teknolojilerini hayatımızın ayrılmaz bir parçası haline getiriyor. Bu hızlı ilerleme dijital dünyada da güvenlik açıklarının ortaya çıkmasına sebep oldu. Siber suçlar, bilgi sızıntıları, fidye yazılımları ve diğer saldırı türleri yaygın şekilde karşımıza çıkıyor. Siber güvenlik bu tür tehditlere karşı bilgi sistemlerini, bilgisayarları, ağları ve diğer dijital varlıkları korumayı amaçlar. Saldırganlar ile savunanlar arasında hiç bitmeyen bir yarış olan bu yolculukta sadece teknolojik önlemler değil, aynı zamanda idari, eğitim, farkındalık ve sürekli iyileştirme süreçleri dikkate alınmalıdır. Bu yazı boyunca özellikle elektronik harp ve siber güvenlik kavramlarının birbiri ile kesiştiği konular irdelenecek ve hem saldırı hem de savunma bakış açısıyla siber elektronik harp ele alınacaktır.

Bununla birlikte, askeri haberleşme özelinde baktığımızda elektronik harp kritik öneme sahiptir.



Elektronik harp kavramından bahsedebilmek için öncelikle elektromanyetik spektrum kavramını tanımlamamız gerekir.

Elektromanyetik spektrum en sade ve teknik olmayan tabirle elektromanyetik radyasyonun yayılabildiği aralık olarak ifade edilebilir. Bu aralık üzerinde elektromanyetik radyasyon, farklı sinyallerin dalga boyları ya da frekanslarına göre sınıflandırılabilmektedir. Spektrum, teoride sonsuz ve sürekli olarak kabul edilse de gerçek hayatta, tanımlı fiziksel sınırlar içinde kalmaktadır. Bu doğrultuda, elektromanyetik spektrumun belirli alanları haberleşme sinyalleri için kullanılmaktadır. Spektrumun nasıl kullanılacağı ulusal ve uluslararası regülasyonlarla belirlenmektedir.

Diğer yandan, bilgisayarların ve insanların haberleşme ağları üzerinden kurduğu etkileşim ile var olan ortama siber uzay denilmektedir. Kara, hava, deniz ve uzaydan sonra beşinci ve yeni bir savaş alanı olarak tanımlanan siber uzay üzerinde tanımlı faaliyetlerin ve aktörlerin diğer alanlara benzer şekilde şekillendiği ifade edilebilir. Ancak, yapısı gereği birçok unsuru siber uzaya uygun şekilde tanımlamak gerekmektedir. Bunun içinde bilgi kavramı temelinde düşünmemiz gerekir. Bir örnek ile buradaki farkı vurgulamaya çalışalım. Gerçek hayatta korumak istediğimiz bir varlığımız olsun. Bu fiziksel bir nesne olabilir. Bu nesneyi korumak için kilitli bir dolap, dolabın bulunduğu güvenli bir oda ya da bina ve onları da çevreleyen bir çit düşünebiliriz. Saldırganın bu nesneye ulaşması için fiziksel olarak bu engelleri geçmesi gerekecektir. Şimdi de benzer senaryoyu siber uzayda düşünelim. Bilginin giderek daha fazla dijital ortama aktarıldığı ve işlendiği günümüzde dijital varlıklarımız siber uzayın en kritik bileşenlerinden birisidir. Siber uzay üzerindeki bir varlığı korumak, fiziksel olarak bir nesneyi korumaktan çok daha farklı olacaktır. Özellikle fiziksel sınırları olmayan bir alanda ve tanımı net olmayan saldırganlara karşı önlemler almak daha karmaşık bir hal alacaktır. Örnekte kullandığımız terimlere bakarsak; saldırgan, güvenlik, sınır, varlık vb. kavramlarının siber uzayda bir karşılığı olduğunu söyleyebiliriz. Ancak yapısı gereği siber uzayın kendi dinamikleri doğrultusunda aksiyonları almamız gerekecektir.

Siber uzay ve bir noktada siber uzayın fiziksel sınırları olarak ifade edebileceğimiz elektromanyetik spektrum aslında birbirinin içine geçmiş durumdadır. Bu da elektronik harp ve siber uzay kavramlarının birbirinden bağımsız düşünülemeyeceği gerçeğini ortaya koymaktadır.

Askeri Haberleşme Güvenliği

Günümüzde askeri alanda etkin bir komuta kontrol sağlanabilmesi için ateş destek ve hava savunma gibi farklı sistemlerin entegre olarak hareket halinde çalışması kritik önem arz etmektedir. Bu sayede, etkin görev icrası, anlık operasyon takibi gibi faaliyetlerin sorunsuz yürütülmesi sağlanmaktadır.

Elektronik harp kavramının detaylarını işlemeden önce askeri sistemlerin haberleşme güvenliğine yönelik tanımlanan katmanları açıklamak faydalı olacaktır. Askeri haberleşme sistemleri, askeri platformların haberleşme ihtiyaçlarını karşılamak için güvenli, güvenilir ve tanımlanabilir bir altyapının sağlandığı sistemlerdir. Ülkelerin kendilerine

ait haberleşme sistemlerinin olması askeri alanda ilerlemeleri için temel unsurlardan birisidir.

Askeri haberleşme güvenliği üç temel başlık altında incelenmektedir:

1. Haberleşme Güvenliği (COMSEC: Communication Security)

Haberleşme güvenliği, bilginin korunması aşamasındaki temel katmandır. Bu katmanda bilginin gizliliği ve bütünlüğü sağlanır, erişim denetimi ve kimlik doğrulama adımları tamamlanır. Bununla birlikte, haberleşmenin yapıldığı cihazın çalışma ortamında karşılaşabileceği kurcalama, hata yaratma, yan kanal analizi ve protokol saldırıları gibi tehditlere karşı da önlemler alınır. Veri imha etme süreçleri bu katmanda tanımlanır.

Haberleşme güvenliği, iletişim ekipmanlarının tasarımından kullanımına kadar bir dizi adımı içerir. Bu adımlar, bilginin kaynağından alıcıya kadar olan tüm iletişim sürecini kapsar. Ulusal ve uluslararası tanımlanmış COMSEC standartları, iletişim ekipmanlarının güvenlik politikalarını belirler ve uygulanmasını sağlar.

Haberleşme güvenliği, bilgi güvenliği stratejisinin önemli bir parçasıdır ve siber saldırılar gibi modern tehditlere karşı kurumların ve devletlerin savunmasını güçlendirmeye yardımcı olur. Başarılı bir COMSEC stratejisi; bilgilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayarak kurumların ve devletlerin güvenliğini artırır.

2. Ağ Güvenliği (NETSEC: Network Security)

Kablosuz ağ haberleşmesinde ağa yetkisiz erişimi engellemek, ağdan erişilebilen kaynakların kötüye kullanımını, değiştirilmesini ya da reddedilmesini önlemek, tespit etmek ve izlemek için ağ seviyesinde alınan kriptografik önlemlerdir. Mobil tasarsız ağlara dahil olma mekanizmaları bu kapsamda değerlendirilebilir. Ayrıca, COMSEC katmanına ek olarak, gönderilen tüm verilerin gizlilik ve bütünlüğünü korumaya yönelik kriptografik çözümler bu katmanda da uygulanabilmektedir.

3. Aktarım Güvenliği (TRANSEC: Transmission Security)

Aktarım güvenliği; kablosuz veri iletiminin alıcı tarafında kesintiye uğramasını, aldatılmasını ya da istihbarat oluşturulmasını, dalga şeklinin kritik işleyiş ve özelliklerinin analizi yoluyla ele geçirilmesini önlemek için iletim katmanında kriptografik yeteneklerden faydalanılarak iletim güvenliğini sağlamayı hedefleyen algoritma ve protokollerdir.

Bu kapsamda, özellikle kriptografik rassallık yetenekleri kullanılarak frekans atlama yeteneklerinin geliştirilmesi ve dalga şekli davranışlarının tahmin edilemez hale getirilmesi sağlanmaktadır. Karıştırma (jamming) saldırılarına karşı dayanıklılık bu katmanda alınan önlemler ile sağlanmaktadır.

Bahsedilen katmanlar arasında sıralı bir ilişki vardır. Haberleşmenin başladığı bir uçta sırasıyla COMSEC, NETSEC ve TRANSEC katmanlarında veri işleme yapılır.

Özgün Dalga Şekli Tasarlamak

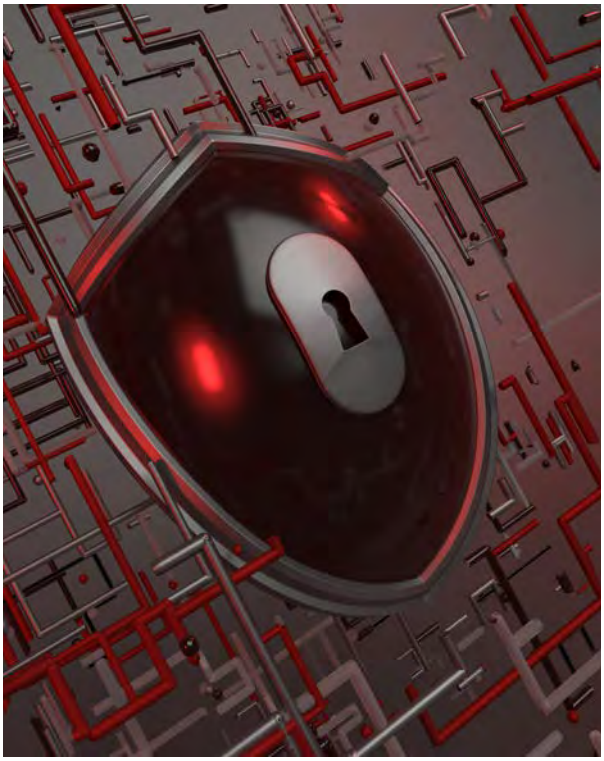
Güvenliğin ilk andan itibaren ele alınması gereken kritik bir unsur olarak değerlendirilmesi ile birlikte haberleşmenin başladığı en alt katmandan itibaren güvenlik önlemleri alınmaya başlaması kritik önem arz etmektedir. Kablosuz sinyallerin havada ne şekilde yayılacağı dalga şekli olarak ifade edilebilir. Açık olarak yayınlanmış bilinen dalga şekillerinin tespiti ve analizi çok daha kolay olduğu için her ne kadar sivil kullanımları yaygın olsa da askeri haberleşme için tercih edilmezler. Bu doğrultuda, özellikle ülke güvenliği değerlendirildiğinde yerli özgün dalga şekillerine sahip olmak önem arz etmektedir. ASELSAN, GBDŞ ve KKDŞ gibi özgün dalga şekli tasarımlarını ürünlerinde kullanmaktadır.

Elektronik Harp

Elektromanyetik spektrum üzerinde sahip olunan kontrol yeteneği elektronik harp olarak tanımlanabilir. Elektromanyetik spektrumu kontrol edebilen, gücü de elinde bulunduracaktır. Elektronik harp yetenekleri devletler için kritik askeri güç unsurlarıdır. Askeri olarak GİZLİ gizlilik seviyesindeki bilgilerin korunması sağlamaktadır. Elektronik harp üç temel başlıktan oluşur.

1. Elektronik Destek (ED)

Savaş alanında elektromanyetik spektrumun izlenmesi ve analiz edilmesi süreçleridir. Elektronik Destek, elektromanyetik spektrum üzerindeki sinyallerin dost düşman sinyali olup olmadığının tespiti, düşman sinyallerinin tespiti ve analizi, kendi sistemlerine yönelik gelen taarruzların tespiti gibi düşmanın elektronik altyapısını anlamak, izlemek ve analiz etmek için kullanılan bir dizi teknik ve yetenekleri ifade eder.



Elektronik destek, düşmanın elektromanyetik spektrum içinde (örneğin, radyo dalgaları, radar sinyalleri, iletişim frekansları vb.) yayılan sinyalleri izleme, tespit etme, sınıflandırma ve analiz etme sürecini kapsar. Bu başlık; düşmanın elektronik iletişim sistemlerini, radarlarını, kablosuz iletişim ekipmanlarını ve diğer elektromanyetik yayıcıları izlemeyi ve anlamayı içerir.

Elektronik destek operasyonları genellikle düşmanın taktik ve stratejik kapasitesini anlamak, düşmanın niyetlerini belirlemek ve dost kuvvetlerin güvenliğini sağlamak için kullanılır. Bu bilgiler, askeri planlama ve karar verme süreçlerinde kritik bir rol oynar ve sahada operasyonların etkinliğini artırmaya yardımcı olur. Bu da diğer askeri faaliyetlerle entegre edilir ve askeri istihbarat toplama çabalarının önemli bir parçasıdır.

2. Elektronik Taarruz (ET)

Elektronik harp yöntemleri kullanılarak düşmana ait elektromanyetik spektrumun kullanımının engellenmesine yönelik yapılan faaliyetlerdir. Elektronik taarruzun amacı, düşmanın elektronik altyapısını etkisiz hale getirmek, engellemek ya da manipüle etmek aracılığıyla operasyonel yetenek-

lerini kısıtlamaktır. Bu, düşmanın iletişimini kesmek, radar sinyallerini yanıltmak veya düşmanın silah sistemlerini etkisiz hale getirmek gibi çeşitli şekillerde gerçekleştirilebilir. Elektronik Taarruz operasyonlarının başarısı Elektronik Destek yeteneklerinin etkinliğine dayanır.

Elektronik taarruz, modern savaş alanlarında giderek daha önemli bir rol oynamaktadır çünkü elektronik sistemlerin kullanımı ve bağımlılığı artmıştır. Düşmanın elektronik altyapısını etkisiz hale getirmek veya manipüle etmek, askeri avantajın sağlanması ve dost kuvvetlerin güvenliğinin sağlanması açısından kritik bir öneme sahiptir. Bu nedenle, elektronik taarruz operasyonları, modern askeri doktrinlerin ve stratejilerin ayrılmaz bir parçası haline gelmiştir.

3. Elektronik Kendini Koruma (EKK)

Kendini Koruma, elektronik sistemlerin kendi güvenliklerini koruma yeteneğini ifade eder. Bu; düşmanın elektronik taarruzlarına, sinyal engelleme veya diğer elektromanyetik müdahalelere karşı savunma sağlama amacıyla gerçekleştirilen önlemleri içerir. ED ve ET yöntemlerinin etkin kullanımını gerektirir.

Siber Güvenlik Modeli

Siber güvenliğin sağlanması için yapılacak faaliyetleri belirlemek için belirli ölçütlere ihtiyaç olacaktır. Bu noktada gizlilik, bütünlük ve erişilebilirlik prensipleri siber güvenlik modelinin çatısını oluşturmaktadır. Bu prensipler, siber güvenliğin temel hedeflerini ve stratejilerini belirler. Kurumlar, bilgi sistemlerini ve dijital varlıklarını korumak için bu prensipler temelinde hareket etmeli ve tehditleri engellemek için gerekli savunma önlemlerini planlamalıdır. Bu doğrultuda hazırlanacak bir siber güvenlik modeli, gizlilik, bütünlük ve erişilebilirlik prensiplerini içeren kapsamlı stratejiyi benimsemelidir.

1. Gizlilik

- Bilginin yetkisiz kişiler tarafından ele geçirilememesini sağlamayı hedefler.
- Gizliliğin sağlanması için kriptografik yöntemler ile şifreleme mekanizmaları kullanılmalıdır.

2. Bütünlük

- Bilgi yetkisiz değişikliklere karşı korunmalıdır.

- Bilginin iletimi sonrasında oluşan hatalar ya da saldırgan kaynaklı oluşabilecek bozulmalar/değişiklikler tespit edilebilmelidir.

- Bütünlüğün sağlanması için alınacak önlemler ve yapılacak kontroller kriptografik olarak güçlü mekanizmalar ile tesis edilmelidir.

3. Erişilebilirlik

- Bilginin ve sistemlerin ihtiyaç duyulduğu anda kullanılabilir olmasını sağlayan önlemler bütünüdür.

- Bilgi iletiminde kanal erişiminin ve kullanılmasının, zamanında ve güvenilir olmasını sağlamayı hedefler.

- Planlanmamış kesintilere, doğal afetlere ve kötü niyetli saldırılara yönelik dirençli bir yapının tesis edilmesi de bu kapsam değerlendirilir.

Siber güvenlik modelini oluşturan prensipler ile birlikte, erişim yönetimi için genel geçer kabul görmüş/görülmüş AAA modeli de uygulanmalıdır. AAA modeli üç temel terimi ifade etmektedir:

1. Kimlik Doğrulama (Authentication)

Haberleşmenin yapıldığı (insanlı ya da makineler arası) ortamda haberleşen uçların kimlik doğrulama süreçlerine tabi tutularak geçerliliklerin doğrulanması süreçleridir. Kimlik doğrulama için merkezi yapılar ve ileri seviye doğrulama yöntemleri gibi çözümler kullanılabilir.

2. Yetkilendirme (Authorization)

Kimlik doğrulaması yapılan bir haberleşmede uçların erişebileceği konumların denetlenmesine yönelik yapılan mantıksal kontroller, yetkilendirme olarak ifade edilmektedir. Yetkilendirme kontrolü temel ve statik kontrollerle yapılabileceği gibi sıfır-güven modeli gibi karmaşık ve dinamik olarak da kontrol edilebilmektedir.

3. Hesap Verilebilirlik (Accounting)

Haberleşen uçların olduğu ortamda, kimlik doğrulama ve yetkilendirme süreçlerinin yönetilmesini destekleme amacıyla özellikle işlem kaydı tutma gibi yeteneklerin geliştirilmesi hesap verilebilirlik başlığı altında ele alınmaktadır. Özellikle geçmişe yönelik olarak kayıtların saklanması, bu kayıtların değiştirilememesi ve inkâr edilememesi gibi özelliklerin sağlanması kritik önem arz etmektedir.

Siber Güvenlik Tehditleri

Günümüzde siber saldırılar tüm haberleşme sistemleri için tehdit oluşturmaktadır. Taktik sahada kullanılan haberleşme sistemleri de bu saldırıların hedefi haline gelmektedir. Taktik haberleşme altyapıları, multi-hop veri ve ses iletişimini mümkün kılan sistemlerden oluşmaktadır. Bu ağlar üzerinde siber güvenlik ihtiyaçları vazgeçilmez bir noktaya gelmektedir.

Siber güvenlik özelinde alınacak önlemlerin tasarım aşamasından itibaren uygulanması sayesinde ilk andan itibaren ürün geliştirme sürecinin her aşamasında siber güvenlik tehditlerinin tanımlanması ve risklerin en aza indirilmesi hedeflenmektedir. Benzer şekilde, ürünün faaliyete geçtikten sonra çalışma ortamında siber güvenliğe yönelik izleme ve test faaliyetlerinin gerçekleştirilmesi de yaşayan bir siber güvenlik anlayışı için kritik önem arz etmektedir.

Kablosuz haberleşme ağları özelinde oluşabilecek tehditler aşağıdaki ana başlıklar altında özetlenmiştir.

1. Gözetleme

Gözetleme saldırıları, elektromanyetik spektrum üzerinde radyo frekansı haberleşmesinin gözetlenmesine yönelik saldırıları içermektedir. Temelinde pasif saldırılardır. Olası bilgi sızmalarını tespit etmeyi hedefler. İletilen verinin içeriği okunamıyor dahi olsa hangi zamanda hangi birimler ne kadar süreli veri iletimi yapıyor, birimlerin kendi haberleşme örüntüsünün tespiti gibi yan bilgiler bile bilgi ifşasına sebep olabilir. Ya da veri yapılarının çözümlenmesi de doğrudan korunmuş bilgiye erişim sağlamasa bile saldırganlar için ilave bir bilgi olacaktır. Örneğin, paket toplama ve trafik keşif (wardriving) faaliyetleri gözetleme saldırıları olarak ifade edilebilir.

2. Tekrarlama

Tekrarlama saldırıları, saldırganın ağ üzerinde ele geçirdiği/topladığı paketleri tekrar ağa göndererek gerçekleştirdiği saldırılardır. Aktif ve pasif aşamaları vardır. Mevcut bir haberleşmenin kaydedilerek, herhangi bir değişiklik yapılmadan aynı paketin başka zamanda tekrar gönderilmesidir. Tekrarlanan paketin içeriğine göre ağ üzerinde haberleşmede ve cihazların davranışlarında problem oluşması hedeflenir. Kimlik doğrulama saldırıları, oturum ele geçirme saldırıları ve taklit etme (impersonation) saldırıları bu kapsamda değerlendirilebilir.

3. Ortadaki Adam

Ortadaki adam saldırıları, ağ haberleşmesinde saldırganın araya girerek gerçekleştirebileceği varsayılan saldırılar olarak ifade edilmektedir. Aktif olarak gerçekleştirilmektedir. Başarılı bir saldırgan iletilen mesajın içeriğini değiştirebilir, mesajın hedefe gitmesine engel olabilir ya da mesajlara erişim sağlayabilir. Bu sayede servis reddi saldırıları, oturum ele geçirme saldırıları, trafik analizi gibi çeşitli zararlı faaliyetleri icra edebilir.

4. Yerine Koyma

Yerine koyma saldırıları, saldırganın kendisini ağ üzerinde tanıtarak gerçekleştirdiği saldırılardır. Kendisini tanıtma işlemi, saldırganın hem yeni bir kimlik ile kendini tanıtması hem de mevcut bir kimliğin yerine kendini koyarak tanıtması şeklinde olabilir. Aktif olarak gerçekleştirilen bir saldırıdır. Ancak, saldırganın kendi mesajlarını oluşturma yeteneği olduğu varsayıldığı için ortadaki adam saldırından farklı olarak, herhangi bir mevcut haberleşme ihtiyacı olmadan gerçekleştirilebilir. Kötücül ikiz (evil twin) ve sahte düğüm (rogue node) saldırıları bu kapsamda değerlendirilebilir.

5. Yönlendirme

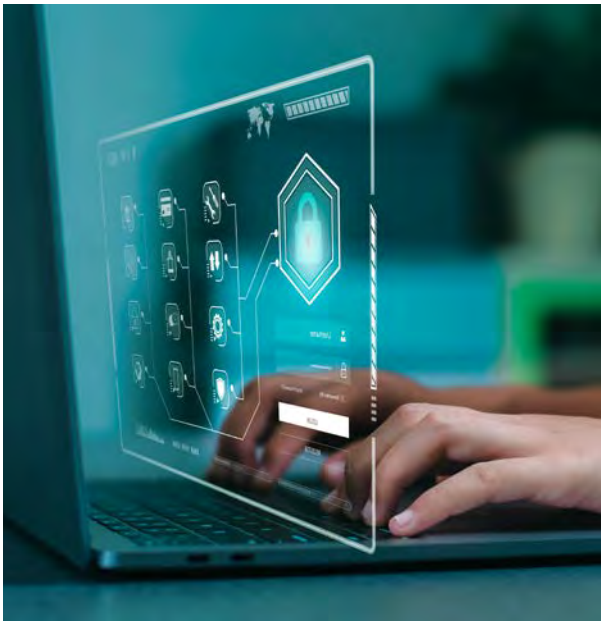
Yönlendirme saldırıları, ağ haberleşmesinde kullanılan yönlendirme protokolüne yönelik gerçekleştirilen saldırılardır. Ağ üzerindeki paket yönlendirmesini manipüle ederek ağda sıkışıklık oluşturma, iletişimi yavaşlatma, kaynak tüketimini arttırma ve paketleri kendi üzerinden taşımayı amaçlayan saldırılar gerçekleştirilir. Kara delik (black hole) saldırıları, solucan deliği (worm hole) saldırıları ve bencil düğüm (selfish node) saldırıları bu kapsamda değerlendirilebilen saldırılardır.

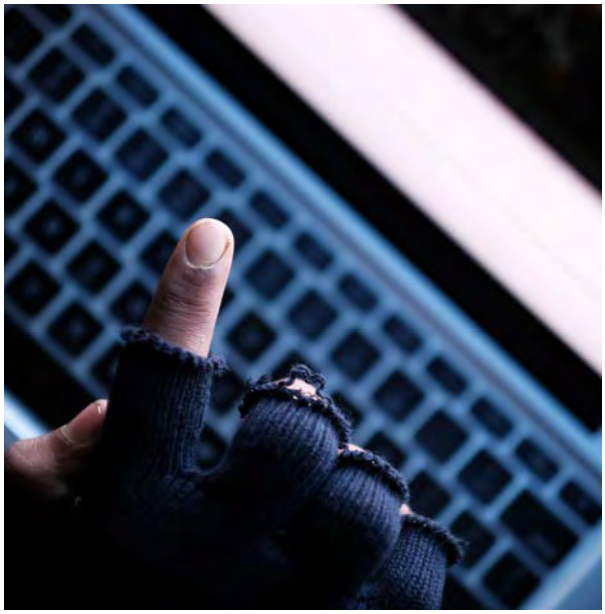
6. Kimlik Doğrulama

Kimlik doğrulama saldırısı, saldırganın mevcut kullanıcıların kimlik doğrulama ya da oturum bilgilerini çalmayı amaçladığı saldırılardır. Ortadaki adam ve gözetleme saldırılarından faydalanılarak gerçekleştirilen saldırılardır. Oturum ele geçirme saldırıları ve ele geçirilen paketlerin analizi ile gerçekleştirilebilecek sözlük ve kaba kuvvet saldırıları bu kapsamda değerlendirilebilir.

7. Fiziksel Erişim

Kullanılan cihazlara yönelik gerçekleştirilen fiziksel saldırılardır. Diğer tehditler için destekleyici unsur olarak kullanılabilir. Bilgi sızmasını ve erişilebilirliği etkilemeyi amaçlar. Cihazın ele geçirilmesi, tersine mühendislik yöntemleri ile cihazın yazılım ve gizli bilgilerin çıkarılması, cihazın kopyalanması gibi faaliyetler bu kapsamda değerlendirilen saldırılardır.





8. Erişilebilirlik

Ağ haberleşmesindeki kaynaklara erişimi kısıtlama ya da ağı işlevsiz hale getirme saldırılarıdır. Cihazların ya da ağ yeteneklerinin kısıtlanmasını amaçlar. Yönlendirme saldırıları ve fiziksel saldırılar da bu amaçla kullanılabilmektedir. Özellikle batarya ile çalışan kaynak kısıtlı cihazlara yönelik yapılacak kaynak tüketim saldırıları ile ilgili cihazların devre dışı bırakılması gibi birden fazla aşama gerektiren saldırılar bu kapsamda değerlendirilmektedir. Ayrıca, karıştırma (jamming) ile haberleşmenin engellenmesi ya da yavaşlatılması da en kritik erişilebilirlik saldırılarından birisidir.

Elektronik harp ve siber güvenliğe yönelik temel tanımları oluşturduktan sonra, tanımlanan tehdit listesi üzerinden her iki kavramı ele aldığımızda, hem saldırı hem de savunma alanında tehditlere yönelik yapılacak faaliyetlerin elektronik harp ve siber güvenlik alanlarının ortak çalışması ile gerçekleştirilebileceği aşikardır. Bu da tanımlanması gereken yeni bir alan doğurmaktadır: Siber-Elektronik Harp

Siber-Elektronik Harp

Siber güvenlik tehditleri, askeri haberleşme güvenliğinde kullanılan üç temel katman; COMSEC, NETSEC, TRANSEC, siber güvenlik modelinin oluşturulması için kullanılan prensipler; gizlilik, bütünlük, erişilebilirlik ve erişim yönetimi için kullanılan kimlik doğrulama, yetkilendirme ve hesap verilebilirlik terimlerini ele aldığımızda, bu üç alan arasındaki bağlantı siber uzay ve elektronik harp kavramlarının kesiştiği alanı gösterecektir.

Savunma tarafından baktığımızda, listelenen siber güvenlik tehditlerine yönelik çözümler askeri haberleşme güvenliğinin her katmanında sağlanan çözümler ile ele alınmaktadır. Bu katmanlar üzerindeki uygulamalar elektronik harp tekniklerinin aktif kullanımını gerektirecektir.

Benzer şekilde, siber güvenlik tehditlerine yönelik gerçekleştirilecek ataklar da siber atak kapsamında yapılacak faaliyetleri içerecektir. Ancak, askeri haberleşme sistemlerinin devrede olması ile birlikte siber saldırıların gerçekleştirilmesi için öncelikle elektronik harp tedbirlerinin aşılmasına yönelik saldırıların gerçekleştirilmesi ve bunların devamında erişim sağlanan sisteme yönelik siber saldırıların gerçekleştirilmesi mümkün olacaktır.

Savunma ve taarruz tarafları için hem elektronik harp hem de siber güvenlik yeteneklerinin bir araya gelmesi ile yapılacak saldırılar siber-elektronik harp olarak ifade edilebilir.

KABLOSUZ AĞLARDA GÜVENLİK

Berkan UFUK

Kablosuz ağlar, özellikle kullanım kolaylığı sebebiyle oldukça yaygın hale geldi. Kabloların getirdiği karmaşıklık ve kısıtlamalara sahip olmayan kablosuz ağlar, evlerde, ofislerde ve halka açık alanlarda kolaylıkla internete bağlanmayı ve iletişim kurmayı sağlamaktadır. Ancak kablosuz ağlar, kolaylıklarla birlikte bazı güvenlik açıklıkları da içerebilmektedir. Bu yazıda, genel olarak IEEE 802.11 Standardı ile ilişkilendirilebilen riskler ve bu riskleri gidermek için yapılabilecekler incelenecektir. Ancak, öncelikle kablosuz ağları tanıyalım.

Kablosuz Ağ Nedir?

Bir kabloya ihtiyaç duymadan cihazların radyo dalgaları ile birbirine bağlanmasını sağlayan ağlardır. Kullanım kolaylığı, daha ucuz maliyeti ve kablo döşenmesi gibi bir altyapı gerektirmediği için günümüzde oldukça yaygın olarak kullanılmaktadır. Kablosuz ağlar başlıca alıcı ve vericiden oluşur. Alıcı, radyo sinyallerini dinleyen verici ise radyo sinyallerini ileten cihazlardır. Kablosuz ağ mimarisinde hem alıcı hem de verici görevi üstlenen cihazlar da vardır. Bu cihazlarla iki tür kablosuz ağ yapısı oluşturulabilir. Bunlar, P2P (Peer to peer – eşler arası) ve Kablosuz Yönlendirici/Erişim Noktası gerektiren bağlantılardır. P2P bağlantısında alıcı ve verici cihazlar direkt olarak birbirlerine sinyal gönderip alabilirler. Erişim Noktası/Kablosuz Yönlendirici gerektiren bağlantılarda ise alıcı ve verici kablosuz yönlendirici üzerinden haberleşirler.

Kablosuz Ağ Çeşitleri (WPAN, WLAN, WPAN, WWAN)

Kablosuz Ağlar kullanım amaçları ve kapsama alanlarına göre dört ayrı kategoride incelenebilir:

1- WPAN (Wireless Personal Area Network – Kablosuz Kişisel Alan Ağı): 10 metreye kadar çok kısa mesafeli kablosuz haberleşme için kullanılır. IEEE 802.15 Standardı olarak bilinen WPAN kapsama alanı içerisindeki tüm cihazlarla veri iletimi yapılmasını sağlar. Bluetooth, ZigBee ve UWB (Ultra Wideband – ultra geniş bant) WPAN teknolojileridir.

a. Bluetooth: Kısa menzilli iletişim teknolojidir ve genellikle veri transferi için kullanılır. Düşük güç tüketimi ve kolay bağlantı sağlanması sayesinde özellikle mobil cihazlar, kulaklıklar, klavye ve fareler gibi taşınabilir cihazlarda yaygın olarak kullanılmaktadır. Bluetooth ayrıca akıllı ev ci-

hazları ve otomotiv uygulamaları gibi farklı alanlarda da kullanılmaktadır.

b. ZigBee: sensörler ve kontrol cihazlarında yaygınca kullanılmaktadır. P2P, Star (yıldız) ve Mesh (örgü) topolojilerine uygundur.

c. UWB (Ultra Wideband): Kısa bir mesafe için geniş bir frekans bandında düşük güç ile büyük miktarlarda veri aktarımı için kullanılan kablosuz kişisel alan ağı teknolojisidir.

2- WLAN (Wireless Local Area Network – Kablosuz Yerel Alan Ağı): 100 metreye kadar olan (eğer engel yoksa) menzil sağlayan kablosuz haberleşme teknolojisidir. Evlerde ve ofislerde yaygın olarak kullanılan WLAN teknolojisi olan Wi-Fi (Wireless Fidelity – Kablosuz İnternet) genellikle Internete bağlanmak için kullanılmaktadır. Servis sağlayıcı ağına bağlı olan kablosuz yönlendiriciler yaydığı Wi-Fi sinyallerinin kapsama alanında olan cihazları birbirine ve Internete bağlayabilir. Wi-Fi, IEEE 802.11 standardına dayanmaktadır. Kablosuz teknolojiler geliştikçe kablosuz ağ protokollerinde de gelişmeler yaşanmıştır. Özetle, bu gelişmeler şu şekildedir:

3- WMAN (Wireless Metropolitan Area Network – Kablosuz Metropol Alan Ağı): IEEE 802.16 Standardı'na dayanan kablosuz haberleşme teknolojileridir. WLAN'a göre daha uzak mesafedeki bilgisayar ağlarını birbirine bağlayabilir. Genellikle kiralık hatlar ve telefon hatları kullanılmaktadır. WIMAX (Worldwide Interoperability for Microwave Access – Mikrodalga Erişimi için Dünya Çapında Birlikte Çalışılabilirlik) bir WMAN teknolojisidir.

4- WWAN (Wireless Wide Area Network – Kablosuz Geniş Alan Ağı): Coğrafi olarak uzaktaki bilgisayar ağlarını birbirine bağlamak için kullanılan teknolojilerdir. Mobil Telekomünikasyon WWAN uygulamalarına örnektir.

802.11 Güvenliği Tarihçesine Hızlı Bir Bakış

Kablosuz ağlar 1990'lı yıllarda ilk tasarlandığında, ana odak unsuru güvenlik değildi. Kablosuz ağlar üzerinden gelen saldırılarla ve performans geliştirmeleri ile birlikte IEEE 802.11 geliştirilmeye devam etti. IEEE 802.11'de kullanılan 4 ana güvenlik protokolü şunlardır.

Wİ-Fİ NESLİ	IEEE STANDARDI	KULLANIMA BAŞLANDIĞI YIL	MAKSİMUM BAĞLANTI HIZI (Mbit/s)	RADYOFREKANSI (GHZ)
Wİ-Fİ 8	802.11bn	2028	100.000	2.4, 5, 6, 7, 42.5, 71
Wİ-Fİ 7	802.11be	2024	1376–46.120	2.4, 5, 6
Wİ-Fİ 6E	802.11ax	2020	574–9.608	6
Wİ-Fİ 6		2019		2.4, 5
Wİ-Fİ 5	802.11ac	2014	433–6.933	5
Wİ-Fİ 4	802.11n	2008	72–600	2.4, 5
Wİ-Fİ 3	802.11g	2003	6–54	2.4
Wİ-Fİ 2	802.11a	1999		5
Wİ-Fİ 1	802.11b	1999	1–11	2.4
Wİ-Fİ 0	802.11	1997	1–2	2.4

WEP (Wired Equivalent Privacy)

WEP, ilk olarak kablosuz ağlar için güvenlik sağlamak amacıyla geliştirilmiş bir şifreleme protokolüdür. 1999 yılında IEEE 802.11 standardının bir parçası olarak tanıtılmıştır. WEP, ağdaki verileri şifrelemek ve bu sayede güvenliği artırmak için kullanılır. Ancak, zamanla WEP'in zayıflıkları ortaya çıkmış ve çeşitli saldırılara karşı savunmasız olduğu kanıtlanmıştır. WEP'in bazı temel özellikleri şunlardır:

- 40-bit ve 104-bit Anahtar Uzunlukları: WEP, şifreleme için 40-bit veya 104-bit şifreleme anahtarları kullanır. Daha uzun anahtarlar, daha güçlü bir şifreleme sağlar, ancak yine de WEP'in güvenlik açıkları nedeniyle etkili değildir.
- Statik Anahtarlar: WEP, ağa bağlanmak için kullanılan şifreleme anahtarlarını manuel olarak yapılandırmak için kullanılır. Bu anahtarlar genellikle kablosuz ağ yönlendiricisi tarafından belirlenir ve tüm kullanıcılar tarafından paylaşılır.
- Yetersiz Rastgelelik: WEP'in anahtar üretme algoritması, yeterli rastgelelik sağlamaz, bu da şifreleme anahtarlarının tahmin edilmesini kolaylaştırır.

Sonuç olarak, WEP artık güvenilir bir kablosuz güvenlik çözümü olarak kabul edilmemekte ve yaygın olarak kullanılmamaktadır. Güvenlik açıklıkları nedeniyle, WEP yerine daha güvenli alternatiflerin kullanılması önerilir.

WPA (Wi-Fi Protected Access)

WEP'te keşfedilen zafiyetler WPA'nın geliştirilmesine öncülük etmiştir. WPA, daha güçlü şifreleme ve kimlik doğrulama yöntemleri sağlar ve bu sayede kablosuz ağların daha güvenli hale gelmesini sağlar. WPA'nın temel özellikleri şunlardır:

- TKIP (Temporal Key Integrity Protocol – Geçici Anahtar Bütünlüğü Protokolü): WPA, verilerin şifrelenmesi için TKIP protokolünü kullanır. TKIP, her veri paketi için dinamik olarak oluşturulan geçici şifreler kullanır, bu da güvenliği artırır.
- PSK (Pre-Shared Key – Önceden Paylaşılan Anahtar) ve Enterprise (Kurumsal) Modları: WPA, ağa bağlanmak için iki farklı kimlik doğrulama modu sunar. PSK modunda, ağa bağlanmak için bir önceden paylaşılan şifre kullanılır. Enterprise modunda ise, her kullanıcı için benzersiz bir kimlik doğrulama yöntemi kullanılır.

WPA, WEP'e göre daha güvenli bir kablosuz iletişim çözümü sağlar ve hala birçok kablosuz ağda kullanılmaktadır. Ancak, zamanla WPA'nın da bazı zayıflıkları ortaya çıkmış ve daha güçlü bir alternatif olan WPA2 geliştirilmiştir.

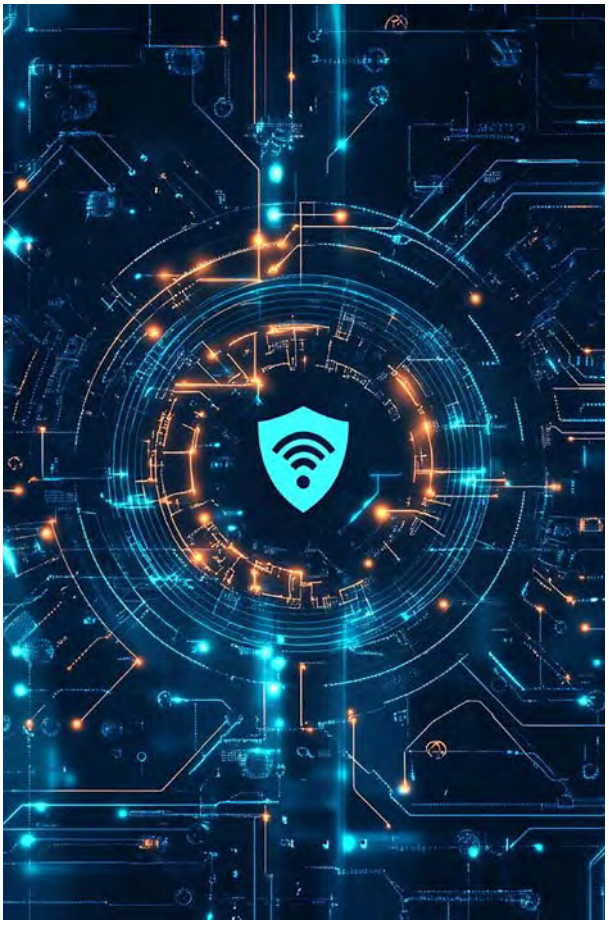
WPA2 (Wi-Fi Protected Access 2)

WPA2, Wi-Fi ağlarını daha güvenli hale getirmek için geliştirilmiş bir protokoldür. İlk olarak 2004 yılında tanıtılmıştır ve orijinal WPA'nın yerini almıştır. WPA2, daha güçlü bir veri şifreleme standardı olan AES (Advanced Encryption Standard – Gelişmiş Şifreleme Standardı) kullanması nedeniyle daha yüksek bir güvenlik seviyesi sağlar. WPA2, iki farklı kimlik doğrulama modu sunar:

- WPA2-Personal (WPA2-PSK): Bu mod, PSK (Pre-Shared Key – önceden paylaşılan anahtar) olarak bilinen bir şifre kullanılarak ağa bağlanmayı sağlar. Kullanıcılar, ağa bağlanırken bu PSK'yi girmeleri gerekmektedir. PSK, ağa bağlanacak tüm cihazlar için aynıdır ve bu nedenle kullanıcılar arasında kolay paylaşılabilir.

- WPA2-Enterprise: Bu mod, her kullanıcı için benzersiz bir kimlik doğrulama yöntemi kullanır. Genellikle 802.1X/EAP (Extensible Authentication Protocol – Genişletilebilir Kimlik Doğrulama Protokolü) protokolü kullanılarak RADIUS (Remote Authentication Dial-In User Service – Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti) sunucuları üzerinden kimlik doğrulama yapılır. Bu, kurumsal ağlarda daha yüksek güvenlik düzeyi sağlar.

WPA2, birçok Wi-Fi ağında hala yaygın olarak kullanılmaktadır ve çoğu durumda güvenilir bir güvenlik seviyesi sağlar. Ancak, bazı zayıflıklar (örneğin, WPA2'nin KRACK (Key Reinstallation Attack – Yeniden Anahtar Yükleme) saldırısına karşı hassas olması, sözlük saldırılarının mümkün olması) ve gelişen teknolojiler nedeniyle, WPA3 daha güçlü bir alternatif olarak ortaya çıkmıştır.



WPA3 (Wi-Fi Protected Access 3)

WPA3, Wi-Fi ağlarını daha da güvenli hale getirmek ve daha gelişmiş koruma sağlamak amacıyla geliştirilmiş bir protokoldür. WPA3, 2018 yılında tanıtılmıştır ve WPA2'nin yerini alması beklenmektedir. WPA3'ün öne çıkan bazı özellikleri şunlardır:

- İyileştirilmiş Şifreleme: WPA3, daha güçlü bir şifreleme standardı olan SAE (Simultaneous Authentication of Equals – Eşit Eş Zamanlı Kimlik Doğrulama) protokolünü kullanır. Bu, kaba kuvvet saldırılarına karşı daha dirençli bir şifreleme sağlar.

- Hassas Ağ Girişi: WPA3, açık ağlarda bile verilerin şifrelenmesini sağlar, böylece ağlara bağlanan cihazlar arasında güvenli bir iletişim sağlar.

- Hedefli Şifreleme: WPA3, her bağlantı için benzersiz bir şifreleme anahtarı kullanır, böylece bir bağlantının ele geçirilmesi diğer bağlantıları etkilemez.

WPA3, daha güçlü bir güvenlik seviyesi sağlamak için tasarlanmıştır ve yeni nesil Wi-Fi ağlarının temelini oluşturması beklenmektedir. Ancak, WPA3'nün daha yaygın olarak benimsenmesi ve yaygınlaşması zaman alabilir, bu nedenle WPA2 hala birçok ağda kullanılmaya devam etmektedir.

Kablosuz Ağlarla İlgili Tehditler

Kablolu ağların aksine, kablosuz ağlar fiziksel bir kablo gerektirmeden ağa dahil olmayı sağladığı için ağa daha kolay dahil olabilen saldırganların tehditlerine karşı daha açıktır. Kablolu bir ağa saldırmak isteyen saldırgan kablolu ağa dahil olmak için fiziksel bir kabloya ihtiyaç duyarken, kablosuz ağlara saldırmak için bir saldırgan, kablosuz ağların veri ilettiği radyo dalgalarına erişim sağlaması yeterlidir. Dolayısıyla, saldırgan, kablosuz bir ağa saldırı yapmak için ağa katılmaya bile ihtiyaç duymayabileceği senaryolar mevcuttur.

Kablosuz ağların içerdiği tehditler STRIDE modeli ile gruplandırabilir. STRIDE, bilgisayar güvenliği tehditlerini gruplandırmak için bir modeldir. STRIDE'ı oluşturan başlıklar şu şekilde tanımlanabilmektedir:

- **Spoofing (Zehirleme)**: Kablosuz ağ trafiğinde saldırganının alıcı ve verici tarafa ulaşıp, kablosuz ağdaki bir kullanıcıyı/makineyi taklit etmesidir. Mesaj değiştirme (message modification), Mesaj tekrar edilmesi (message replay) saldırıları bu kategori altında yer alabilir.

- **Tampering (Kurcalama):** Kablosuz ağ trafiğinde saldırganının alıcı ve verici tarafa ulaşıp, alıcı ve verici taraflarında iletilen paketlerin içeriğini değiştirebilmesidir. Böylece saldırgan, alıcı ve verici arasındaki

trafiği istediği gibi yöneterek kendi emelleri doğrultusunda işlemler yapılmasını hedefler. Mesaj eklenmesi (message injection) saldırıları bu kategori altında ele alınabilir.

- **Repudiation (İnkar Etme):** Kablosuz ağda gerçekleştirilen bir işlemin inkar edilebilmesidir.
- **Information Disclosure (Bilgi İfşası):** Kablosuz ağda iletilen bir verinin gizliliğinin açığa çıkmasıdır. Gözetleme (eavesdropping) saldırıları bu kategori altında yer alabilir.
- **Denial of Service (Servis Kesintisi):** Kablosuz ağın erişilemez olması sağlanıp alıcı ve verici arasında veri iletiminin önlenmesidir. Diğer tehditlerden farklı olarak, saldırganın yalnızca alıcının ya da vericinin sinyallerine ulaşması yeterlidir.
- **Elevation of Privilege (Yetki Yükseltme):** Kablosuz ağları kullanarak bir saldırganın erişmemesi gereken bir yere erişebilmesidir. Kimlik Doğrulamayı Atlatma (Broken Authentication) saldırıları bu kategori altında yer alabilir.

Örnek verilen bu tehditler, kablosuz ağın kullanım senaryosuna göre farklılık gösterebilir. Dolayısıyla kablosuz ağ kullanımı için tehdit modellemesi yapılırken kablosuz ağın kullanım şekline göre yeni tehditler ortaya çıkabilir veya bahsedilen tehditlerden bazıları geçersiz olabilir.

Evdeki/ofisteki kablosuz ağları güvenli hale getirmek (Wi-Fi güvenliği) için yapılabilecekler:

1- Varsayılan Ayarların Güçlendirilmesi: Servis sağlayıcısı tarafından sağlanan modemler, ilk kurulumlarında cihazların üzerindeki etiketlerde yazan bilgilerle yapılandırılmıştır. Bu yapılandırmalar varsayılan kullanıcı adı ve parola içerdiği için saldırganların hedefi olabilir. Dolayısıyla, ilk yapılabilecek şey ağa katılmayı zorlaştırmaktır. Bunun için modemin varsayılan yapılandırmasını değiştirmek gerekmektedir. Değiştirilmesi gereken yapılandırma ayarları başlıca, varsayılan kullanıcı adı, varsayılan parola, varsayılan ağ adıdır.

2- Şifreleme Kullanılması: Kablosuz ağ trafiğinin şifrelenmesi için WPA2 (Wi-Fi Protected Access – Wi-Fi Korumalı Erişim) veya WPA3 şifrelemesi kullanılmalıdır. WEP gibi güncel olmayan protokoller içerdikleri zafiyetler sebebiyle kablosuz ağları güvensiz hale getirebilmektedir.

3- Güçlü Parolalar Kullanılması: Kablosuz ağa dahil olmak için gerekli olan parolayı güçlü seçmek, ağa dahil olmak isteyen saldırganın işini zorlaştıracaktır. Güçlü bir parola için tahmin edilmesi zor, büyük ve küçük harf, özel karakter ve sayıların kullanılması önerilmektedir.

4- Ağ Şifrelemesi Kullanımı: Kablosuz ağda iletilen trafik, zaten ağda olan kullanıcılar tarafından çeşitli durumlarda görülebilir. Dolayısıyla, özellikle kamuya açık kablosuz ağlarda, şifresiz protokoller kullanılmaması gerekmektedir. HTTPS (Hyper-Text Transfer Protocol Secure) gibi protokoller varsayılan olarak sunucu ve istemci arasındaki trafiğin şifrelenmesini sağladığı için bir seviye güvenlik katmaktadır. Ancak, HTTPS yerine HTTP kullanıldığı takdirde, sunucu ve istemci arasındaki trafik varsayılan olarak şifrelenmediği için ağı dinleyebilen bir saldırgan bu trafiği izleyebilir. Dolayısıyla, bu trafikte geçen gizli bir verinin ifşa olması oldukça muhtemeldir. Ancak, unutulmamalıdır ki, güvenmediğiniz bir ağ zaten saldırganların kontrolü altında olabileceği için, şifreleme kullanan bir protokol kullanmak da kesinlikle güvende olmayı sağlamaz. Kamuya açık ağlarda her zaman gizliliği ve mahremiyeti göz önünde bulundurarak hareket edilmelidir.

5- UPnP (Universal Plug and Play) ve WPS (Wi-Fi Protected Setup) Özelliklerinin Devre Dışı Bırakılması: Kablosuz ağlara bağlanmayı kolaylaştıran özellikler saldırganların da ağa kolay bağlanmasını sağlayabileceğinden, fiziksel koruması olmayan ortamlarda bu özelliklerin devre dışı bırakılması önerilmektedir.

6- Ağ Segmentasyonu Yapılması: Ağın rol ve sorumluluklara göre farklı sanal ağlara (Virtual Networks – VLAN) bölünmesi, bir sızma yaşandığında veri kaybını azaltıcı bir etki gösterecektir.

7- Cihaz Yazılımlarının Güncellenmesi: Her ağ cihazı gibi, zaman zaman kablosuz yönlendiricilerde de güvenlik açıklıkları keşfedilmektedir. Bu güvenlik açıklıkları, saldırganların çeşitli saldırılar yapabilmesine olanak sağlayabilmektedir. Bunu önlemek için, kablosuz yönlendirici üreticileri periyodik olarak güvenlik yamaları yayınlamaktadır. Bu yamaların takip edilmesi ve güncellenmesi, kablosuz yönlendiricilerdeki bilinen güvenlik açıklıklarının giderilmesini sağlayacaktır.

8- Uzaktan Yönetimin Devre Dışı Bırakılması: Kablosuz yönlendiricilerin uzaktan yönetilmesi eğer şart değilse, devre dışı bırakılmalıdır. Uzaktan yönetimin, saldırganın eline geçmesini engellemek için yönetimin yalnızca yerel ağdaki güvenilir cihazlardan yapılabilmesinin sağlanması iyi bir pratik olacaktır.

9- Saldırı Tespit Sistemleri (IDS – Intrusion Detection System) Kullanılması: Ağ trafiğindeki şüpheli hareketlerin tespit edilmesi ve olası güvenlik ihlallerine karşı izlemek için IDS'ler kullanılabilir.

10- MAC (Media Access Control – Ortam Erişimi Kontrolü) Filtrelemesinin Etkinleştirilmesi: Yalnızca, izin verilen bilgisayarların ağa dahil olmasını sağlayacak beyaz liste yaklaşımı uygulanabilir. Ancak dikkat edilmelidir ki, MAC adresleri taklit edilebilir ve bu yüzden bu yaklaşım kesin bir çözüm değildir. Yine fazladan bir seviye güvenlik sağlayacağı için saldırganın işini zorlaştırabilir.

11- Kullanıcıların Farkındalık Düzeylerinin Artırılması: Kablosuz ağ kullanıcılarının güvenlik için yapılabilecekleri öğrenmesi, daha iyi bir güvenlik duruşu sergilenmesini sağlayacaktır. Güvenlikteki en zayıf halka olan insanlar, alınan çok fazla sayıdaki güvenlik önleminin atlatılmasını sağlayıp ağınızı saldırılara açık hale getirebilir. Dolayısıyla kullanıcıların güvenlik farkındalığına sahip olması saldırıların başarılı olma ihtimalini azaltacaktır.

BAĞLI ARAÇLAR VE SİBER GÜVENLİK

Dr. Halil Kemal TAŞKIN

Bağlı Araç Nedir?

Bağlı araçlar, modern ulaşım teknolojisinin en yenilikçi ve hızla gelişen alanlarından biridir. Bağlı araçlar (connected cars), Internet erişimi olan, aynı zamanda diğer araçlarla da iletişime geçebilen, genellikle 4G ve 5G gibi kablosuz iletişim teknolojilerini kullanarak bilgi alışverişinde bulunabilen araçlara verilen genel isimdir. Sistem mühendisliği bakış açışı ile değerlendirdiğimizde, araçları sistemlerin sistemi olarak ifade edebiliriz. Bu durumda, bağlı araçlar sistemlerin sistemi olarak ele alındığında tasarımlarında sahip oldukları arayüzlerin çevresel etkileşimi dikkate alınmaktadır.

Bu tür araçlar, çeşitli sensörler ve iletişim cihazları ile donatılmıştır ve bu sayede gerçek zamanlı veri paylaşımı yapabilirler. Bağlı araçlar, sürücülere daha güvenli, daha verimli ve daha keyifli bir sürüş deneyimi sunmayı amaçlar.

Kişisel olarak kullanımı da giderek yaygınlaşmakla birlikte, bağlı araç teknolojileri, akıllı şehir projelerinde, filo yönetiminde, lojistik ve taşımacılıkta yaygın olarak kullanılmaktadır. Ayrıca, otomotiv endüstrisinde otonom sürüş teknolojilerinin gelişimi için de temel bir role sahiptir.

Araçların Bağlantı Arayüzleri

Bağlı araçlar, birçok farklı iletişim protokolü ve cihaz arasında veri alışverişinde bulunabilir. Bağlantı arayüzlerini iki temel alanda ifade edebiliriz. İlk olarak aracın kendi içinde ve kullanıcısı ile etkileşimde olduğu haberleşmenin yapıldığı arayüzler, ikinci olarak da aracın dış dünya ile haberleşme sağladığı arayüzler ele alınabilir.

Aracın dış dünya ile haberleşmeye geçebileceği arayüzleri tanımlamak için 3GPP ve 5GAA tarafından geliştirilen V2X (Vehicle-to-Everything) kavramını kullanabiliriz. V2X, araçların birbirleriyle, altyapıyla ve diğer çevresel unsurlarla iletişim kurmasını ifade eden bir kavramdır. Araç üzerinde bulunan Telematik Kontrol Birimi (TCU) bu haberleşmelerden sorumludur.

V2X haberleşmesi aşağıdaki dört ana başlık altında toplanmıştır.

1. V2N (Vehicle-to-Network) Haberleşme

Araçlar ile ağ arasındaki iletişimi ifade eder. V2N iletişimi, araçların internete ya da bulut tabanlı hizmetlere bağlanmasını sağlar. Bu, araçların üretici firma sunucusu ile bilgi paylaşımı, yazılım güncelleme, uzaktan araç kontrolü ve eğlence sistemi içeriklerine erişim gibi işlemleri yapmasına ve bu bilgileri kullanarak araç ve sürüş deneyiminin iyileştirilmesini hedefler.

2. V2I (Vehicle-to-Infrastructure) Haberleşme

Araçlar ile altyapı arasındaki iletişimi ifade eder. V2I iletişimi, araçların trafik ışıkları, yol işaretleri, yol kenarı üniteleri ve diğer altyapı elemanları gibi altyapı unsurlarıyla iletişim kurmasını sağlar. Bu, araçların trafik akışını optimize etmek, trafik sıkışıklıklarını azaltmak ya da trafik kazalarını önlemek için altyapıyla etkileşimde bulunmalarını hedefler.

3. V2V (Vehicle-to-Vehicle) Haberleşme

Araçlar arası iletişimi ifade eder. V2V iletişimi, araçların birbirlerine konum, hız, yön ve diğer güvenlik bilgilerini kablosuz olarak iletebilmesini sağlar. Bu, araçların çevresel tehlikeleri tespit etmek, kazaları önlemek ya da trafiği optimize etmek için birbirleriyle iletişim kurmalarını hedefler.

4. V2P (Vehicle-to-Pedestrian) Haberleşme

Araçlar ile yayalar arasındaki iletişimi ifade eder. V2P iletişimi, araçların yakındaki yayaları tespit etmesini ve onlara uyarılar göndermesini hedefler. V2P, araçların çevredeki yayaları fark etmeleri ve güvenli bir şekilde etkileşimde bulunmaları için tasarlanmıştır.

Bunlarla birlikte, artık birçok araçta bulunması zorunlu hale gelen e-Call acil çağrı sistemi de bu kapsamda değerlendirilebilir. e-Call sistemleri acil durumlarda otomatik ya da manuel tetiklenerek devreye giren ve 112 acil yardım merkezine otomatik bağlantı sağlayan sistemlerdir. Bu sistemler hem araç içi ses bağlantısı ile acil durum görevlisine bağlanmayı sağlayan hem de araç ile ilgili konum, hız vb. bilgileri yetkililere iletebilen yeteneklere sahiptir.

Bir diğer yandan, aracın kendi iç haberleşmesi ve kullanıcısı ile etkileşimde olması için kullandığı çeşitli arayüzler de mevcuttur. Bu arayüzleri Wi-Fi, Bluetooth, USB, Ethernet, elektrik şarj portu, OBD-II, araçların mobil uygulamaları, uzaktan kumanda haberleşmesi, Immobilizer arayüzü, GNSS alıcısı, kameralar, radar sistemleri, sensörler (TPMS vb.) ve araç içi ECU haberleşmesi (CAN hattı) şeklinde çeşitlendirmek mümkündür.

Emniyet ve Güvenlik

Araçlarda emniyet (safety) ve güvenlik (security) kavramları sıklıkla birbiri ile karıştırılmaktadır. Aslında iki kavram farklı yaklaşımları ele almaktadır.

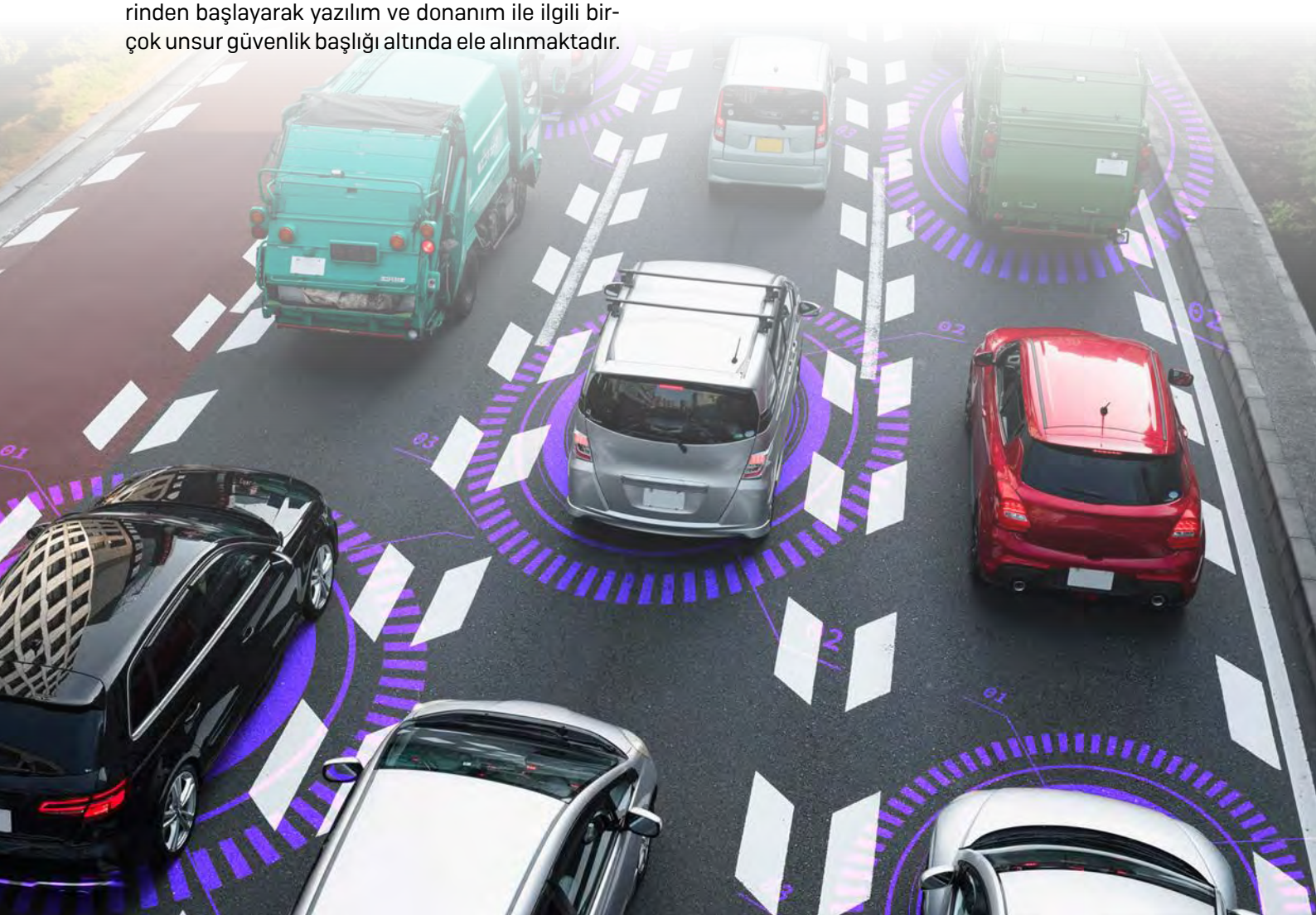
Emniyet, bir aracın içindeki veya dışındaki tehlikelerden korunma durumunu ifade etmektedir. Emniyet için öncelikli olan can güvenliğidir. Emniyet, kaza sonrası yaralanmaları ve maddi hasarı önlemeyi ya da azaltmayı amaçlar. Emniyet kemeri kullanımı, hava yastıkları, fren sistemleri, kaza önleme sistemleri ve e-Call gibi donanımlar emniyeti artırmaya yöneliktir.

Güvenlik ise temelinde aracın sistemlerinin siber tehditlere karşı korunma durumunu ifade etmektedir. Güvenlik, olası bir siber saldırısı sonrası aracın emniyetini korumak için alınan önlemleri de içerir. Bu doğrultuda aracın bilişim sistemlerini, yazılım ve donanımını siber saldırılara karşı korumayı amaçlar. Güvenli yazılım geliştirme süreçlerinden başlayarak yazılım ve donanım ile ilgili birçok unsur güvenlik başlığı altında ele alınmaktadır.

Örneğin, bir otonom sürüş esnasında sensörlerden ya da yazılımdan kaynaklı bir hatadan dolayı aracın tehlikeli bir manevra yapması emniyet sorunu olarak ele alınırken, otonom sürüş sistemine yönelik dışarıdan yapılan bir müdahale ile sistemin olması gerektiği gibi çalışmasının engellenmesi güvenlik sorunu olarak değerlendirilmektedir.

Emniyet fiziksel tehlikelere karşı korunmayı ifade ederken, güvenlik siber tehditlere karşı korunmayı ifade eder. Her ikisi de araçların, sürücülerin ve yolcuların güvenliğini sağlamayı amaçlar, ancak farklı risk alanlarına odaklanırlar. İdeal olarak, bir araç hem emniyet hem de güvenlik açısından yüksek standartlara sahip olmalıdır. Bu, sürücülerin ve yolcuların hem fiziksel hem de siber tehditlere karşı korunmasını sağlayarak güvenli bir sürüş deneyimi sunmayı hedefler.

Araçlarda emniyet kriterleri için ISO 26262 standardı takip edilirken, siber güvenlik ISO/SAE 21434 standardı ile takip edilmektedir.



Araçlarda Sistem Güvenliği Mühendisliği Uygulamaları

Sistem mühendisliği yaklaşımı ile araçları sistemlerin sistemi olarak ele aldığımızda araç tasarım ve geliştirme süreçleri sistem mühendisliği faaliyetleri kapsamında değerlendirilmektedir. Sistem mühendisliği süreçlerinde siber güvenlik çalışmaları sistem güvenliği mühendisliği ile tanımlanmaktadır. Sistem güvenliği mühendisliği, siber güvenlik risklerini kabul edilebilir seviyeye getirecek fiziki, idari ve teknolojik faaliyetlerin bütünü olarak tanımlanabilir. Bu doğrultuda, güvenlik açıklarını önceden belirlemek ve bu güvenlik açıklarıyla ilişkili riskleri en aza indirgemek için bilimsel ve mühendislik ilkelerini uygulamak sistem güvenliği mühendisliğinin en temel unsurlarından birisidir. Güvenlik gereksinimleri tasarım aşamasında belirlenmeli, sistemlerin iş ve görev başarım kriterlerini destekleyecek şekilde bütünleşik olarak ele alınmalıdır.

Sistem güvenlik mühendisliğinin amaçları aşağıda listelenmiştir:

1. Güvenli sistemler tasarlamak ve geliştirmek

2. Sistemlerin varsayılan güvenlik ayarlarında kullanılmasını sağlamak

3. Siber olgunluk ve siber direnç seviyesi yüksek sistemler tasarlamak

4. Güvenlik güvencesi sağlanmış sistemleri kullanıma sunmak

Bu amaçlar doğrultusunda özellikle yazılım geliştirme süreçlerinin siber güvenlik ön planda tutularak planlanması kritik önem arz etmektedir. Bu da güvenli yazılım geliştirme yaşam döngüsü kavramının önemini göstermektedir. Yazılım geliştirme yaşam döngüsü belirli temel adımları takip ederek, yazılımın gereksinimlerinin belirlenmesi aşamasından devreye alma aşamasına kadar süreçlerin tanımlanmasıdır. Güvenli yazılım geliştirme yaşam döngüsü ise, yazılım geliştirme yaşam döngüsünde her adımda güvenlik ile ilgili süreçlerin tanımlanmasıdır. Bununla birlikte, güvenliğin tasarım aşamasından itibaren başlaması ve sürekli olarak ele alınması da kritik önem arz etmektedir. Bu da özellikle DevSecOps kavramının önemini ön

plana çıkarmaktadır. Bu kapsamda özellikle statik uygulama güvenlik testleri (SAST), dinamik uygulama güvenlik testleri (DAST) ve yazılım bileşen analizi (SCA) süreçlerinin DevSecOps kurguları içinde sürekli olarak işletilmesi kritik öneme sahip olacaktır.

Bir diğer yandan, bağlı araçların siber tehdit yüzeyini oluşturan bağlantı arayüzlerini ele aldığımızda, araçlar sürekli olarak internete ve çevrelerindeki diğer ortamlara bağlı olacakları için siber güvenlik tehditlerine karşı açık olacaktır. Arayüzlerin çeşitliliği göz önüne alındığında her arayüz için alınması gereken siber güvenlik önlemleri farklılık gösterecektir. Bu da farklı siber güvenlik alanlarının bir arada çalışmasını gerektirecek yetkinlikler ile sağlanabilecektir.

Ayrıca, araç üreticisi olarak araçların V2N ağları üzerinden erişim sağladığı uygulama sunucuları da ayrı bir atak yüzeyi oluşturmaktadır. Uygulama sunucularına yönelik olarak gerçekleştirilecek siber saldırılar sonucunda birçok aracın saldırıdan etkilenmesi olası olacaktır.

Bağlı Araçlarda Siber Güvenliğe Yönelik Standartlar

Bağlı araçların siber güvenliği, kullanıcıların güvenliği ve veri gizliliği açısından kritik öneme sahiptir. Siber güvenlik standartları, bağlı araçların yazılım ve donanımındaki güvenlik açıklarının tespit edilmesi ve kapatılması için gerekli önlemleri belirler. Bu standartlar, araçların siber saldırılara karşı daha dirençli olmasını sağlar. Özellikle, kişisel veri olarak değerlendirilebilecek araç kullanım alışkanlıkları gibi verilerin buluta aktarılması ve işlenmesi süreçleri mahremiyet açısından kritik önem arz eder hale gelmiştir. Siber güvenlik standartları, araçların güvenliğini sağlamak için gerekli çerçeveleri ve rehberleri sunmaktadır. ISO/SAE 21434, UNECE WP.29 ve SAE J3061 gibi araçlar için özelleşmiş standartlar ve NIST Siber Güvenlik Çerçeve Programı gibi genel geçer rehberler araç üreticilerinin ve tedarikçilerinin uyum sağlaması gereken güvenlik gereksinimlerini belirler. Özellikle, ISO/SAE 21434 standardı, araç güvenliği ile ilgili süreçlerin sistem mühendisliği süreçleri ile birlikte yürütülmesine yönelik detayları belirtmektedir. Bu standartlara uyum, bağlı araçların siber saldırılara karşı korunmasını, veri gizliliğinin sağlanmasını ve küresel uyumluluk ve iş birliğinin teşvik edilmesini sağlar.

Elektrikli Araç Şarj Ekosistemi ve Siber Güvenlik

Elektrikli araçların hayatımıza girmesi ile birlikte elektrikli araç şarj altyapıları da yaygınlaşmaya başladı. Araçlar üzerinde bulunan şarj portu da siber güvenlik için yeni bir tehdit yüzeyi haline geldi.

Elektrikli araç sahiplerinin kullanacakları her şarj firması için ayrı bir yöntem kullanmaları gerekmektedir. Genel olarak birçok firma mobil uygulama hizmeti sunmakta ve kullanıcılar her uygulamaya kredi kartı bilgileri dahil kişisel bilgilerini girme durumunda kalmaktadır. Dolayısıyla, bu ekosistem içindeki her şarj firması da bir hedef haline gelmekte ve özellikle kişisel verilerin saklanmasına yönelik regülasyonlara uymaları önem arz etmektedir.

Bu doğrultuda, araç şarjı ekosistemini şarj istasyonları ve bu istasyonlarla araçlar arasındaki iletişim protokollerini içerecek şekilde iki temel başlık altında değerlendirebiliriz.

1. Şarj İstasyonları

Elektrikli araç şarj istasyonları hem enerji transferi hem de veri iletişimi sağlar. Bu istasyonlar, potansiyel olarak kötü niyetli saldırılara karşı savunmasız olabilir.

2. İletişim Protokolleri

Şarj işlemi sırasında kullanılan iletişim protokollerinin güvenliği, araç ve şarj istasyonu arasında güvenli bir veri alışverişi sağlamak için kritik öneme sahiptir. Özellikle bu alan için tasarlanan OCPP (Open Charge Point Protocol) gibi protokoller siber güvenlik araştırmacıları için yeni hedefler olarak değerlendirilebilir.

Elektrikli araç şarj ekosistemi, bağlı araç sistemlerinin önemli bir bileşeni haline gelmektedir. Dolayısıyla, bu ekosistemin siber güvenliği, kullanıcı güvenliği ve sistemin bütünlüğü için kritik öneme sahiptir. Bağlı araçların ve şarj ekosisteminin güvenliğini sağlamak için şifreleme, kimlik doğrulama, ağ güvenliği ve düzenli yazılım güncellemeleri gibi çeşitli siber güvenlik önlemleri uygulanmalıdır. Bu önlemler, sadece mevcut tehditlere karşı koruma sağlamakla kalmaz, aynı zamanda gelecekte ortaya çıkabilecek yeni tehditlere karşı da hazırlıklı olmayı sağlayacaktır. Siber güvenlik stratejilerinin de sürekli olarak güncellenmesi ve iyileştirilmesi gerekmektedir.

Otonom Sürüş, Veri Toplama ve Mahremiyet

Bağlı araçlar, sürekli olarak sensörler, kameralar ve diğer veri toplama cihazları aracılığıyla büyük miktarda veri üretir ve iletir. Bu veriler, sürüş alışkanlıklarından konum bilgilerine, araç performansından yol koşullarına kadar geniş bir yelpazeyi kapsar.

Bağlı araçların yaygınlaşması ile birlikte araçlardaki hata durumlarına yönelik uzaktan tespit ve müdahale yeteneklerinin geliştirilmesi de veri toplamanın bir boyutu olarak değerlendirilmektedir. Diagnostics over IP (DoIP, IP üzerinden Teşhis) protokolü ile araçlardaki mevcut hata teşhis ve izleme yetenekleri uzaktan da yapılabilmektedir.

Ancak, bu veri toplama süreci, mahremiyet sorunlarını da beraberinde getirmektedir. Toplanan veriler, kullanıcıların kişisel yaşamlarına dair hassas bilgileri içerebilir ve bu bilgilerin yetkisiz kişilerce ele geçirilmesi mahremiyet ihlallerine yol açabilir. Araç üreticileri ve veri hizmet sağlayıcıları, toplanan verileri üçüncü taraflarla paylaşabilir ya da üçüncü taraflara satabilir. Bu durum, kullanıcıların izni olmadan mahremiyetlerinin ihlal edilmesine neden olabilir. Kullanıcıların, araçlarının topladığı veriler hakkında yeterince bilgi sahibi olmaması ve bu verilere nasıl erişileceği veya kontrol edileceği konusunda bilinçli olmamaları, mahremiyet sorunlarını artırır. Dolayısıyla, kullanıcılar da verilerin toplanması ve işlenmesi konusunda rızalarını etkin bir şekilde takip ederek yönetmelidir, aksi durumlar mahremiyet ihlallerine yol açabilir. Ek olarak, toplanan verilerin anonimleştirilerek işlen-

mesi konusunda da firmaların gerekli açıklamaları yapmaları ve kullanıcıların bu konularda bilgilendirilmesi gerekmektedir.

Otonom sürüş, modern ulaşım teknolojisinin en heyecan verici ve çok hızlı ilerleme sağlanan yeniliklerinden biridir. Bu araçlar, yapay zeka, sensör ve görüntüleme teknolojileri sayesinde sürücü müdahalesi olmadan hareket edebilir. Bu noktada, birçok firma mevcut bağlı araç kullanıcılarının verilerini toplayarak yapay zeka çözümleri ile işlemekte ve otonom sürüş iyileştirme geliştirmelerinde kullanmaktadır. Kişisel verilerin işlenmesine yönelik mahremiyet problemi burada da dikkatli şekilde ele alınmalıdır.

Üreticiler, mahremiyet problemlerine çözüm için, veri maskeleme, veri anonimleştirme, gereksiz verilerin toplanmaması, verilerin şifrelenmesi, kullanıcıların verileri üzerinde kontrolü ve kullanıcılara karşı şeffaf olma, yasalara ve standartlara uyum ile sertifikasyon konularındaki politikalarını ve faaliyetlerini açık şekilde ifade etmelidirler.

Otonom sürüşün güvenli ve etkin bir şekilde çalışabilmesi için siber güvenliğin sağlanması kritik öneme sahiptir. Siber güvenlik açıkları, otonom sürüş sistemlerinde hatalara ve hatta kazalara neden olabilir. Bu noktada farklı başlıklar altında siber saldırılar gerçekleştirilebilir:

1. Yazılım güvenliği kaynaklı açıklıklar

Yazılım manipülasyonu ve kötü amaçlı yazılımlar, araçların normal çalışma düzenini bozarak ciddi hatalara ve kazalara yol açabilir. Araçların kontrol sistemlerine bulaşan kötü amaçlı yazılımlar, sistemin işleyişini bozarak sensör verilerini manipüle edebilir ve araçların yanlış kararlar almasına yol açabilir. Bu tür yazılımlar, kazalara neden olabilecek kritik hatalar yaratabilir.

2. Sensör manipülasyonu

Otonom araçlar, çevrelerini algılamak ve karar vermek için bir dizi sensör kullanır. Bu sensörlerden gelen verilerin manipüle edilmesi, araçların yanlış bilgilere dayalı kararlar almasına neden olabilir. GPS verilerinin yanıltılması, araçların yanlış konum bilgilerine dayanarak hareket etmesine yol açabilir. Bu durum, aracın rotasından sapmasına ve kazalara neden olabilir.

3. Haberleşmeye yönelik saldırılar

Otonom araçlar, diğer araçlarla ve trafik altyapısıyla iletişim kurarak daha güvenli ve verimli bir sürüş deneyimi sunmayı hedeflemektedir. Ancak, bu iletişim ağlarına yönelik saldırılar, sistemin işleyişini bozabilir ve kazalara yol açabilir. V2X haberleşmesinin kesilmesi, aracın çevresindeki durumları doğru bir şekilde değerlendirememesine neden olabilir. Bu durum, koordinasyon eksikliğine ve kazalara yol açabilir.

Yazılım manipülasyonu, sensör ve veri manipülasyonu, iletişim ağlarına yönelik saldırılar ve donanım-yazılım uyumsuzlukları gibi siber güvenlik kaynaklı problemler, otonom sürüş hatalarına ve kazalara neden olabilir. Bu tehditlerle başa çıkmak için, otonom araçların siber güvenliğini sağlamak amacıyla kapsamlı güvenlik önlemleri alınmalı ve sürekli olarak güncellenmelidir.

IOT (INTERNET OF THINGS) GÜVENLİĞİ

Halil UFUK

IoT cihazları, network ağına bağlanabilen ve veri işleme/iletme yeteneklerine sahip standart olmayan bilgi işleme cihazlarıdır. Akıllı ev/şehir cihazlarından kişisel asistanlara sürücüsüz arabalardan endüstriyel kontrol sistemlerine kadar geniş bir yelpazede yer almaktadır. Hayatımızın hemen hemen her noktasında yer alan ve doğrudan yaşam standartlarımıza etki eden bu cihazların ve içerisinde yer alan bilgilerin korunması kritik önem arz etmektedir.

IoT cihazlarına etki edebilecek başlıca tehditleri sıralayacak olursak:

Varsayılan Parola Kullanımı: Birçok IoT cihazı kolaylıkla tahmin edilebilen, Internet üzerinde bulunabilen, değiştirilmemiş varsayılan parolalar ile birlikte gelir. Bu durum onları Sözlük/Kaba Kuvvet saldırılarına karşı savunmamız hale getirir.

Güncellenmemiş Yazılımlar: IoT cihazları sayı fazlalıkları ve kaynak yetersizliklerinden dolayı genellikle uygulama/donanım güncelleme yönetimlerinin yapılmadığı cihazlardır. Bu durum cihazlarda bilinen zafiyetlerin (public vulnerabilities) ortaya çıkmasına sebep olup, onları güncel saldırılara karşı savunmasız bırakır.

Zayıf Şifreleme: IoT cihazları veri iletimi (data in transit) ve veri depolama (data at rest) aşamalarında gerek kaynak yetersizliği gerek zayıf algoritmalarının kullanımı nedeni Zayıf Şifreleme metotlarının kullanımı ya da hiç kullanılmaması, hassas verilerin gizliliğinin ve bütünlüğünün ihlaline yol açabilir.

Tedarik Zinciri Saldırıları: Üretim veya tedarik zinciri aşamalarında IoT cihazları ele geçirilebilir ve bu durum Tedarik Zincirinde yer alan firmalar güvenilir kabul edildiği sürece tespit edilemeyebilir.

Fiziksel Saldırılar: Korunmasız ortamlarda bulunan IoT cihazlarına fiziksel olarak erişim sağlanabilir. Cihazın içerisindeki verilere donanımsal bağlantılar ile ulaşılmaya çalışılabilir ya da IoT cihazının bağlı olduğu ağa sızılmaya çalışılabilir.

Kullanıcı Farkındalık/Eğitim Eksikliği: Birçok IoT kullanıcısı ve yöneticisi IoT cihazlarına genellikle operasyonel açıdan yaklaşmakta ve güvenlik sıkılaştırmaları ihmal edilebilmektedir.

Üçüncü Parti Uygulama/API Entegrasyonları: IoT cihazları genellikle Üçüncü parti uygulamalar ve API'lerle entegre olması nedeni ile bu uygulama/API'lerde ortaya çıkan zafiyetler, IoT cihazları için tehdit oluşturabilmektedir.

Gelişen Tehdit Modelleri: IoT cihazlarını ile ilgili sürekli yeni açıklar ve saldırı metotları (Sıfırıncı Gün Saldırıları) geliştirilmektedir. Hem barındırdığı bilgiler hem de BotNet ağları için başlıca kaynak olarak tercih edilmesi sebebi ile IoT cihazları saldırganların özellikle ilgisini çekmektedir.

IoT Güvenliği konusunda alınması gereken belli başlı güvenlik önlemleri sıralayacak olursak:

Güvenlik İlkeleriyle Tasarım

- Güvenliği Tasarıma Dahil Etme: IoT cihazları üretilirken güvenlik, temel bir tasarım ilkesi olarak ele alınmalıdır. Tasarım aşamasından başlayarak yazılım/donanım hayat döngüsünün her seviyesinde güvenlik önlemlerinin entegre edilmesini gerekmektedir.

- Minimum Yetki İlkesi (Principle of Least Privileged- PoLP): Cihazlar ve uygulamalar, yalnızca işlevlerini yerine getirmek için gerekli olan minimum erişim haklarına sahip olmalıdır. Bu, olası bir güvenlik ihlali durumunda zararın sınırlı kalmasını sağlar.

Erişim Kontrolü

- Authentication, Authorization, Accounting (AAA): Kimlik doğrulama, yetkilendirme ve aktivite izleme olarak adlandırılan AAA erişim kontrolleri mutlaka uygulanmalıdır. Sisteme erişim sağlayan her kullanıcının ayrı bir hesabı olmalı, görevi ölçüsünde ve PoLP çerçevesinde yetkilendirme yapılmalı ve kullanıcı aktiveleri kayıt altına alınmalıdır.

- Varsayılan Parola Kullanımı: Cihazlar ile birlikte gelen varsayılan parolalar, cihaz kullanımı sırasında mutlaka karmaşık parolalar (Ör: en az 10 karakter, büyük harf, küçük harf, rakam ve sembol içeren) ile değiştirilmeli ve parola değişimi düzenli aralıklar ile tekrarlanmalıdır. Parolalar şirket, kişi, proje vb. bilgileri içermemelidir.

Yama Yönetimi

- Yama Yönetimi: Güvenlik yamaları cihazların kritikliği ölçüsünde düzenli olarak uygulanmalıdır. Cihazların güncel kalması için ayrıca yama yönetim sistemleri kullanılabilir ya da güvenlik açıklarının hızlı gideril-

mesi için otomatik yazılım güncellemeleri aktif hale getirilebilir. Kritik sistemler için güncelleme işlemi personel gözetimde ve olası hata ya da servis kayıplarına karşı geri alma (roll-back) planları çerçevesinde gerçekleştirilmelidir.

Veri Koruma ve Şifreleme

- Veri Şifreleme: İletilen ve depolanan tüm hassas veriler, güçlü şifreleme standartları kullanılarak korunmalıdır. IoT cihazlarında mevcut olan kaynak yetersizliği nedeni ile zayıf şifreleme metotlarının kullanımı yaygındır. Bu nedenle bu konuya özellikle dikkat edilmelidir.

- Anonimleştirme/Pseudonimizasyon: Mümkün olduğunca kişisel verilerin anonimleştirilmesi, veri ihlallerinin etkisini azaltacaktır.

Ağ Güvenliği

- Ağ Segmentasyonu: Farklı cihaz ve hizmet türlerini ayırmak için ağ segmentasyonu kullanılmalıdır. Bu ayrım, olası güvenlik ihlalinin diğer sistemlere sıçramasını engeller.

- Güvenlik Duvarları ve Saldırı Tespit/Önleme (IPS/IDS) Sistemleri: Ağ trafiğini izlemek ve zararlı trafiği engellemek için güvenlik duvarları ve Saldırı Tespit/Önleme (IPS/IDS) Sistemleri kullanılmalıdır.

Olay Yanıt ve İzleme

- Sürekli İzleme ve Güvenlik Olaylarına Yanıt: Cihazlar ve ağlar, şüpheli etkinlikleri tespit etmek için sürekli olarak izlenmelidir. Güvenlik ihlalleri durumunda etkili olay yanıt planları devreye alınmalıdır.

- Güvenlik Olay Kayıtları: Güvenlik olaylarının kayıtları, analiz ve gelecekteki güvenlik stratejilerinin geliştirilmesi için saklanmalıdır. Olay Kayıtları, Güvenlik Bilgi ve Olay Yönetim (SIEM) yazılımları ile entegre edilerek güvenlik olayları korelasyona sokulabilir, bu sayede detaylı Güvenlik Olay analizleri yapılabilir.

Farkındalık ve Eğitim

- Kullanıcı Eğitimi ve Farkındalık Programları: IoT cihazlarının güvenli kullanımı konusunda kullanıcıların bilgilendirilmesi ve eğitilmesi, güvenlik risklerini azaltabilir.

- Geliştirici ve Yönetici Eğitimi: IoT cihazlarını ve sistemlerini geliştiren ve yöneten profesyoneller, güncel güvenlik uygulamaları ve tehditler konusunda eğitilmelidir.

Risk Değerlendirme ve Yönetimi

- Risk Değerlendirme Süreçleri: IoT sistemlerinin güvenliğini sağlamak için, potansiyel tehditlerin ve zayıflıkların sistematik bir şekilde değerlendirilmesi gerekir. Bu süreç, cihazların, ağların ve verilerin karşı karşıya olduğu riskleri belirlemeyi ve önceliklendirmeyi içerir.

- Kapsamlı Güvenlik Politikaları: İşletmeler, IoT cihazlarının ve sistemlerinin yönetimi için kapsamlı güvenlik politikaları ve prosedürleri geliştirmelidir. Bu politikalar, cihaz yönetimi, veri koruma ve erişim kontrolü gibi konuları kapsamalıdır.

Uluslararası Standart ve Kılavuzlar

IoT güvenliği ile ilgili daha detaylı bilgilere ulaşmak için aşağıda yer alan Standart ve kılavuzlardan yararlanılabilir.

– ISO/IEC 27400:2022 Cybersecurity – IoT security and privacy – Guidelines

– ISO/IEC 27402:2023 Cybersecurity – IoT security and privacy – Device baseline requirements

– ISO/IEC FDIS 27403 Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics

– ISO/IEC TR 30164:2020 – Internet of things (IoT) – Edge Computing

– NIST SP 800-213 IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements

– NIST SP 800-213A IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog

– NIST IR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

– NIST IR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers

– NIST IR 8259A IoT Device Cybersecurity Capability Core Baseline

– NIST IR 8259B IoT Non-Technical Supporting Capability Core Baseline

– NIST IR 8425 Profile of the IoT Core Baseline for Consumer IoT Products

BULUT BİLİŞİM GÜVENLİĞİ VE UYUM: ZORLUKLAR VE ÇÖZÜM ÖNERİLERİ

Hakan MUTLU

Bulut bilişim, işletmelerin ve bireylerin veri depolama, erişim ve işleme yöntemlerini dönüştürmüştür. Ayrıca, kaynak kullanımında büyük esneklikler ve maliyet avantajları sunarak, dijital yeni çağda veri yönetimini kolaylaştırmaktadır. Ancak, bulut bilişimin getirdiği bu yenilikler, aynı zamanda yeni güvenlik ve gizlilik zorluklarını da beraberinde getirmektedir. Bulut ortamları, çoklu kiracılı yapıları ve geniş coğrafi dağılımları nedeniyle, siber saldırılara karşı normalden daha fazla savunmasız olabilir. Bu nedenle, bulut teknolojisinin sağladığı avantajlardan tam olarak faydalanabilmek için, güvenlik tehditlerini anlamak ve bu tehditlere karşı etkili stratejiler geliştirmek şarttır. Bu yazıda, öncelikle bulut bilişimin gelişiminden bahsedeceğiz. Daha sonra bulut bilişim ortamlarının karşılaştığı başlıca güvenlik sorunları ve bu sorunlara yönelik çözüm önerilerini ele alacağız.

Bulut bilişiminin geçmişi 1960'lara kadar uzanır ve başlangıçta paylaşımlı hesaplama sunucularına uzaktan işlem girişinin popüler hale gelmesiyle başlar. Kullanıcıların yüksek hesaplama işlemlerini operatörlere göndererek sunucularda çalıştırılmasını sağladığı "veri merkezi" modeli, bu dönemde yaygın olarak kullanılmıştır. Bu durum, büyük ölçekli bilgi işlem gücünü zaman paylaşımı yoluyla daha fazla kullanıcıya sunma, altyapıyı, platformu ve uygulamaları optimize etme sonucunda son kullanıcılar için verimliliği artırma yöntemlerini araştırma sonucunda bulut bilişimin temelini oluşturdu.

"Bulut" kelimesinin kullanımı, 1994 yılına dayanır ve General Magic tarafından telekomünikasyon ortamındaki mobil cihazların "gidebileceği yerler" evreni için kullanılmıştır. David Hoffman tarafından önerilmiş olan bu terim ağ ve telekomünikasyon alanında uzun süre kullanılmıştır. "Bulut bilişim" terimi ise 1996 yılında Compaq tarafından, bir iş planı hazırlarken daha yaygın bir şekilde kullanılmaya başlanmıştır. Compaq, "Bulut Bilişimde Etkin Uygulamalar" ile satışları hızlandırmayı amaçlamış ve çevrimiçi dosya depolamanın ticari olarak başarılı olacağını öngörmüştür. Bu durum, şirketin sunucu donanımlarını İnternet servis sağlayıcılarına satmasını sağlamıştır.

2000'li yıllarda, bulut bilişimin günümüzdekine yakın uygulanması şekil almaya başladı. 2000'li yılların başında Amazon şirketinin kendi iç bilişim ihtiyaçlarını karşılamak için kurduğu altyapının ortalama olarak %10'unu kullanıyordu. Şirket bu hazırda bekleyen kaynakları bilgi işlem servisi olarak kiralamak için 2002 yılında Amazon Web Services (AWS)'i kurdu ve bu çalışma modeliyle geliştiricilere bağımsız olarak uygulamalar oluşturma im-

kânı da tanıdı. 2006 yılında Google Docs'un beta sürümü piyasaya sürüldü. 2008 yılında ise Amazon Simple Storage Service, yani Amazon S3 ve Amazon Elastic Compute Cloud (EC2) hizmetleri sunuldu. Bununla birlikte asıl buluş S3 için geliştirilen fiyatlandırma modeliydi, kullandıkça öde modeli şu an bulut hizmetleri fiyatlandırılmasında fiili standart olmuştur. Ayrıca, NASA, özel ve hibrit bulutlar için ilk açık kaynaklı yazılımı geliştirdi.

2010'lu yıllarda bulut bilişim, büyük bir ivme kazanarak birçok alanda yaygınlaştı. Bulut bilişim hizmetleri, IaaS(Infrastructure as a Service, Hizmet Olarak Altyapı), PaaS(Platform as a Service, Hizmet Olarak Platform) ve SaaS(Software as a Service, Hizmet Olarak Yazılım) gibi farklı modellerde daha fazla çeşitlendi. Bulut tabanlı depolama, hesaplama, veritabanı yönetimi, yapay zekâ, makine öğrenmesi, IoT ve daha birçok alanda yeni hizmetler sunulmaya başlandı. Bulut bilişim sağlayıcıları arasındaki rekabet arttı ve küresel olarak büyümeye devam ettiler. Amazon Web Services, Microsoft Azure, Google Cloud Platform (GCP) gibi büyük sağlayıcılar, pazarın büyük bir kısmını elinde tutmaya devam etti. Günümüzde, bulut bilişim halen hızla büyümeye devam ediyor ve birçok işletme, dijital dönüşüm stratejilerinin merkezine bulut teknolojilerini yerleştiriyor. Veri analitiği, yapay zekâ, IoT ve diğer yenilikçi teknolojilerle birleştirilerek, bulut bilişim daha da güçlü bir konuma gelmektedir. Ayrıca, COVID-19 salgını gibi olaylar, uzaktan çalışma ve dijital iş süreçlerinin daha da yaygınlaşmasına ve bulut bilişimin öneminin artmasına neden olmuştur. Bu nedenle, bulut bilişimin önümüzdeki yıllarda bilişim sektöründe daha da büyük bir rol oynaması beklenmektedir.

Bulut bilişim, teknolojik ilerlemelerle birlikte bazı önemli endişeleri de beraberinde getirmiştir. Özellikle verilerin bulut sağlayıcıları aracılığıyla saklanması ve kaynakların paylaşımlı olarak kullanılması, güvenlik ve gizlilik konularında çeşitli kaygılara yol açmaktadır. Kritik bilgilerin başka bir şirkete teslim edilmesi, birçok kişi ve kurum için rahatsızlık verici bir durum olabilir. Bulut bilişim sistemlerine geçiş yapmakta tereddüt eden şirketlerin veri yöneticileri, bilgilerinin bir başkasının kontrolünde olmasından dolayı endişe duymaktadırlar.

Bulut bilişim modeli, barındırma şirketi ile kullanıcı arasındaki iletişimi ve depolanan bilgiyi yasal veya yasa dışı bir şekilde görüntüleyebilen bulut hizmeti sağlayıcıları sebebiyle gizlilik hakkının ihlal edildiğini düşünenlerce eleştirilmektedir. 2013 yılında Edward Snowden adlı eski bir NSA çalışanının kamuoyuna sızdırdığı bilgilerde, NSA'nın Amerikan telekomünikasyon şirketleriyle iş birliği yaparak geniş kapsamlı bir telefon ve internet trafiği izleme programı yürüttüğü ortaya çıkmıştır. Bu programlar, Amerikan vatandaşlarının iletişim verilerini izlemeyi içermekteydi. Bulut hizmet sağlayıcılarıyla ilgili kritik nokta, müşteri veya kullanıcının verisinin aynı sistemde (sunucu üzerinde) kalmayabileceği ya da aynı veri merkezinde, hatta aynı sağlayıcının bulutunda bulunmayabileceğidir. Bununla birlikte yasal ortamları uyumlu hale getirmek için yapılan çabalar bulunmaktadır.

Amazon gibi sağlayıcılar, ABD ve Avrupa Birliği gibi büyük marketlere yerel altyapı yerleştirerek ve müşterilere erişilebilirlik alanlarını seçmesine izin vererek hizmet sağlamaya devam etmektedir.

Buna karşın, bulut bilişim gizlilik endişelerini tam olarak gidememiştir. Çünkü hizmet sağlayıcıları bulut üzerinde bulunan veriye istedikleri zaman erişebilir, hatta kazayla veya kasıtlı olarak bu verileri değiştirebilir veya silebilirler. Bu sorunlar ve endişeler nedeniyle, bulut bilişimde uyum, çeşitli düzenleyici ve yasal gerekliliklere uyma zorluğunu beraberinde getirmektedir. İşletmeler, bulut hizmetlerini kullanarak veri depoladıkça ve işledikçe, faaliyet gösterdikleri endüstri ve bölgelere göre yasalara ve standartlara uyum sağlamak zorundadır. Veri koruma ve gizlilik yasaları, farklı ülkelerde değişiklik göstermektedir. Örneğin, Avrupa Birliği'nde Genel Veri Koruma Tüzüğü (GDPR), Amerika Birleşik Devletleri'nde California Tüketici Gizlilik Yasası (CCPA) ve Türkiye'de Kişisel Verilerin Korunması Kanunu (KVKK) gibi düzenlemeler bulunmaktadır. Ayrıca, sağlık, finansal hizmetler ve kamu sektörü gibi belirli alanlar için özel düzenlemeler bulunmaktadır; örneğin, ABD'deki sağlık kuruluşları Sağlık Sigortası Taşınabilirliği ve Sorumluluk Yasası'na (HIPAA) uymak zorundadır.

Birçok ülke, sınırları içerisinde üretilen verilerin yerel olarak saklanmasını zorunlu kılarak, bulut hizmetlerinin kullanımında veri egemenliği yasalarına uyulmasını talep etmektedir. Bu, özellikle verilerin farklı ülkelerdeki veri merkezlerinde saklandığı durumlarda, yasalara aykırılıkların ortaya çıkmasına neden olabilir. Ayrıca, şirketlerin ISO 27001 gibi bilgi güvenliği yönetimi standartlarına, NIST çerçevelerine veya PCI DSS gibi ödeme verilerinin güvenliği standartlarına uyum sağlaması gerekmektedir. Bu uyum, bulut hizmet sağlayıcılarıyla yapılan sözleşmelerde ve hizmet seviyesi anlaşmalarında (SLA, Service Level Agreement) belirtilen güvenlik önlemleri, veri işleme uygulamaları ve belirli düzenlemelere uyum konularında net rollerin ve sorumlulukların tanımlanmasını da içerir.

Uyumun sürekli olarak sağlanması için düzenli denetimler şarttır, fakat bulut ortamındaki denetimler, hizmetlerin dağıtık doğası nedeniyle karmaşık olabilir. Bu nedenle, bulut hizmetlerinin uyumunu doğrulamak amacıyla üçüncü taraf denetçiler tarafından sertifikasyonlar gerekebilir. Ayrıca, birçok kuruluş birden fazla bulut sağlayıcıdan hizmet aldığı için, farklı sağlayıcıların sunduğu değişik uyum standartları ve uygulamaları yönetmek zorlaşabilir. Bu, tüm platformlarda tutarlı bir uyumun sağlanmasını güçleştirir. Bu tür uyum zorluklarını etkili bir şekilde yönetebilmek için, düzenleyici çerçeve ve bulut hizmet sağlayıcılarının teknik yetenekleri hakkında derinlemesine bir anlayış gereklidir. Şirketler, genellikle kapsamlı yönetim ve uyum yönetimi programları uygulamakta, uyuma özgü araçlar kullanmakta ve bu karmaşıklıkları etkin bir şekilde yönetmek için hukuk ve bulut bilişim uzmanlarından rehberlik almak zorundadır. Bu çabalar, bulut bilişimde güvenliği ve gizliliği maksimize ederek hem işletmelerin hem de son kullanıcıların çıkarlarını korumaya yöneliktir.

Bulut bilişimde veri bütünlüğü, verilerin yetkisiz veya istenmeyen değişikliklere uğramadan korunmasını sağlamak amacıyla büyük önem taşır ve bu alanda karşılaşılan zorluklar oldukça çeşitlidir. Özellikle bulut ortamlarında, çok sayıda kullanıcının verilere erişim yetkisi olması, verilerin kasıtlı veya kasıtsız olarak yetkisiz değişikliklere uğramasına neden olabilir. Kullanıcı hataları sonucunda veriler yanlışlıkla değiştirilebilir veya silinebilir ve bu tür hatalar bulut ortamlarında geniş çapta etkiler yaratabilir. Ayrıca, bulut hizmetlerinin çoğunlukla API(Application Programming Interface, Uygulama Programlama Arabirimi)'ler aracılığıyla yönetilmesi, API güvenlik zafiyetlerinin kötü niyetli kişiler tarafından veri bütünlüğüne zarar vermek için kullanılmasına yol açabilir. Çok sayıda kullanıcı aynı veri kümeleri üzerinde çalıştığında, eşzamanlılık kontrollerinin yetersiz olması da veri bütünlüğünü bozabilir.

Bu tür zorluklarla başa çıkmak için bulut bilişimde veri bütünlüğünün korunması adına alınabilecek önlemler birden fazla katmandan oluşur. İlk olarak, erişim kontrolü mekanizmalarını güçlendirerek kullanıcıların verilere erişim düzeylerini sıkı bir şekilde yönetmek ve denetlemek önemlidir; bu yaklaşım, yetkisiz değişiklikleri önleyebilir.

İkinci olarak, kullanıcı hatalarını minimize etmek amacıyla veri işleme işlemleri sırasında otomatik kontroller ve doğrulamaların uygulanması gerekir; bu kontroller, yanlış veri girişini veya kazara silinmeleri önlemeye yardımcı olabilir. API güvenliği de bulut servislerinin güvenli bir şekilde yönetilmesi için kritik bir önem taşımaktadır; bu nedenle, API'lerin güvenliği için düzenli güvenlik taramaları yapılmalı ve güvenlik açıklarını hızla gidermek için güncellemeler uygulanmalıdır. Son olarak, veri bütünlüğünü bozabilecek eşzamanlılık sorunlarına karşı, işlem kilitleme veya versiyon kontrol sistemleri gibi tekniklerin kullanılması faydalı olacaktır. Bu tür önlemler, bulut ortamında veri bütünlüğünü etkin bir şekilde korumak ve yönetmek için oldukça önemlidir.

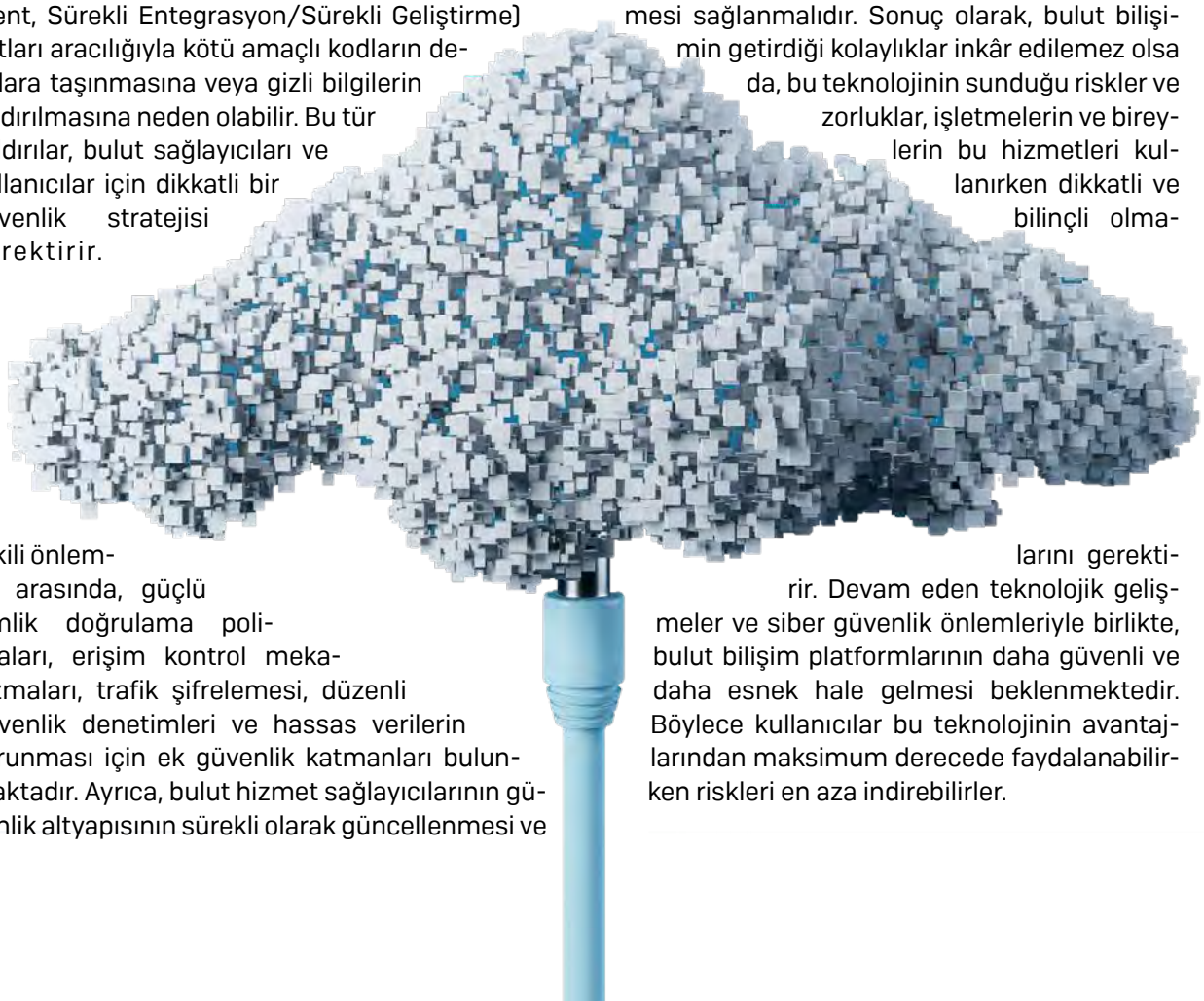
Bulut bilişimde erişilebilirlik, kullanıcıların ihtiyaç duydukları anda verilere sürekli ve güvenilir şekilde erişebilmesini sağlamayı amaçlar; fakat bu alanda çeşitli zorluklarla karşılaşılmaktadır. Bulut hizmet sağlayıcıları genellikle yüksek erişilebilirlik oranları sunsa da donanım arızaları, yazılım hataları, doğal afetler veya siber saldırılar gibi faktörler zaman zaman kesintilere neden olabilir. Bulut hizmetlerine çoğunlukla internet üzerinden erişildiği için, ağ bağlantı problemleri de erişilebilirliği doğrudan etkileyebilir. Örneğin, ağ yavaşlamaları veya kesintileri, bulut servislerine erişimi geçici olarak engelleyebilir. Ayrıca, bulut sağlayıcılarının talep artışlarını doğru bir şekilde öngörememesi veya buna uygun ölçeklendirme yapamaması, servislerin erişilebilirliğini olumsuz etkileyebilir. Dağıtık hizmet reddi (DDoS, Distributed Denial of Service, Dağıtık Servis Kesintisi) saldırıları gibi siber saldırılar da bulut hizmetlerine yapılan erişimi engelleyerek ciddi sorunlara neden olabilir.

Bu sorunlarla başa çıkmak için alınması gereken güvenlik önlemleri arasında veri şifreleme, düzenli yedeklemeler, kapsamlı yetkilendirme ve kimlik doğrulama yöntemleri, etkin trafik yönetimi ve DDoS koruma mekanizmaları bulunmaktadır. Ayrıca, bulut sağlayıcıların hizmet seviyesi anlaşmalarının (SLA) detaylarına dikkat edilerek, bu anlaşmaların gerektiğinde yeterli hizmet kalitesi ve sürekliliğini garanti ettiğinden emin olunması önemlidir. Böylece, bulut bilişimde erişilebilirlik hem teknik hem de sözleşmesel yollarla desteklenmiş olur, kullanıcıların ve işletmelerin bu hizmetlerden maksimum fayda sağlaması için gerekli zemin hazırlanır.

Bulut bilişim ortamları, özgün yapısı sebebiyle çeşitli benzersiz siber saldırılara maruz kalmakta ve bu durum, bulutun paylaşılan kaynak yapısı ve hizmet modellerine özgü risklerden kaynaklanmaktadır. Yan Kanal Saldırıları gibi saldırılar, çoklu kiracılı bulut ortamlarında gerçekleşir ve saldırganlar, bir sanal makinedeki işlemleri analiz ederek başka bir kiracının sanal makinesindeki hassas bilgilere erişmeye çalışır. Örneğin, bir saldırgan işlem yüküne göre sanal makinedeki kriptografik anahtarları çıkarmaya çalışabilir. Ayrıca, Sanal Makinadan Kaçış saldırıları, saldırganların kendi sanal makine ortamlarından çıkarak, bulut ortamındaki diğer kiracıların kaynaklarına veya altta yatan ana sisteme yetkisiz erişim sağlamasını içerir. Bu durum genellikle izolasyon mekanizmalarının zayıflığından kaynaklanır ve ciddi güvenlik ihlallerine yol açabilir.

Bulut servislerinin API'ler aracılığıyla yönetilmesi, güvensiz API'lerin veri ihlallerine, yetkisiz erişimlere ve hizmet yönetimi ile ilgili diğer saldırılara açık kapı bırakmasına neden olabilir. Kötü niyetli kişiler bu API'leri kullanarak verilere erişebilir veya bulut kaynaklarını kötüye kullanabilir. Man-in-the-Cloud(Buluttaki Aradaki Adam) saldırıları, genellikle kimlik avı saldırıları veya zararlı yazılımlar aracılığıyla gerçekleşir ve saldırganlar, kullanıcıların bulut hizmetlerindeki oturum açma bilgilerini ele geçirerek bulut kaynaklarına erişim sağlayabilir. Ayrıca, veri manipülasyonu saldırıları, bulut ortamındaki verilerin gizlice değiştirilmesi veya bozulmasıyla ilişkilidir ve saldırganlar bu yöntemle verileri manipüle ederek yanlış iş süreçleri veya kararlar alınmasına sebep olabilir.

Çerez Zehirleme (Cookie Poisoning) saldırıları, bulut uygulamalarında çerezlere zararlı içerik enjekte edilerek kullanıcı bilgilerinin kötüye kullanılmasını içerir. Bulut Kod Zinciri Saldırıları ise, saldırganların kod teslim zincirlerini hedef alarak, güvensiz versiyon kontrol sistemleri veya CI/CD(Continuous Integration/Continuous Development, Sürekli Entegrasyon/Sürekli Geliştirme) hatları aracılığıyla kötü amaçlı kodların depolara taşınmasına veya gizli bilgilerin sızdırılmasına neden olabilir. Bu tür saldırılar, bulut sağlayıcıları ve kullanıcılar için dikkatli bir güvenlik stratejisi gerektirir.



Etkili önlemler arasında, güçlü kimlik doğrulama politikaları, erişim kontrol mekanizmaları, trafik şifrelemesi, düzenli güvenlik denetimleri ve hassas verilerin korunması için ek güvenlik katmanları bulunmaktadır. Ayrıca, bulut hizmet sağlayıcılarının güvenlik altyapısının sürekli olarak güncellenmesi ve iyileştirilmesi, bu tür siber tehditlere karşı korunmada hayati öneme sahiptir.

Bulut bilişim, modern iş dünyasının vazgeçilmez bir parçası haline gelmiştir ve sayısız avantaj sunarken, aynı zamanda ciddi güvenlik ve gizlilik sorunlarına da yol açmaktadır. Bu teknoloji, veri erişimini kolaylaştırıp iş süreçlerini hızlandırsa da verilerin korunması ve yönetimi konusunda karmaşık zorluklar ortaya çıkarabilmektedir. Özellikle veri egemenliği, bulut sağlayıcılar arası geçişlerde uyum sorunları ve farklı ülkelerdeki veri koruma yasalarına riayet etme zorunluluğu, işletmeler için önemli endişe kaynaklarıdır. Bulut sağlayıcıları ve kullanıcılar, sürekli güvenlik tehditleriyle mücadele etmek zorunda kaldığından, etkili bir güvenlik stratejisi uygulamak zorunlu hale gelmiştir. Bu strateji, güçlü kimlik doğrulama politikaları, erişim kontrol mekanizmaları, trafik şifrelemesi, düzenli güvenlik denetimleri ve veri bütünlüğünü korumaya yönelik önlemleri içermelidir. Aynı zamanda, bulut sağlayıcılarının hizmet seviyesi anlaşmaları detaylı bir şekilde incelenmeli ve bu anlaşmaların yeterli hizmet kalitesi ve sürekliliğini garanti etmesi sağlanmalıdır. Sonuç olarak, bulut bilişimin getirdiği kolaylıklar inkâr edilemez olsa da, bu teknolojinin sunduğu riskler ve zorluklar, işletmelerin ve bireylerin bu hizmetleri kullanırken dikkatli ve bilinçli olmalarını gerektirir. Devam eden teknolojik gelişmeler ve siber güvenlik önlemleriyle birlikte, bulut bilişim platformlarının daha güvenli ve daha esnek hale gelmesi beklenmektedir. Böylece kullanıcılar bu teknolojinin avantajlarından maksimum derecede faydalanabilirken riskleri en aza indirebilirler.

KUBERNETES ALTYAPILARINDA GÜVENLİK DENETİMİ VE İZLEME

Dr. Adnan KILIÇ

1. Kubernetes'in Genel Bakışı ve Modern Altyapıdaki Önemi

Kubernetes, kısa ismiyle K8s, Google tarafından geliştirilen ve şu anda Cloud Native Computing Foundation (CNCF) tarafından sürdürülen açık kaynaklı bir konteyner orkestrasyon platformudur. Konteynerleştirilmiş uygulamaların dağıtımını, ölçeklenmesini ve yönetimini otomatikleştirmesi modern bulut tabanlı geliştirme için önemli bir araç olmasını sağlamaktadır. Kubernetes, otomatik dağıtım ve geri alma, yük dengeleme ve kendi kendini iyileştirme mekanizmaları gibi özelliklerle dağıtık sistemleri dayanıklı bir şekilde çalıştırmak için sağlam bir altyapı sağlar.

Günümüzün BT ortamında, mikroservis mimarisine geçiş ve hızlı geliştirme döngüleri ihtiyacı, Kubernetes'i birçok kuruluş için kritik bir bileşen haline getirmiştir. Geliştiricilerin uygulamaları daha verimli ve tutarlı bir şekilde dağıtmasına ve yönetmesine olanak tanıması yüksek tempolu bir ortamda rekabet avantajını korumak için önemlidir.

Kubernetes, modern altyapılar için başta aşağıdaki nedenlerden dolayı önemli hale gelmiştir:

- **Ölçeklenebilirlik:** Uygulamaları talebe göre otomatik olarak ölçekler.
- **Taşınabilirlik:** Yerel veri merkezlerinden bulutlara kadar çeşitli ortamlarda çalışır.
- **Verimlilik:** Kaynak kullanımını optimize eder, yükü dengeler ve iş yüklerini verimli bir şekilde yönetir.
- **Geliştirici Verimliliği:** Geliştirme ve dağıtım süreçlerini hızlandırır, üretime çıkış süresini kısaltır.

1.1 Kubernetes Altyapılarında Güvenlik Denetimi ve İzlemenin Önemi

Kubernetes'in benimsenmesi arttıkça, bu ortamların güvenliğinin sağlanmasının önemi de artmaktadır. Kubernetes kümelerinin genellikle hassas verileri ve kritik uygulama iş yüklerini yönetiyor olması siber saldırılar için çekici hedefler haline gelmelerine sebep olmuştur. Bu kümelerin güvenliğini sağlamak, veri ihlallerine, hizmet kesintilerine ve diğer kötü niyetli faaliyetlere karşı korunmak için hayati önem taşımaktadır.

Güvenlik denetimi, bir Kubernetes ortamının güvenliğini sistematik olarak gözden geçirmeyi ve değerlendirmeyi, potansiyel güvenlik açıklarını belirlemeyi ve güvenlik politikaları ile standartlarına uyum sağlamayı içerir. İzleme ise, kümenin performansını ve güvenlik durumunu sürekli olarak gözlemlemeyi ve anormalliklere gerçek zamanlı olarak yanıt vermeyi içerir. Denetim ve izleme, organizasyonların Kubernetes altyapılarını ortaya çıkan tehditlere karşı korumasına olanak tanıyan proaktif bir güvenlik stratejisinin temelini oluşturur.

Kubernetes'te denetim aşağıdaki nedenlerden önemlidir:

- **Uyumluluk:** Kümenin endüstri standartlarına ve yasal gerekliliklere uyumunu sağlamak.
- **Güvenlik Açığı Tespiti:** Yanlış yapılandırmaları ve saldırganlar tarafından istismar edilebilecek güvenlik açıklarını tespit etmek.
- **Risk Yönetimi:** Konteynerleştirilmiş uygulamaların çalıştırılmasıyla ilgili riskleri değerlendirmek ve hafifletmek.

Etkili izleme, aşağıdaki gereksinimleri sağlar:

Erken Tespit: Şüpheli faaliyetlerin ve potansiyel güvenlik olaylarının hızla tespit edilmesi.

Operasyonel İçgörüler: Kaynak kullanım örüntülerinin anlaşılması ve performansın optimize edilmesi.

Olay Yanıtı: Tespit edilen anormalliklere ve ihlallere hızlı yanıt verilmesi.

2. Kubernetes Altyapısı

2.1 Temel Kavramlar

Kubernetes, konteynerleştirilmiş uygulamaları verimli bir şekilde yönetmek ve organize etmek için podlar, servisler, dağıtımlar ve alan adları gibi birkaç temel kavramı barındırır.

2.1.1 Podlar

Pod, Kubernetes'te dağıtılabilir en küçük birimdir. Bir veya daha fazla konteyneri, depolama kaynaklarını, benzersiz bir ağ IP'sini ve konteyner(ler)in nasıl çalıştırılacağını yöneten seçenekleri kapsar. Podlar geçicidir, oluşturulabilir ve yok edilebilirler. Kısa ömürlü olacak şekilde tasarlanmışlardır ve başarısız olmaları durumunda değiştirilirler. Podlar, bir uygulamanın tek bir örneğini, toplu bir işi veya daha büyük bir uygulamanın bir bileşenini çalıştırmak için kullanılırlar.

2.1.2 Servisler

Servisler, bir dizi pod'u soyutlar ve bunlara erişim için sabit bir uç nokta sağlar. Bu soyutlama, ön ucu arka uçtan ayırır ve arka uç podlarının ölçeklendirilmesine veya değiştirilmesine olanak tanır. Servis türleri arasında ClusterIP, NodePort, LoadBalancer ve ExternalName bulunur.

2.1.3 Dağıtımlar

Dağıtımlar, podların ve ReplicaSet'lerin dağıtımını yönetir, istenen sayıda replikanın her zaman çalışmasını sağlar. Kubernetes dağıtımları, uygulamaların kolayca güncellenmesini ve geri alınmasını sağlayan rollout ve rollback özelliklerine sahiptir. Ayrıca, pod replikalarının talebe göre dinamik olarak ayarlanmasını sağlayarak ölçeklendirmeyi destekler. Ek olarak, Kubernetes, başarısız veya sağlıksız podları otomatik olarak değiştirerek uygulama kullanılabilirliğini ve performansını koruyan kendi kendini iyileştirme yetenekleri sağlar.

2.1.4 Alan Adları

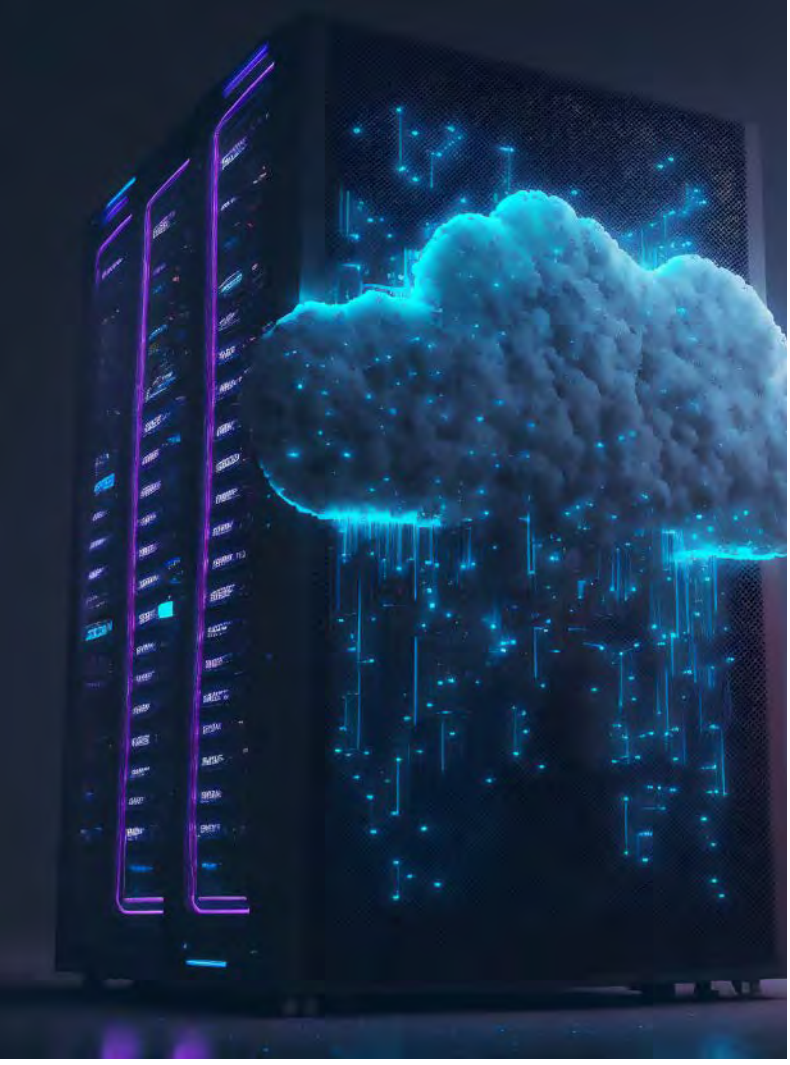
Alan adları, küme kaynaklarını birden fazla kullanıcı ve ekip arasında bölünmesini sağlar. Birçok kullanıcıya yayılan büyük ekiplerin veya projelerin bulunduğu ortamlarda kullanılması amaçlanmıştır. Alan adları, geliştirme ve üretim gibi ortamları ayırmak, uygulamaları veya hizmetleri izole etmek ve kaynak kotalarını yönetmek için kullanılabilir.

2.2 Kubernetes Mimarisi

Kubernetes mimarisi, kümenin durumunu yönetmek ve uygulamaların düzgün çalışmasını sağlamak için birlikte çalışan ana bileşenler ve düğüm bileşenlerinden oluşur.

2.2.1 Ana Bileşenler

- **API Sunucusu:** Kubernetes kontrol düzleminin ön yüzüdür. Küme ile etkileşimde bulunmak için birincil arayüz olan Kubernetes API'sini sunar. Tüm yönetim görevleri API sunucusu aracılığıyla gerçekleştirilir, dolayısıyla Kubernetes mimarisi içindeki iletişimin merkezi konumundadır.
- **etcd:** Tüm küme verileri için Kubernetes'in destek deposu olarak kullanılan tutarlı ve yüksek erişilebilirlikte bir anahtar-değer deposudur. Verilerin güvenilir bir şekilde depolanmasını ve hata durumunda bile alınabilmesini sağlayan tüm yapılandırma verileri etcd'de saklanır.
- **Scheduler:** İş yükünü düğümler arasında dağıtmaktan sorumludur. Yeni podların yerleştirilmesi için uygun düğümleri, kaynak kullanılabilirliği ve benzeri kısıtlamalar gibi diğer faktörlere dayanarak belirler.
- **Controller Manager:** Kontrolcü işlemleri çalıştırır. Kontrolcüler, küme durumu istenen durumdan saptığında fark etme ve yanıt verme sorumluluğundadır. Örnekler arasında belirli sayıda pod replikasının çalışmasını sağlayan replika kontrolcüsü ve düğüm durumunu ve yaşam döngüsünü yöneten düğüm kontrolcüsü bulunur.



2.2.2 Düğüm Bileşenleri

- **Container Runtime:** Konteynerleri çalıştırmaktan sorumlu yazılımdır. Kubernetes, docker, containerd ve CRI-O gibi birden çok konteyner çalışma ortamını destekler.
- **Kubelet:** Kümedeki her düğümde çalışan bir ajandır. Bir podda konteynerlerin çalışmasını sağlar. Kubelet, konteyner yaşam döngüsünü yönetmek için konteyner çalışma ortamı ile etkileşime girer.
- **Kube-proxy:** Her düğümde çalışan bir ağ vekilidir. Düğümler üzerindeki ağ kurallarını korur ve kümenin içindeki veya dışındaki ağ oturumlarından podlara iletişimi sağlar.

2.3 Ortak Kullanım Durumları ve Dağıtım Senaryoları

Kubernetes, mikroservis mimarisi, CI/CD hatları, hibrit ve çoklu bulut dağıtımları, büyük veri ve makine öğrenimi iş yükleri gibi çeşitli kullanım durumlarını destekleyen çok yönlü bir platformdur.

2.3.1 Mikroservis Mimarisi

Kubernetes, çok sayıda hizmeti yönetme ve bunların etkili bir şekilde iletişim kurmasını sağlama yeteneği sayesinde mikroservisleri çalıştırmaya uygundur. Her mikroservis, kendi pod'unda çalışabilir, servisler bunları soyutlayabilir ve dağıtımlar ile yaşam döngülerini yönetebilir.

2.3.2 CI/CD Hatları

Kubernetes, uygulamaların otomatik dağıtımını ve geri alınmasını sağlayarak sürekli entegrasyon ve sürekli dağıtımı (CI/CD) destekler. Araçlarla entegrasyon, otomatik derlemeler, testler ve dağıtımlar sağlar.

2.3.3 Hibrit ve Çoklu Bulut Dağıtımları

Kubernetes, iş yüklerini yerel veri merkezleri, genel bulutlar ve hibrit bulut yapılandırmaları dahil olmak üzere farklı ortamlarda çalıştırma esnekliği sağlar. Bu yetenek iş yüklerini birden fazla konuma dağıtarak yüksek kullanılabilirlik ve felaket kurtarma sağlar.

2.3.4 Büyük Veri ve Makine Öğrenimi

Kubernetes, dağıtık sistemleri ve büyük ölçekli veri işleme görevlerini yönetebilir.

2.4 Güvenlik Hususları

Güvenlik, Kubernetes kümelerinin yönetiminin kritik bir parçasıdır. Güçlü güvenlik önlemlerinin uygulanması, yetkisiz erişim, veri ihlalleri ve diğer tehditlere karşı korunmaya yardımcı olur. Kubernetes'teki önemli güvenlik hususları arasında rol tabanlı erişim kontrolü, gizli bilgilerin yönetimi ve pod güvenlik politikaları bulunur.

2.4.1 RBAC (Rol Tabanlı Erişim Kontrolü)

RBAC, Kubernetes'te yetkilendirmeyi yönetir ve hangi kullanıcıların veya hizmet hesaplarının hangi işlemleri gerçekleştirebileceğini belirler. İzinler vermek için roller ve bağlantılar kullanır.

2.4.2 Gizli Bilgilerin Yönetimi

Gizli bilgiler, şifreler, OAuth tokenleri ve SSH anahtarları gibi hassas bilgileri depolamak ve yönetmek için kullanılır. Gizli bilgiler Base64 ile kodlanırlar, dosya olarak monte edilebilir veya pod'larda ortam değişkenleri olarak gösterilebilirler.

2.4.3 Pod Güvenlik Politikaları

Pod Güvenlik Politikaları, bir pod'un sistem tarafından kabul edilmesi için karşılaması gereken bir dizi koşulu tanımlar. root olarak çalıştırma, ayrıcalık yükseltme ve ana bilgisayar alan adlarının kullanımı gibi kritik konuları kontrol ederler.

3. Kubernetes Ortamlarında Güvenlik Tehditleri

Kubernetes ortamları güçlü ve esnek olmasına rağmen güvenlik tehditlerine kapalı değildir. Potansiyel güvenlik açıklarını ve saldırganların bunları nasıl istismar edebileceğini anlamak, güvenli bir altyapı sağlamak için çok önemlidir.

3.1 Yaygın Güvenlik Açıkları ve Saldırı Yöntemleri

Kubernetes kümeleri, düzgün yapılandırılmadığında ve izlenmediğinde çeşitli güvenlik tehditlerine karşı hassas olabilir. Yaygın güvenlik açıkları arasında yanlış yapılandırmalar, ağ güvenliği tehditleri, yetkisiz erişim bulunur ve bunlar saldırganlar tarafından istismar edilebilir.

3.1.1 Yanlış Yapılandırmalar

- Varsayılan Ayarlar: Kubernetes bileşenleri için varsayılan ayarların kullanılması kümeleri saldırıya açık bırakabilir. Varsayılan ayarlar güçlü güvenlik politikalarını zorunlu kılmayabilir ve bu durum istismar edilebilecek boşluklar bırakabilir.

- Erişim Kontrolleri: Yanlış yapılandırılmış Rol Tabanlı Erişim Kontrolü (RBAC) ayarları, kullanıcılara veya hizmetlere gereğinden fazla izinler verebilir ve yetkisiz erişim riskini artırır.

- Ağ Yapılandırması: Yanlış yapılandırılmış ağ politikaları, podlar arasında sınırsız iletişime izin verebilir ve saldırganların küme içinde yatay hareket etme olasılığını artırır.

3.1.2 Ağ Güvenliği Tehditleri

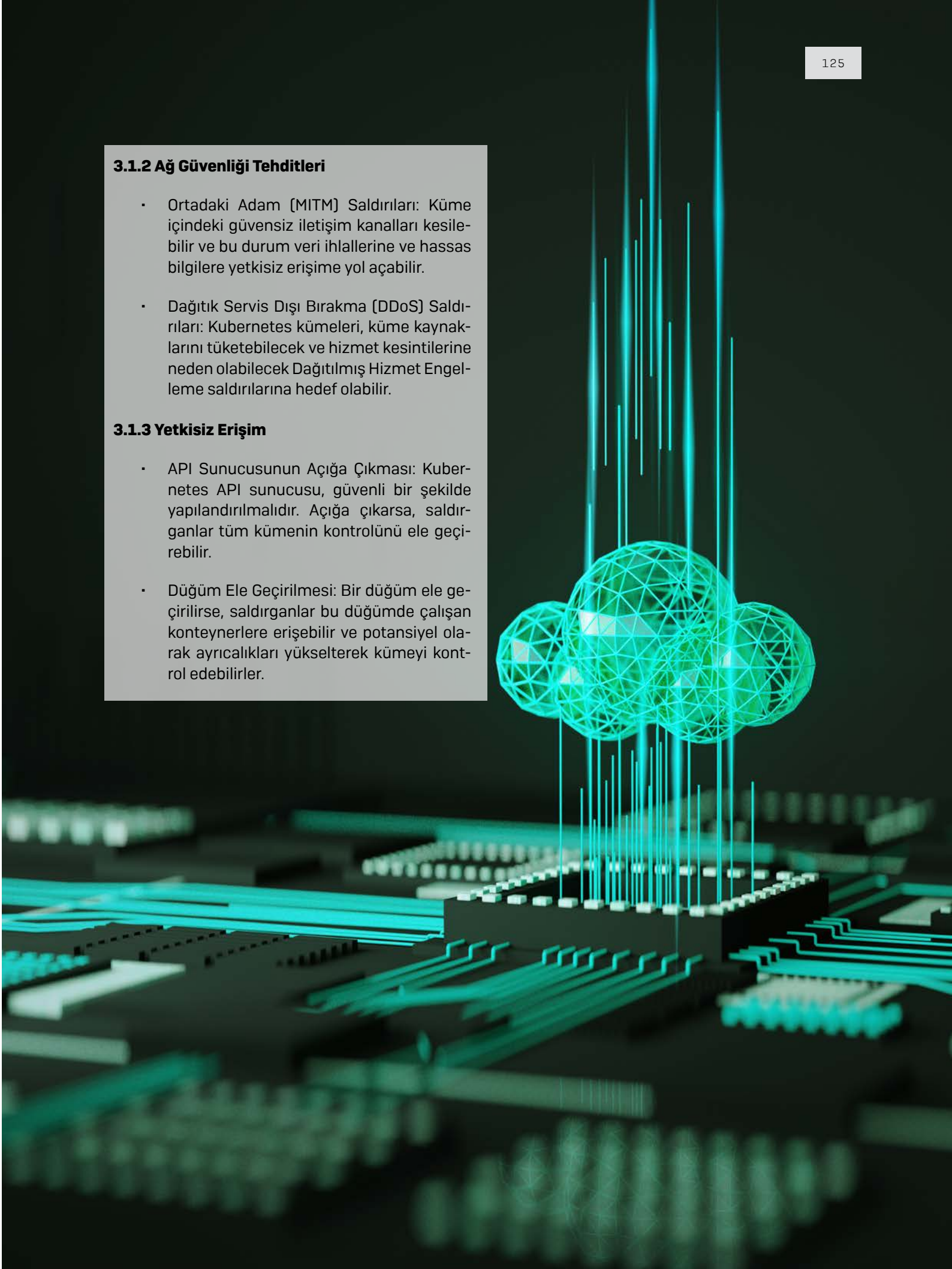
- Ortadaki Adam (MITM) Saldırıları: Küme içindeki güvensiz iletişim kanalları kesilebilir ve bu durum veri ihlallerine ve hassas bilgilere yetkisiz erişime yol açabilir.

- Dağıtık Servis Dışı Bırakma (DDoS) Saldırıları: Kubernetes kümeleri, küme kaynaklarını tüketebilecek ve hizmet kesintilerine neden olabilecek Dağıtılmış Hizmet Engelleme saldırılarına hedef olabilir.

3.1.3 Yetkisiz Erişim

- API Sunucusunun Açığa Çıkması: Kubernetes API sunucusu, güvenli bir şekilde yapılandırılmalıdır. Açığa çıkarsa, saldırganlar tüm kümenin kontrolünü ele geçirebilir.

- Düğüm Ele Geçirilmesi: Bir düğüm ele geçirilirse, saldırganlar bu düğümde çalışan konteynerlere erişebilir ve potansiyel olarak ayrıcalıkları yükselterek kümeyi kontrol edebilirler.



3.2 Önemli Güvenlik Olaylarının İncelenmesi

Gerçek dünya örnekleri, Kubernetes ortamlarının güvenliğinin önemini vurgular. Bu olaylar, yaygın güvenlik ihlallerinin etkilerini net bir şekilde gösterir.

3.2.1 Tesla'nın Kubernetes Kümesi İhlali

2018'de, Tesla'nın Kubernetes konsolunun parola olmadan erişime açık olduğu tespit edildi ve önemli bir veri ihlali oluştu. Saldırganlar hassas bilgilere erişip, hesaplama gücünü kripto para madenciliği için kullandılar.

3.2.2 Shopify Güvenlik Olayı

Shopify, üçüncü taraf bir kullanıcının Kubernetes kümesine eriştiği bir güvenlik olayı yaşadı. Bu olay, üçüncü taraf erişiminin güvenliğinin sağlanmasının ve sıkı güvenlik politikalarının uygulanmasının önemini göstermiştir.

3.2.3 Kubernetes API Sunucusu Güvenlik Açığı

Kubernetes API sunucusunda, kimliği doğrulanmamış kullanıcıların ayrıcalıklarını yükseltmelerine olanak tanıyan kritik bir güvenlik açığı keşfedildi. Bu olay, Kubernetes bileşenlerini düzenli olarak güncellemenin ve yamaların önemini vurgulamış oldu.

Kubernetes ortamlarında güvenlik tehditlerini anlamak ve bunları azaltmak, güvenli ve dayanıklı bir altyapı sağlamak için gereklidir. Yaygın güvenlik açıklarını tanıyarak ve sağlam güvenlik uygulamaları uygulayarak, kuruluşlar Kubernetes altyapılarını potansiyel saldırılardan koruyabilir, hizmetlerinin bütünlüğünü ve kullanılabilirliğini sağlayabilir.

4. Kubernetes Altyapılarında Güvenlik Denetimi

Güvenlik denetimi, bir Kubernetes altyapısının güvenliğini değerlendirme ve sağlama sürecidir. Bu, güvenlik açıklarını belirlemeyi, güvenlik politikalarına ve standartlarına uyumu değerlendirmeyi ve riskleri azaltmak için en iyi uygulamaları uygulamayı içerir.

4.1 Güvenlik Denetiminin Hedefleri

Kubernetes'teki güvenlik denetimi, kümenin güvenlik duruşunu kapsamlı bir şekilde değerlendirmeyi amaçlar. Birincil hedefler arasında yanlış yapılandırmaları belirlemek, endüstri standartlarına uyumu sağlamak ve güvenlik önlemlerini sürekli olarak iyileştirmek yer alır.

Güvenlik denetimi, bir Kubernetes kümesinin yapılandırmasını ve işlemlerini gözden geçirmeyi ve değerlendirmeyi içerir, böylece güvenlik standartlarına ve en iyi uygulamalara uygun olup olmadığını belirler.

4.2 Kubernetes Kümeleri için Denetim Pratikleri

Kubernetes kümelerini denetlemek için en iyi pratikleri uygulamak, sağlam bir güvenlik duruşu sağlamak için gereklidir. Bu pratikler, yapılandırmaların, rollerin ve güvenlik politikalarının düzenli olarak gözden geçirilmesini ve güncellenmesini içerir.

Yapılandırma Denetimleri:

- Altyapı Yapılandırması: Kubernetes altyapı yapılandırmaları düzenli olarak gözden geçirilmeli ve güncellenmelidir, en yaygın güvenlik pratikleri ve CIS kriterlerine uygun hale getirilmelidir.
- Denetim Günlükleri: Tüm küme etkinliklerinin ayrıntılı kayıtlarını tutan, güvenlik olaylarını tespit etmek ve araştırmak için hayati önem taşıyan denetim günlükleri etkinleştirilmelidir.

RBAC İncelemeleri:

- En Az Ayrıcalık İlkesi: Kullanıcı ve hizmet hesaplarına yalnızca görevlerini yerine getirmeleri için gereken izinler verilerek, en az ayrıcalık ilkesi uygulanmalıdır.
- Düzenli İncelemeler: RBAC politikaları periyodik olarak gözden geçirilmeli ve güncellenmelidir. Kurumsal gereksinimlere ve güvenlik politikalarına uygun hale getirilmelidir.

Görüntü ve Konteyner Güvenliği Kontrolleri:

- Konteyner İmajları: Konteyner imajları düzenli olarak bu alanda özelleştirilmiş güvenlik araçları ile taranmalıdır.
- Güvenilir İmaj Kullanma: Güvenilir kaynaklardan ve depolardan gelen imajlar kullanılmalı, bu imajların imzalı ve doğrulanmış olduğundan emin olunmalıdır.

Bu en iyi pratikleri uygulayarak ve doğru araçları kullanarak, organizasyonlar Kubernetes altyapılarını etkili bir şekilde denetleyebilir, sağlam güvenlik ve uyumluluk sağlayabilir. Sürekli denetim, güvenli bir altyapıyı sürdürmeye ve ortamda ortaya çıkan yeni tehditlere uyum sağlamaya yardımcı olur.

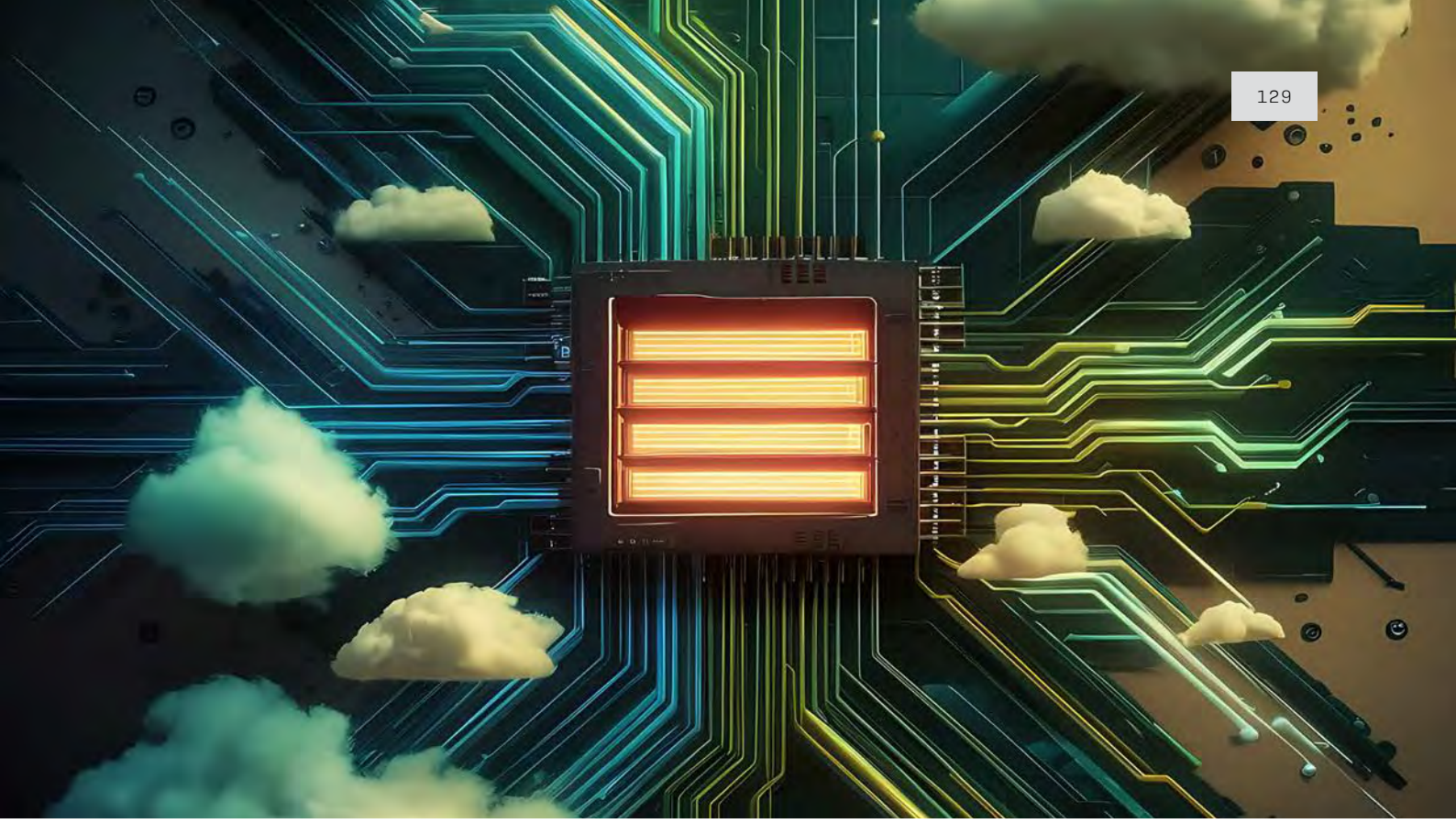
5. Kubernetes Altyapılarında İzleme

Kubernetes ortamlarında sürekli izleme, uygulamaların, altyapının güvenliğini, performansını ve güvenilirliğini sağlamak için hayati öneme sahiptir. Etkili izleme, sorunların erken tespit edilmesine, kaynak kullanımının anlaşılmasına ve kümenin genel sağlığının korunmasına yardımcı olur.

5.1 Sürekli İzlemenin Önemi

Kubernetes'te izleme, altyapının sağlığını ve performansını korumak için gereklidir. Anormalliklerin tespit edilmesine, kaynakların verimli yönetilmesine, sorun giderme ve optimizasyon için gerekli içgörülerin sağlanmasına olanak tanır.

Sürekli izleme, şüpheli faaliyetlerin ve potansiyel güvenlik olaylarının hızla tespit edilmesini sağlayarak hızlı müdahaleye olanak tanır. Kaynak kullanım örüntülerini anlamak, performansı optimize etmeye ve gelecekteki kapasite ihtiyaçlarını planlamaya yardımcı olur. İzleme, etkin olay yanıtı için gereken verileri sağlar, sorunların hızlı teşhisi ve çözümünü mümkün kılar.



5.2 İzlenmesi Gereken Temel Metrikler ve Göstergeler

Belirli metriklerin ve göstergelerin izlenmesi, sağlıklı ve güvenli bir Kubernetes ortamının sürdürülmesi için çok önemlidir. Bu metrikler, performans, kaynak kullanımı ve kümenin genel durumu hakkında fikir sağlar.

Kaynak Kullanımı:

- **CPU ve Bellek:** Kaynakların yeterli şekilde tahsis edilmesini sağlamak ve aşırı veya yetersiz kullanımını önlemek için CPU ve bellek kullanımı izlenmelidir.
- **Disk I/O:** Potansiyel darboğazları tespit etmek için disk giriş/çıkış işlemleri takip edilmelidir.

Ağ Trafiği:

- Gelen ve Giden Trafik: Güvenlik ihlali veya performans sorunu olabileceğini gösterebilecek alışılmadık örüntüleri tespit etmek için ağ trafiği izlenmelidir.
- Podlar Arası İletişim: Podlar arasındaki iletişimin beklenen örüntüleri takip ettiğinden emin olunmalıdır.

Günlükler ve Olaylar:

- Uygulama Günlükleri: Kümedeki uygulamalardan gelen günlükler toplanmalı ve analiz edilmeli, hataları ve performans sorunları belirlenmelidir.
- Kubernetes Olayları: Kubernetes olayları izlenmeli, değişiklikler takip edilmeli ve altyapının operasyonundaki anormallikler tespit edilmelidir.

6. Sonuç

Kubernetes altyapılarının güvenliğini sağlamak, proaktif olarak tehdit azaltmayı ve sağlam denetim ve izleme uygulamalarının uygulanmasını içeren kapsamlı bir yaklaşım gerektirir. Kubernetes altyapıları benzersiz güvenlik unsurları barındırır. Proaktif bir güvenlik stratejisi, güvenlik açıklarının hızla tespit edilmesini sağlamak için sistematik güvenlik denetimlerini ve sürekli izlemeyi kapsamalıdır. Bu uygulamaları CI/CD hatlarına entegre etmek, güvenlik sorunlarının tespitini ve çözümünü otomatikleştirerek uygulama teslim hızı ve güvenliği arasında denge kurmasına yardımcı olabilir.

FİNANSAL SİSTEMLERDE BLOKZİNCİR GÜVENLİĞİ

Ahmet Anıl DÜNDAR

Geleneksel veri tabanı teknolojileri, gerçekleştirilen tüm işlemlerin kaydını dağıtık veya merkezi bir sistem halinde tutabilir fakat tüm bilgilerin, tek bir noktadan yönetilebilir olan bir sistem altında tutulması nedeniyle bir güven veya güvenlik zafiyeti barındırmaktadır. Öte yandan geleneksel veri tabanları, kolaylıkla değiştirilebilir ve bu değişiklikler işlem yapan tarafların onayına sunulmadığından dolayı kesin bir güven ortamı oluşturamaz. Bu değişebilirlik ve merkezi otoriteye olan güven zorunluluğu blokzincir sistemini yaratmıştır.

Her ne kadar blokzincir teknolojisi Bitcoin ve kripto paralar ile tanınır olmuş olsa da aslında blokzincir arkasında daha farklı bir felsefe ve teknoloji barındırmaktadır. Blokzincir genel tanımıyla adını işlem verilerini bir zincir oluşturacak şekilde birbirine bağlı bloklar halinde saklama şeklinden almıştır. Bu birbirine bağlı bloklar, blokzincirin yapısı gereği

şeffaf bilgi paylaşımına izin veren gelişmiş bir veri tabanı mekanizması oluşturur ve görüş birliği esasına dayanmaktadır. Başka bir deyişle blokzincir ağında görüş birliği sağlanmadan zincir silinemez veya değiştirilemez. Bu yüzden girilen veriler kronolojik ve mantıksal olarak tutarlı ve takip edilebilir verilerdir.

Sistem basit olarak dağıtık kopyaların birkaç merkezde dağıtık olarak saklanması ve saklanan verilerin geçerli olması için bu merkezlerin hepsinin veya bir kısmının çevrimiçi olması ve birbiriyle eşleşmesi gerektiği anlamı gelir. Yetkili bir kullanıcı, blokzincir teknolojisi tarafından doğrulanması gereken bir işlem yapar ve bir blok oluşturur veya blokta bir parçanın içinde yer alır. Bu blok her bir düğüme (node) gönderilir ve yetkili düğümler bu işlemi mevcut bloğa ekler. Bu adımlar neredeyse gerçek zamanlı olarak gerçekleşir ve her blok saklanan verinin yanında özet değeri (hash) adı verilen benzersiz bir kodu da barındırır. Kriptografik olarak üretilen bu özet değeri, her blok için dijital bir parmak izi olarak düşünülebilir. Zincire bir blok eklemeden önce bu bilginin orijinalliğinin doğrulanması ve onaylanması gerekir. Kriptografik olarak özet değeri geri döndürülemez bir fonksiyon olduğu için önceki bloklara ait olan bir bilgi değiş-

tirilemez ve önceki bir blok değiştirilmeye çalışılırsa onun önündeki ve ondan sonraki blokların özet değerleri de değişeceğinden dolayı blokzincirin kayıtları oluşturduğu kayıt defterinin yapısı bozulacaktır. Çünkü önceki bloğun özet değerinden yeni bloklar oluşturulduğundan, özet değerleri blokları birbirine bağlamada rol oynarlar, böylece kurcalamaya karşı korumanın yanı sıra kronolojik bir sıra oluştururlar. Ek olarak, blokzincirlerin tek bir merkezi konum yerine dağıtık mimaride çalışması tek bir hata noktası (single point of failure) riskini azaltır.

Bir blokzincir sistemine yeni bir bloğun eklenmesi için bir fikir birliğine, anlaşmaya varılması gerekmektedir. Blokzincir konsensusu, blokzincir ağındaki tüm düğümlerin aynı veriler üzerinde anlaşmaya varması süreci olarak adlandırılabilir. Blokzincirin dağıtık mimarisi gereği bir sonraki blokta hangi işlemlerin olacağına karar verilmesi gerekmektedir. Bu nedenle de çeşitli konsensus algoritmaları geliştirilmiştir. En yaygın kullanılan konsensus algortimaları İş İspati (Proof of Work, PoW) ve Hisse İspatı (Proof of Stake, PoS) ve Otorite İspatı (Proof of Authority, PoA) olarak değerlendirilebilir. PoW mekanizmasında katılımcılar karmaşık matematik problemlerini çözer ve ilk doğru cevabı bulan düğüm yeni bloğu ağa ekler. PoS mekanizmasında ise katılımcılar sahip oldukları varlık miktarına göre yeni blokları üretme hakkına ve ihtimaline sahiptir. Son olarak PoA mekanizmasında ise blok üretimi belirli bir grup tarafından gerçekleştirilir. PoA anlayışı daha az merkeziyetsiz ancak daha hızlıdır.

Blokzincirin diğer bir özelliği de merkeziyetsiz oluşudur. Merkezi yönetilen bir sistem yerine, blokzincirler kontrolü birbirine bağlı bilgisayarlardan veya düğümlerden oluşan bir ağ üzerinden dağıtır. Bu düğümler birbirleriyle sürekli iletişim halinde olup dijital defteri güncel tutar. Dolayısıyla, iki eş arasında bir işlem gerçekleştiğinde, tüm düğümler fikir birliği mekanizmalarını kullanarak işlemin doğrulanmasında rol alır.

Bir blokzincirin güvenli ve dağıtık hale getirilmiş bir veri tabanından ayıran en büyük özelliği ise akıllı sözleşme (smart contract) özelliğidir. Blokzincir 2.0 ile gelmiş olan akıllı sözleşmeler, blokzincir tabanlı platformlarda kodlanan ve otomatik olarak yürütülen sözleşmelerdir. Bu sözleşmeler, belirli bir blokzincir platformu için özel bir programlama diliyle yazılır ve sözleşmenin işlevselliğini tanımlar. Belirli koşulların gerçekleşmesi durumunda

otomatik olarak çalışarak belirlenen eylemleri gerçekleştirebilir ve taraflar arasında güvenli, şeffaf ve merkezi olmayan bir şekilde işlem yapılmasını sağlar. Finansal sistemlerde, sigortacılık sistemlerinde, tedarik zinciri sistemlerinde kullanılması güvenli ve faydalı iş geliştirilmesini sağlayacaktır.

Bir diğer blokzincir özelliği de açık (public) ve özel (private) blokzincir ağlarının oluşturulabiliyor olmasıdır. Açık blokzincir ağları herkesin katılımına, veri okumasına ve işlem yapmasına izin verir ve merkeziyetsizliği, şeffaflığı hedef alarak güvenliği konsensus mekanizmalarıyla sağlamayı hedefler. Öte yandan özel blokzincir ağları ise yalnızca belirli bir grup tarafından erişilebilen ve kontrol edilebilen ağlardır. Yalnızca yetkili kullanıcılar düğüm olarak katılabilir ve işlem yapabilir şeklinde değerlendirebiliriz. Özel blokzincir ağları daha merkezi ve daha yüksek performanslı olarak kabul edilmektedir.

Blokzincirin merkeziyetsiz, değiştirilemez, takip edilebilir ve şeffaf yapısından dolayı birçok sektör ve kurum iş akışlarında blokzincir teknolojisinden faydalanmaktadır. Örneğin Singapur Exchange Limited, bankalar arası ödeme hesabı oluşturmak için blokzincir teknolojisi kullanmaktadır. Öte yandan Sony, telif hakkı ve dijital hakların korunması için blokzincir teknolojisinden faydalanmaktadır.

Her ne kadar bazı zafiyetleri ve karşılaştığı zorluklar olsa da blokzincir bahsedilmiş olan güven, güvenlilik, şeffaflık ilkeleri içermesiyle; akıllı sözleşmeler ile programlanabilirlik ve yapısı nedeniyle finans gibi kritik sistemlerde kullanılabilir durumda gözükmektedir. Öte yandan ülkeler arası para transferlerinin gerçekleştirilebilmesi, aracı kurumlara olan bağlılığın azalması veya kaybolması, tedarikten ödemeye direkt olarak bir akış başlatılabilmesi özelliklerinden dolayı blokzincir teknolojisi finansal işlemlerde kullanılmaktadır. 2024 yılına 19 milyar dolarlık bir iş büyüklüğüyle giren blokzincir teknolojisinin toplam sektör değerinin 2030 yılında 3,1 trilyon dolar olması öngörülmektedir. Bu nedenle blokzincir üzerinde çok fazla araştırma yapılmakta ve blokzincirin güvenliği daha önemli hale gelmektedir.

Blokzincir teknolojisi ve altyapısı kullanılarak kurulmuş olan bir finans sistemi hem finans sistemi zafiyetlerini hem de blokzincir zafiyetlerini doğal olarak içeriyor olacaktır. Dolayısıyla kurulacak olan sistem hem finansal bakımdan hem de teknolojik bakımdan zafiyetler içermemelidir. Finansal bir blokzincir güvenliğini tehdit edebilecek zafiyetler ve alınabilecek güvenlik önlemleri aşağıdakiler gibi özetlenebilir:

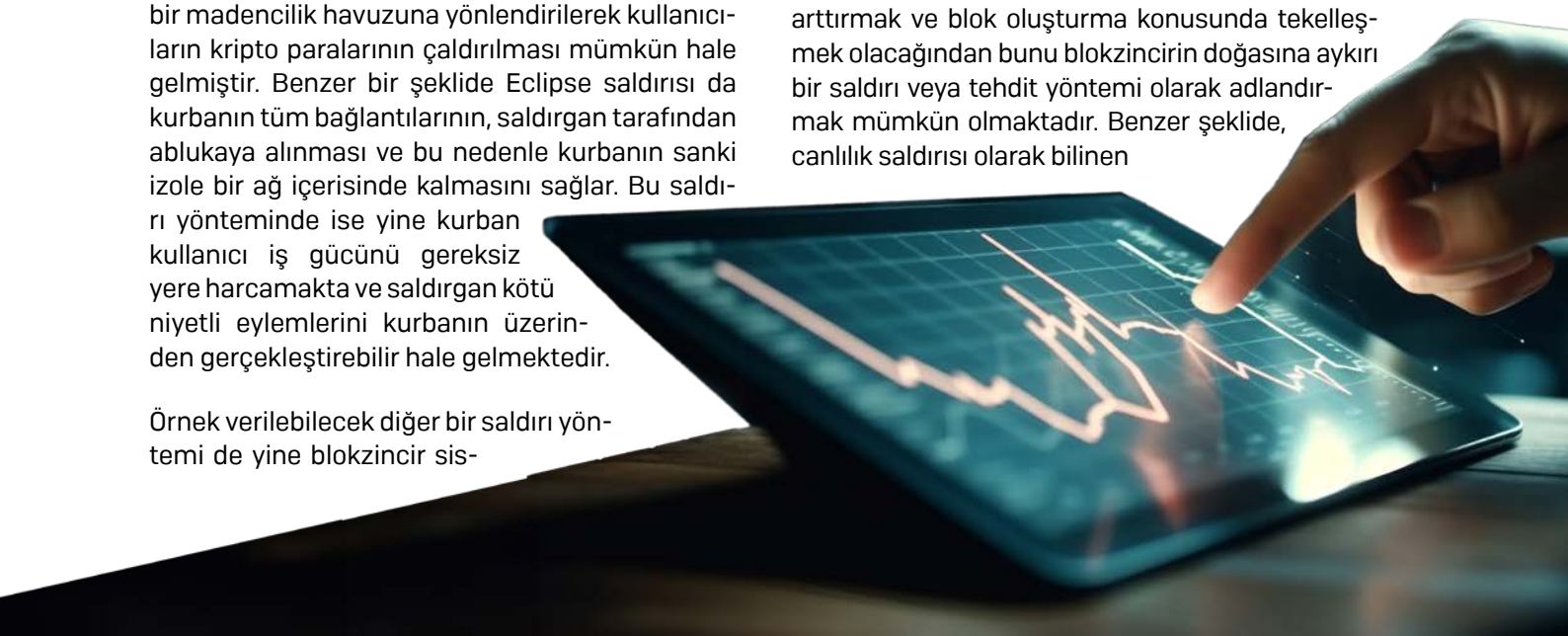
%51 zafiyeti, blokzincirin karşılıklı güven oluşturmak için dağıtılmış fikir birliği mekanizmasına dayanır. Basit bir mantıkla PoW tabanlı bir blokzincirde bir madencinin yani işlemleri bloklara yazarak yeni bloklar oluşturan bir kişinin veya grubun özet değeri üretme gücü toplam sistem gücünün yarısından daha fazla ise ve bu madenci kişisi veya grubu kötü niyetli olarak yapılmayan işlemleri zincirin içine dahil etmek isterse %51 saldırısı başlatılabilir. Bu nedenle, madencilik gücünün birkaç madencilik havuzunda yoğunlaşması, tek bir havuzun tüm bilgi işlem gücünün yarısından fazlasını kontrol etmesi gibi istenmeyen bir durumun ortaya çıkması korkusuna neden olabilir. 2014 yılında Gstash adlı kripto para madencilik havuzu toplam madencilik gücünün yüzde 42'sine ulaştıktan sonra kendi isteğiyle bölünerek olası bir %51 zafiyetinin önüne geçmiştir. Öte yandan PoS tabanlı bir blokzincirde, ağ altyapısına düğüm olarak dahil olan kullanıcılar değil kripto paraların sahipleri tarafından onaylandığından dolayı, teorik olarak bir kullanıcı veya grup tüm kripto paraların yarısından fazlasına sahip olursa sistemi istediği şekilde yönlendirebilme yeteneğine sahip olacaktır.

Alışılagelmiş finansal sistemlerin neredeyse tamamı bir merkez üzerinden yürütüldüğünden dolayı, üretilmiş bir paranın iki kez harcanması sıkıntısı, diğer bir deyişle çifte harcama (double spending) bir problem olarak sistemlerin karşısına çıkmazken blokzincirde bir sorun olarak sistemin karşısına çıkabilmektedir. Merkezi yönetilmiş finansal sistemlerde -örneğin bankalarda- banka sistemleri tüm hesaplardaki miktarları ve aktarılan miktarları bilebileceğinden dolayı işlemlerdeki veya sayılardaki bir tutarsızlığı anlayabilir. Öte yandan blokzincirde teorik olarak gerçek bir bloğun zincire eklenmesinden sonra hızlıca gizli bir blok çıkarıp ağa tanıtmak ve doğru olarak devam eden zincirin üstüne ekleyerek çifte harcamayı gerçekleştirmek mümkündü. Ancak gerçek bir zincire gizli bir ağın yeterli onayı almadan bağlan-

ması ve diğer madenciler tarafından doğrulanması ihtimali düşüktür. Bununla birlikte blokların özet değerlerinden dolayı değiştirilememesi, dallanan ve iptal edilen blokların varlığı, PoW yapısından dolayı düğümlerin (node) ortaya çıkan her bloğa koşulsuz güvenip kabul etmemeleri, çifte harcama tehlikesini azaltmaktadır.

Bir diğer direkt olarak yapılmış olan saldırı da BGP (Border Gateway Protocol) üzerinden yapılan saldırıdır. BGP temel olarak IP paketlerinin hedefe nasıl ilerleyeceğini düzenleyen bir yönlendirme protokolü olarak ele alınabilir. 2014 yılında yapılmış olan bir saldırıda, saldırganlar BGP sistemini ele geçirerek trafiği saldırganların kontrol ettiği bir madencilik havuzuna yönlendirilerek kullanıcıların kripto paralarının çaldırılması mümkün hale gelmiştir. Benzer bir şeklide Eclipse saldırısı da kurbanın tüm bağlantılarının, saldırgan tarafından ablukaya alınması ve bu nedenle kurbanın sanki izole bir ağ içerisinde kalmasını sağlar. Bu saldırı yönteminde ise yine kurban kullanıcı iş gücünü gereksiz yere harcamakta ve saldırgan kötü niyetli eylemlerini kurbanın üzerinden gerçekleştirebilir hale gelmektedir.

Örnek verilebilecek diğer bir saldırı yöntemi de yine blokzincir sistemi içindeki katılımcılara yapılmış olan saldırı yöntemidir. Önceden bahsedildiği şekilde, blokzincirde işlemleri onaylayarak blokları oluşturan ve zincire ekleyen kullanıcılar bulunmaktadır. Bu kullanıcıların bir grubunun diğer kullanıcıların işlem gücünü boşa harcamak amacıyla uyguladığı saldırı yöntemleri de mevcuttur. Buna örnek olarak düğümlerin buldukları blokları yayınlamayarak zinciri farklı bir çatal (fork) yapısı ile dallandırmaları sonucunda yeni ve gizli blokları kendileri oluşturup diğer işlemleri onaylayan ve blokları oluşturmaya çalışan katılımcıların işlem gücü boşa harcanmış olur. Burada hedef, blokları oluşturamayan katılımcıların, gizli bir şekilde blokları yayınlayan madencilerin havuzuna katılmasını sağlayarak işlem gücünü daha da arttırmak ve blok oluşturma konusunda tekelleşmek olacağından bunu blokzincirin doğasına aykırı bir saldırı veya tehdit yöntemi olarak adlandırmak mümkün olmaktadır. Benzer şeklide, canlılık saldırısı olarak bilinen



saldırıda ise temel olarak 3 aşamada saldırı gerçekleşir. İlk iki aşamada yine bahsedilmiş olan gibi gizli ve özel bir zincir oluşturularak diğer madencilere karşı bir avantaj elde edilir ve bloğun devamlılığı, bloğu gizli tutanlarca sağlanır. Son aşamada ise gerçek zincirin büyüme hızını yavaşlatmak için oluşturulan bloklar uygun zamanlarda zincire eklenir ve böylece ağda yer alan düğümlerin doğru ve güvenilir blokzincir işlemleri gerçekleştirmesi engellenmeye ve işlem yapma hızında düşürülmeye çalışılmaktadır.

Ayrıca bir saldırı yöntemi olmasa da blokzincir dünyasında yanlış kişilerin eline geçtiğinde günümüz bankacılık sisteminden daha fazla tehlike oluşturabilecek olan anahtarlar bulunmaktadır. Anahtarlar ve şifreleme teknikleri günümüz finans ve bankacılık uygulamalarında güvenliğin temelini oluşturmaktadır. Alışılmış mobil bankacılık ve finans sistemlerinin aksine blokzincir mimarisinde kullanıcının gizli anahtarı, üçüncü taraf kurumlar ve sistemler yerine kullanıcı tarafından saklanır. Bu şekilde tüm sorumluluk ve yönetim kullanıcı taraftadır. Bu nedenle bir kullanıcının özel anahtarı veya anımsatıcıları (nimonik, mnemonic) kaybolduğunda hesabın geri döndürülemez bir şekilde kaybolması çok olasıdır. Öte yandan kullanılan gizli anahtar veya hatırlatıcı kombinasyonun yabancı bir kişi tarafından biliniyor olması da finansal hesabın güvenliği için bir risk oluşturmaktadır.

Bunlarla beraber blokzincirin dağıtık veri tabanlarından ayıran en önemli özelliklerden olan akıllı kontratlar üzerinde de zafiyetlerin oluşma ihtimali bulunmaktadır. Akıllı sözleşmelerin kurguları düzgün yapılmalı, zaman damgasını merkezi bir zaman sunucusundan almalı, kullanılan blokzincirin konsensüs ve güvenlik mekanizmaları güncel ve güvenli olmalıdır.

Blokzincir güvenliğine zarar verebilecek tehdit ve tehdit aktörlerine karşı alınabilecek güvenlik önlemleri ise aşağıdaki şekilde örneklenmiştir:

Madencilikle ilgili bahsedilmiş olan bu tehdit veya saldırı yöntemlerine karşı smartpool adı verilen bir madencilik havuzu sistemi önerilmiştir. Smartpool merkeziyetçi olmayan bir madencilik havuzu protokolüdür ve blokzincirlerin daha adil, güvenli ve verimli çalışmasını sağlar. Bir akıllı sözleşme şeklinde yaratılmış olan smartpool üzerinden madencilik yapmak için ilgili paranın konsensusuna güvenilmektedir. Bu sayede madencilik havuzu merkezi olmayan ve ayrıca bir havuz operatörü gerektirmeyen bir mekanizmaya sahip olur. Smartpool havuz Sistemi ile BGP ve Eclipse saldırılarının önüne geçilebilmektedir. Smartpool, sistemine bir saldırgan dahil olsa dahi hak eden madencilerin kazanacağını garanti ederek madencilik konusunda tekelleşmeyi engeller ve blokların içindeki işlemlerin tekrar gönderilmesini engelleyecek bir sisteme sahiptir.

Anahtar ve anımsatıcıların güvenliğinin sağlanması ise blokzincir hesap güvenliği için son derece önemlidir. Günümüz bankacılık uygulamaları, hesaplara oturum açılmasını onaylamak için cep telefonu numarası ve kullanılan telefonun modeli gibi birkaç bilgiyi kullanır ve şifrenin unutulması veya artık güvenli olmadığının düşünülmesi durumunda hesap sahibi olunduğu kolay bir şekilde ispatlanarak yeni şifre alınabilmektedir. Ancak kripto para borsaları uygulamaları haricinde blokzincir ağları yalnızca anahtar ve anımsatıcıları kullanırlar. Yani diğer bir deyişle, kriptografik özel (private) anahtarlar hesaba erişim için kullanılacak olan tek ve en değerli bilgidir. Herhangi bir şekilde kaybedilmesi veya üçüncü kişilerin eline geçmesi ise tüm bilgilerin veya kripto paranın üçüncü kişilerin eline geçebileceğini veya kaybolabileceğini göstermektedir. Bu nedenle HSM (Hardware Security Module) gibi fiziksel bir cihaz veya kasa, cüzdan (vault) uygulamaları gibi anahtarları saklamaya yarayacak bir uygulamanın varlığı hesabın güvenliğini arttıracaktır.

2009'lu yılların başında ortaya çıkmış olan DeFi (decentralized finance, merkeziyetsiz finans) anlayışı ile merkezi otoriteden bağımsız ve sadece yapılacak işlemi, yalnızca işlemi gerçekleştiren eşler (peer) arasında bilinir kılan fakat bunun da güvenilir olmasını amaçlayan bir vizyon ortaya atılmıştır. Her ne kadar yine kripto paralarla yapılması düşünülse de DeFi için düşünülen ana para

birimi kripto para veya NFT olmak zorunda değildir. Ortaya atılan herhangi yeni bir para biriminin, tıpkı günümüzde kullanılan bankacılık ve finans sistemlerindeki gibi kullanılması için akıllı sözleşmelerin kullanılması gerekmektedir. Akıllı sözleşmelerin varlığı ile ödünç alma, borç alma, kripto paralar üzerinden faiz getirisi elde etmek gibi daha çok temel bankacılık ve finans sistemlerinde karşımıza çıkan bu özelliklerin DeFi'de kullanılması mümkün hale gelmiştir. Bu nedenle hem DeFi anlayışı hem de ileride ortaya çıkabilecek blokzincir tabanlı bankacılık ve finans anlayışları eğer gerçekten bir üst yönetimin altında çalışmayacaksa, Ethereum gibi akıllı sözleşmeleri yapısında barındıran blokzincir ağları üzerinde çalışacaktır. Öte yandan blokzincir yalnızca dağıtık mimari yapısı için kullanılıp tüm işlemler yine bir veya birkaç düğüm tarafından onaylanacak veya ledger denen tüm işlemlerin yazılmış olduğu deftere yalnızca bir veya birkaç düğüm tarafından ulaşılabilecekse; gerçekten merkeziyetsiz ve blokzincir mimarisinin tam olarak doğru bir şekilde kullanıldığı/kurgulandığı bir sistemden söz edilmesi mümkün olmayacaktır.

Blokzincirin finans konusunda kullanımı ve geneli kripto paralarla ilgili olsa da akıllı sözleşmeler veya blokzincirin yapısı gereği yapılabilecek saldırılar veya oluşturulabilecek tehditler göz önüne alındığında; blokzincir teknik olarak geleneksel dağıtık mimarideki veri tabanlarından daha yüksek teknik bir özellik sunmuyor gibi görülebilmektedir. Merkeziyetsiz yapısı her ne kadar günümüz banka, finans ve devlet kurumları gibi sistemler için uygun görünmüyor olsa da değiştirilemezlik ve inkar edilemezlik prensiplerini doğasında barındıran blokzincirin günümüz sistemlerine göre daha güvensiz oluşu tartışmaya hala açık bir konudur. Öte yandan veri depolama konusundaki başarısı, tek bir noktaya bağlı kalmadan veya tek bir hata noktası içermeyen yapısı, içeriğinin değiştirilemez oluşu, zero-knowledge proof (ZKP, sıfır güven ispatı) gibi bir bilginin doğruluğunu, bilgiyi açık etmeden ispatlayarak kendisini ifşa etmemeye; dolayısıyla gizliliği ve güvenliği arttırmayı amaçlayan yapıların kullanılması, DeFi (decentralized finance, merkeziyetsiz finans) gibi sistemlerin çalışılarak merkeziyetsiz bir finans altyapı amaçlanması nedeniyle blokzincir, sadece kripto paralar değil belki günümüzde kullanıldığımız tüm bankacılık ve finans sistemlerinin içinde yer alacaktır.

RTCA DO-326 UÇUŞA ELVERİŞLİLİK GÜVENLİK SÜRECİ SPESİFİKASYONU

Zaliha YÜCE TOK, İsa Can BABİR, Mehmet Atınç GÖKYER

Aviyonik endüstrisindeki süregelen dijital dönüşüm, havacılık sektörünün sınırlarını genişleterek, karmaşık hava aracı sistemlerinin yönetiminde

önemli gelişmelere neden oldu. Bu dönüşümle birlikte, aviyonik platformlarda siber güvenlik çözümlerinin kullanım ihtiyacı arttı. Aviyonik sistemlerin kendine has bir disipline ve uzmanlık alanına ihtiyaç duyması, siber güvenlik çözümlerinde de özelleşmiş analiz tekniklerine ve güvence hususlarının gelişmesine yol açtı. Bu ilerlemeler ışığında, hava araçlarının geliştirilme aşamasında kullanılmak üzere Uçuşa Elverişlilik Güvenlik Süreci Spesifikasyonunu (DO-326/ ED-202) yayınladı.

DO-326, hava araçlarında siber güvenlik için fiili endüstri yol haritasıdır. Bu standart, hava araçlarına yönelik kötü niyetli müdahaleleri, yani siber güvenlik tehditlerini, sistemli bir şekilde nasıl önleyeceğine ve azaltacağına rehberlik etmektedir. Genellikle endüstride "havacılık siber güvenliğine giriş" olarak adlandırılan DO-326A, tüm hava taşıtları, motorlar, rotorlu taşıtlar ve pervaneler için resmi uyumluluk gereksinimlerini temsil etmektedir. Standart, platform üreticileri için uyumluluk hedeflerini ve veri gereksinimlerini ana hatlarıyla belirlenirken, güvenli bir ekosistem oluşturmanın önemini de vurgulanmaktadır. DO-326A'nın temel odak noktası, bir saldırının uçağın işleyişini ciddi şekilde etkileyebileceği ve yolcu ile operatör güvenliğini tehlikeye atabileceği durumlarda, kötücül yazılımların aviyonik sistemlere bulaşmasının nasıl önlenebileceğini belirlemektedir.

DO-326/ED-202 seti içindeki her bir spesifikasyon, belirli bir amaca yönelik olarak oluşturulmuştur. DO-326/ED-202

spesifikasyonu, sertifikasyon sürecinde nelerin yapılması gerektiğini belirtirken, DO-356/ED-203 spesifikasyonu, nasıl yapılması gerektiğini açıklar. DO-355/ED-204 dokümanı, üretim sonrası bakım faaliyetlerini kapsarken, ED-205 özellikle Avrupa kullanımına yönelik yer sistemleri spesifikasyonunu içermektedir.

Uçuşa elverişlilik emniyet süreçleri ve uçuşa elverişlilik güvenlik süreçleri, hava araçlarındaki güvenliği sağlamaya yönelik iki ayrı ama birbirini tamamlayan süreçleri oluşturmaktadır. Uçuşa elverişlilik emniyet süreçleri, hava araçlarının güvenli bir şekilde uçabilmesi için temel standartları ve gereksinimleri karşılar. Bu süreç, olası kasıtsız istenmeyen elektronik etkileşimlerden kaynaklanabilecek tehditlere karşı önlemler içerir.

Diğer yandan, uçuşa elverişlilik güvenlik süreci, hava aracını kasıtlı olarak gerçekleştirilen izinsiz elektronik etkileşimlerden korumak için gerekli gereksinimleri belirler ve hava aracının siber güvenliğini sağlamaya odaklanır. Kasıtlı olarak gerçekleştirilen izinsiz etkileşimler, özel verilere yetkisiz erişim, sistem kaynaklarını veya iletişim

hatlarını işlevsiz hale getirmeye yönelik kullanılan kötücül yazılımlar, veri iletişimini bozmaya yönelik girişimler ve verilerin pasif olarak dinlenerek ele geçirilmesi başta olmak üzere hava aracının güvenliğini tehlikeye atacak girişimleri kapsar. Emniyet ve güvenlik süreçleri hava araçlarının güvenliğini sağlamak için birbirini tamamlayan önemli bileşenlerdir. Bu iki süreç bir arada çalışarak, hava araçlarının güvenliği için kapsamlı bir koruma sağlar.

Uçuşa elverişlilik güvenliğini sağlamak için, DO-326A güvenlik ve risk yönetimi çerçevesi tanımlanmıştır. Bu çerçeve, güvenlik risklerini tanımlamak, analiz etmek, değerlendirmek ve yönetmek için belirli adımları içerir. Temel olarak varlık tanımlama, tehdit ve zafiyet tanımlama, risk değerlendirmesi ve analizi, risklerin kabul edilebilirliğinin değerlendirilmesi, risk azaltma, risklerin izlenmesi ve gözden geçirilmesi gibi adımları içeren süreci tanımlar. Şekil 1, Uçuşa Elverişlilik Güvenlik Süreci'nin ana hatlarını tanımlamaktadır.

Güvenlik Sertifikasyon Planı'nın (PSecAC) hazırlanması güvenlik risk yönetim çerçevesinin ilk adımıdır. Bu belge, uçak veya sistem için sertifikasyona yönelik izlenmesi gereken adımları belirler. Bu kapsamda güvenlikle ilgili gereksinimlerin ve önlemlerin nasıl doğrulanacağı, güvenlik risklerini ve tehditleri nasıl değerlendirileceği ve bunlara karşı alınacak tedbirlerin nasıl belirleneceği gibi güvenlik sürecinin etkin bir şekilde yönetilmesine ve uçağın güvenlik açısından uygunluğunun sağlanmasına yönelik planı oluşturur.

Sonraki aşama, güvenlik kapsamının belirlendiği ve uçuşa elverişlilik güvenlik sürecinden geçirilecek varlıkların tanımlandığı adımdır. Varlıklar (Assets), uçağın uçuşa elverişliliğine katkıda bulunan fonksiyonlar, sistemler, veriler, arayüzler, süreçler ve bilgiler gibi mantıksal ve fiziksel kaynakları tanımlar. Bu varlıklara yönelik başarılı saldırılar uçağın güvenliğini riske atıyorsa önlem alınması gerekir. Tüm varlıkların korunması gerekmez ve

bu nedenle güvenlik kapsamında olmak zorunda değildir. Ancak bu sistemlerdeki herhangi bir arayüz, potansiyel saldırı vektörü olarak değerlendirilmelidir.

Varlık tanımlaması, risk değerlendirmesini kolaylaştırmak için uygun bir detay seviyesinde olmalıdır. Bu kapsamda, güvenlik çeperi ve güvenlik ortamının tanımlanması gereklidir. Güvenlik çeperi, uçağın veya sistemlerin dış sistemlerle ve kişilerle olan arayüzlerini tanımlar. Çeper, uçağın etkilenebileceği veya etkileşime girebileceği unsurları içerir. Güvenlik ortamı, güvenlik çeperinin dışında bulunan ve değerlendirme altındaki varlıklarla etkileşimde olan kişiler ve harici sistemlerle ilgili varsayımlar ve gereksinimleri içerir. Varlık tanımlaması sırasında belirlenen tüm ilgili varsayımlar ve arayüzlere erişimi olan unsurlarla birlikte, güvenlik ortamının açıklaması oluşturur.

Güvenlik kapsamı belirlendikten sonra risk değerlendirme süreci başlatılır. Bu adımda tehdit koşulları listelenir, tehditlerin etki şiddeti belirlenir ve güvenliğe olan etkisinin değerlendirilir. Tehdit senaryoları oluşturularak önlem alınmasını gereken potansiyel saldırı yolları listelenir.

Risk değerlendirmesi sonucunda tanımlanan riskler kabul edilebilir bir seviyede ise kanıt olarak sertifikasyon sürecine eklenir. Güvenlik riskleri kabul edilebilir bir seviyede değil ise, tehditin ciddiyet seviyesine göre çeşitli önlemler güvenlik geliştirme süreci kapsamında tasarlanır. Bu süreçte, tanımlanan riskleri önlemeye yönelik yazılım ve donanım siber güvenlik gereksinimleri belirlenir ve belirlenen gereksinimler doğrultusunda yazılım ve donanım geliştirme faaliyetleri gerçekleştirilir. Güvenlik geliştirme faaliyetleri çerçevesinde oluşturulan önlemlerin güvenlik korumasının etkinliğini ölçülür. Bir başka deyişle yazılım ve donanım siber güvenlik gereksinimleri doğrulanır. Doğrulanan gereksinimler sonucunda tehditlere karşı kabul edilebilir bir seviyede riske ulaşılmışsa kanıtlar ile birlikte sertifikasyon sürecine dahil edilir. Tüm tehditlere karşı önlemler alındığında süreç başarıyla tamamlanır ve hava aracının güvenliği güvence altına alınmış olur.

DO-326 spesifikasyonu, havacılık endüstrisinde siber tehditlere karşı alınabilecek önlemlerin tanımlandığı kritik bir süreç olarak yerini almıştır. Bu spesifikasyon, havacılık güvenliğinin dijital çağa ayak uydurması için önemli bir kilometre taşıdır. Bu spesifikasyonun aviyonik geliştirme süreçlerine eklenmesi, platformların siber tehditlere karşı dirençli hale gelmesine olanak sağlayacaktır.

ASELSAN AVİYONİK SİBER GÜVENLİK ÖNCÜL ARGE LABORATUVARI

Ayşegül ORHAN, Zaliha YÜCE TOK

ASELSAN Aviyonik Sistemler Tasarım Direktörlüğü bünyesinde aviyonik alanında yürütülen siber güvenlik araştırmalarını destelemek amacı ile TÜBİTAK 1515 Destek Programı'na "Aviyonik Siber Güvenlik Öncül ARGE Laboratuvarı Kurulumu" için başvuruda bulunulmuştur. TÜBİTAK 1515 Öncül ARGE Laboratuvarları Destekleme Programı tarafından desteklenmesi uygun bulunan laboratuvar, 1 Temmuz 2023 tarihinde ASELSAN ve TÜBİTAK arasında imzalanan sözleşme ile destek kapsamına alınmıştır. Ülkemizde ilk defa ASELSAN tarafından kurulan bu laboratuvar kapsamında elde edilecek bilgi birikimi ve altyapının yeni nesil aviyonik platformlarda kullanılması ve aviyonik siber güvenlik alanında uzmanlaşmış bir ekibin oluşturulması hedeflenmiştir.

Aviyonik platformlar zaman içinde hızlı ve dikkate değer bir evrim geçirmiştir. Birinci nesil askeri hava araçları, temel ve ilkel cihazlar, analog göstergeler, bağımsız ekranlar ve sınırlı radar ile radyo iletişimi ile karakterize edilmiştir. İkinci nesil askeri hava araçlarında ise, yüksek hızda kullanılan silah sistemlerinin doğruluğunu ve etkinliğini artırmak için pilotların iş yükünü hafifletecek sistemlere ihtiyaç duyulmuş ve bu gereksinimi karşılamak amacıyla merkezi ve dağıtık mimariler, analog veri aktarımı, dijital ve senkron arayüzler, sınırlı tümleşik ekranlar ve görev kritik aviyonikler kullanılmaya başlanmıştır.

Üçüncü nesilde federatif mimarilere geçilmiş, uzak terminallerin sayısı artmış ve hataya dayanıklı aviyonik sistemler geliştirilmiştir. Federatif yapılar, hava aracının her bir fonksiyonunun kendi işlemci ve sensörlerine sahip olduğu, verilerin farklı fonksiyonlar arasında paylaşılmadığı ve her bir kutunun tek bir görevi yerine getirdiği mimariler olarak yerini almıştır.

Dördüncü nesil askeri hava araçları ise dijital veri yollarının yoğun olarak kullanıldığı ve IMA (Integrated Modular Avionics) mimarisinin uygulandığı nesil olarak öne çıkmıştır. IMA mimarisi, federatif mimarilere karşılık olarak, ortak donanım modüllerinin bir araya getirildiği, sensör verilerinin paylaşıldığı ve bir ana işlemcinin aviyonik fonksiyonların çoğunu yerine getirdiği, aynı zamanda alan

ve zaman bölütlendirmesine imkan tanıyan bir yapı sunmuştur.

Beşinci nesil askeri hava araçlarıyla birlikte, 5G, Bulut, Wi-Fi, Uydu Haberleşmesi ve Yapay Zeka gibi ileri teknolojiler ve yenilikçi konseptler, yeni nesil aviyonik süitlerde yerini almaya başlamıştır. Bu gelişmeler, otonom uçuş, sanal yardımcı pilot, yapay zeka destekli otomatik iniş kalkış gibi birçok ileri teknolojinin entegrasyonunu da mümkün kılmıştır.

Uzun yıllar boyunca, aviyonik platformlar nispeten siber güvenlik tehditlerine karşı korunaklı kaldı. Bu durumun temel sebepleri arasında, platformların dış dünyaya kapalı olması ve aviyonik sistemlerin özgün yapısıyla saldırılarda kullanılabilecek bilgilerin içerdeki uzmanlarda bulunması yer alıyordu. Ancak, 5. Nesil hava platformlarının dış dünya ile bağlantılı hale gelmesi, bu sistemleri siber saldırılara karşı savunmasız hale getirerek, siber güvenlik çözümlerinin geliştirilmesini kaçınılmaz kıldı.

Aviyonik sistemlerin kendine has bir disipline ve uzmanlık alanına ihtiyaç duyması, siber güvenlik çözümlerinin de özelleşmiş analiz tekniklerine ve güvence hususlarının gelişmesine yol açtı. Bu gelişmeler ışığında EASA, hava aracı geliştirme aşamasında kullanılmak üzere Uçuşa Elverişlilik Güvenlik Süreci Spesifikasyonunu (Airworthiness Security Process Specification ED202/DO326) yayınlandı. Bu spesifikasyonun önümüzdeki yıllarda zorunlu hale gelmesi ve geliştirilecek yeni platformların güvenlik standartlarını karşılaması planlandı. ASELSAN da, bu spesifikasyona uygun ürünler geliştirmek amacıyla laboratuvar çalışmaları yürüterek gerekli altyapı ve bilgi birikimini oluşturmayı hedeflemektedir. Bu çalışmalar, ED202/DO326 spesifikasyonuna uygun aviyonik ürünlerin geliştirilmesini sağlayacak bir temel oluşturacaktır.

ASELSAN Aviyonik Siber Güvenlik Öncül AR-GE Laboratuvarında, aviyonik platformlarda uçtan uca güvenliği sağlamaya yönelik geleceğin teknolojileri diyebileceğimiz alanlarda çalışmalara başlanmıştır. Laboratuvar kapsamında Ana Bilgisayar tabanlı Saldırı Tespit Sistemleri, Aviyonik Veri Yolu Saldırı Tespit Sistemleri, Aviyonikte Kuantum Sonrası Güvenlik Çözümleri ve Aviyonik Kablosuz Ağ Güvenliği başta olmak üzere birçok yenilikçi alanda çalışmalar yürütülecektir.

AVİYONİK VERİ YOLU SALDIRI TESPİT SİSTEMLERİ

Zaliha YÜCE TOK, Mustafa EVCİL

Aviyonik platformlar uzun yıllar boyunca dış dünya ile iletişim kurmamış ve bu bağlamda geliştirilen mimarilerde, dış kaynaklı tehditlere karşı siber güvenlik önlemlerinin alınmasına gerek duyulmamıştır. Ancak, bulut tabanlı sistemlerle bütünleşen, 5G, Wi-Fi ve uydu iletişiminin aktif olarak kullanıldığı, yapay zekâ destekli otonom uçuş ve sanal pilot gibi yenilikçi uygulamaların yer aldığı yeni nesil aviyonik süitlerle birlikte, pek çok sistem arasında etkileşim artmıştır. Bu gelişmeler, aviyonik sistemlerin işlevsel kullanımını zarar verebilecek herhangi bir siber tehdidi tespit etmek ve doğabilecek zararlardan korunmak için, uçtan uca güvenliği sağlayacak siber güvenlik önlemlerine ihtiyacı doğurmuştur. Bu önlemler arasında, aviyonik veri yollarının güvenliği de kritik bir faktör olarak ortaya çıkmıştır.

Aviyonik veri yolları platform üzerindeki farklı aviyonik sistemlerin haberleşmesi için aviyonik platform ihtiyaçlarına özel tasarlanan iletişim kanallarıdır. Aviyonik veri yolları kesintisiz ve güvenilir çalışma, düşük gecikme, çevresel koşullardan etkilenmeme gibi daha çok uçuşa elverişlilik gereksinimlerini sağlayacak şekilde tasarlanmış, siber güvenlik anlamında tasarım çözümlerine yer verilmemiştir. Özellikle MIL-STD-1553 ve Arinc-429 gibi çok uzun yıllardır kullanılan ve uzun vade de kullanılması planlanan veri yolları bu kapsamda geliştirilen en yaygın veri yollarıdır.

Saldırı tespit sistemleri, veri yolu güvenliğini sağlamak için saldırıları gerçek zamanlı olarak tespit eden bir ağ izleme sistemidir. Saldırılar, güvenlik prosedürlerini ihlal eden ve veri gizliliğini, bütünlüğünü veya erişilebilirliğini tehlikeye atan tüm kötü amaçlı faaliyetleri içerir. Bu kapsamda güvenlik zafiyeti oluşturacak yetkisiz erişim, istenmeyen davranış veya anomali barındıran veriler tespit edilir, tanımlanır ve raporlanır. Aviyonik platformların dış dünya ile bağlantılı hale gelmesiyle birlikte saldırı tespit sistemleri de aviyonik veri yollarının güvenliğini sağlamaya yönelik kullanılan güncel teknolojilerden biridir.

MIL-STD-1553 ve Arinc-429 veri yolları güvenilirlik ve hata toleransı gibi uçuşa elverişlilik tasarım kriterleri göz önünde bulunarak tasarlanmış as-

keri veri yolu protokolleridir. 1970'lerin sonunda tasarlanmış bu veri yollarında siber saldırı kavramlarının gerçekçi görünmemesi sebebi ile protokollerde güvenlik önlemlerine yer verilmemiştir. Bu sebeple protokollerde veri bütünlüğü, kimlik doğrulama ve şifreli haberleşme altyapıları mevcut değildir. Bununla birlikte MIL-STD-1553 ve Arinc-429 veri yollarının güvenlik analizi sonucunda, bu veri yollarının kullanıldığı sistemlerin siber saldırılara karşı savunmasız olduğu ve gerçekleştirilecek saldırıların sistemlere çok ciddi zararlar verebileceği ortaya çıkmıştır. İlgili veri yolu protokollerin tasarımının güvenlik önlemlerini barındıracak şekilde güncellenmesi ise maliyet ve zaman açısından uygulanabilir değildir. Saldırı tespit sistemleri ise var olan veri yolu mimarisini bozmadan ve düşük maliyet ile geliştirilebilecek öne çıkan çözümlerden biridir.

MIL-STD-1553 ve Arinc-429 veri yollarında güvenliği sağlamaya yönelik üç farklı tip saldırı tespit sistemini kombine olarak kullanan sistemler mevcuttur. İçerik tabanlı saldırı tespit sistemi, donanımsal parmak izi saldırı tespit sistemi ve fiziksel saldırı tespit sisteminin birlikte kullanılmasıyla veri yollarında uçtan uca güvenliği sağlamak amaçlanmıştır.

İçerik tabanlı saldırı tespit sistemleri veri yollarındaki mesaj dizilimlerinin izlenerek istatistiksel ve derin öğrenme yöntemleriyle sistemin normal

koşullarının modellendiği araçlardır. Veri yoluna enjekte edilen mesajların yarattığı anomaliler içerik tabanlı saldırı tespit sistemiyle yakalanarak gerekli uyarılar oluşturulur. Ancak bu sistemler normal sistem davranışını sergileyen saldırganları kimlik doğrulama yetenekleri olmadığı için tespit edilemezler. Bu sorunu çözmek için, donanım parmak izi saldırı tespit sistemlerinden faydalanılmaktadır.

Donanımsal parmak izi saldırı tespit sistemi ile veri yolundaki cihazlara yönelik kimlik doğrulama sağlanır. Donanım parmak izi, sadece meşru cihazların veri yolunda varlığını tespit etmeye yönelik donanımların sinyal özelliklerini kullanır. Her veri yolu kartı, hatta aynı modeller dahi, üretim sırasında küçük hatalar nedeniyle farklı sinyal özellikleri gösterir. Bu benzersiz özellik, kimlik doğrulama amacıyla bir donanım parmak izi olarak kullanılır. Veri yolundaki yetkili cihazlara ait donanım parmak izleri çeşitli makine ve derin öğrenme yöntemleri ile modellenerek, çalışma anında cihazlara yönelik kimlik doğrulama işlevini yerine getirir.

Donanım parmak izi saldırı tespit sistemleri, veri yoluna mesaj ileten yetkisiz cihazları algılayabilirken, veri yolunu izleyen sessiz cihazları tespit edemezler. Bu sorunu ele almak için yan kanal analiz teknikleri kullanılır. Bir cihaz mesaj iletimine katılmadan sadece monitör faaliyetiyle bile veri yolundaki voltaj karakteristiğini değiştirebilmektedir. Fiziksel saldırı tespit sistemi, makine ve derin öğrenme yöntemleriyle veri yolundaki voltaj davranışını modeller ve çalışma anında modelle voltaj seviyelerini karşılaştırarak herhangi bir sapma durumunda uyarı oluşturur. Bu sayede veri yolu üzerindeki dinlemede olan yetkisiz cihazların tespiti sağlanır. Donanımsal parmak izi ve fiziksel saldırı tespit sistemleri, platform üzerinde zamanla ortaya çıkabilecek voltaj değişikliklerine karşı yeniden eğitim gereksinimi duyar. Bu kapsamda belirli aralıklarla voltaj değerleri ölçülerek model güncellenir. İçerik tabanlı saldırı tespit sistemi, donanımsal parmak izi saldırı tespit sistemi ve fiziksel saldırı tespit sistemlerinin bir araya gelmesiyle, kapsamlı bir uçtan uca güvenlik çözümü sağlanır.

TSN (Time-Sensitive Networking), IEEE 802.1 standardı altında tanımlanan gerçek zamanlı, deterministik ve güvenilir veri iletimini sağlayan Ethernet tabanlı bir veri yolu protokolüdür. MIL-STD-1553 aviyonik başta olmak üzere otomotiv, havacılık ve askeri uygulamalarda güvenilirliği ve sağlamlığı nedeniyle sıkça kullanılırken, TSN geleceğin veri yolu olarak öne çıkar. TSN, paylaşılan veri boyutunun arttığı ve gerçek zamanlı iletişimin kritik olduğu durumlarda performans, uyumluluk ve ölçeklenebilirlik açısından da büyük avantajlar sunar. TSN protokolünün temelini oluşturan zaman duyarlı ağ yapısında zamanın kendisi de bir saldırı vektörüdür. Saldırgan tarafından tetiklenen bir gecikmenin ciddi sonuçlara yol açması sebebi ile zaman senkronizasyonu sadece ana performans ölçütü değil, aynı zamanda bir güvenlik gereksinimidir. TSN protokolü üzerinde yapılan güvenlik analizlerinde tespit edilen zayıflıklara karşı tasarımda güncellemeye yönelik çalışmalar başlatılmıştır. Ayrıca, saldırı tespit sistemleri, TSN veri yolu güvenliğine katkı sağlayacak diğer önemli bir önlem olarak ele alınmaktadır.

AFDX (Avionics Full-Duplex Switched Ethernet) güvenlik açısından kritik havacılık sistemlerinin sıkı gereksinimlerini karşılamak üzere geliştirilen Ethernet bazlı diğer bir veri iletişim standardıdır. AFDX, yüksek güvenilirlik, düşük gecikme süresi ve hata toleransı sağlaması gerçek zamanlı veri iletiminin uçuş güvenliği için hayati olduğu uçak sistemlerinde kullanım için uygun bir seçenek sunmaktadır. TSN otomotiv, endüstriyel otomasyon ve telekomünikasyon dahil olmak üzere çeşitli endüstrilere uygun olarak geliştirilirken AFDX aviyonik sistemler özelinde tasarlanmış bir veri yolu standardıdır. AFDX veri yollarındaki güvenliği sağlamak üzere diğer veri yollarındaki çözümlere benzer şekilde makine ve derin öğrenme tabanlı saldırı tespit sistemleri ile atakların tespiti amaçlanmıştır.

Aviyonik veri yolu saldırı tespit sistemleri veri yolları üzerindeki saldırıları tespit etmeye yönelik verimli ve maliyet etkin çözümler sunmaktadır. Makine ve derin öğrenme yöntemleri ile yüksek doğrulukta başarım elde edilirken, mevcut mimarilerde değişikliğe gerek duymadan entegre edilebilir olmaları ile de büyük avantaj sağlamaktadır. Aviyonik veri yolu saldırı tespit sistemleri, günden güne dış dünya ile bağlantısı artan aviyonik sistemlerin değişen tehditlerine karşı direncini arttırmak için gelecekte de önemli bir rol oynamaya devam edecektir.

AVYONİK SİSTEMLERDE KRİPTO MEKANİZMALARI İLE GÜVENLİK

Elif ERDEM GÜNAY, Neşe KOÇAK, Yeliz ERKEK

Aviyonik sistemlerde siber güvenlik tehditlerine farklı katmanlarda ve farklı seviyelerde önlem almak amacı ile kripto mekanizmaları kullanılmaktadır. Bu kripto mekanizmaları sayesinde haberleşme yapısına rassallık eklenerek COMSEC, TRANSEC ve NETSEC önlemleri alınmakta ve sırası ile güvenlik haberleşme ihtiyacını sağlamak için havada paylaşılan kritik kullanıcı verilerinin gizliliği, frekans atlama mekanizmalarının rassallığı ve ağ seviyesinde güvenlik sağlanmaktadır.

COMSEC önlemleri ile havada paylaşılan kritik veriler için siber tehditlere karşı gizlilik, bütünlük ve kaynak/kimlik doğrulama mekanizmaları ile önlemler alınmaktadır. Bu şekilde havada dinleme, tekrarlama saldırısı ve yetkisiz bir kişinin araya girmesi ya da mesaj göndermesi engellenmektedir.

TRANSEC önlemleri ile havada paylaşılan verilerin iletim güvenliği sağlanmakta ve kripto yetenekleri ile hem elektronik harp hem de siber güvenlik saldırılarına karşı güvenlik sağlanmaktadır. Bu şekilde havada dinleme, karıştırma, tekrarlama saldırısı ve yetkisiz kişilerin araya girmesi ve mesaj göndermesi engellenmektedir.

NETSEC önlemleri ile haberleşme ağının güvenliğinin sağlanması amaçlanmakta ve kripto mekanizmaları kullanılarak bu güvenlik sağlanmaktadır.

Bunlara ek olarak aviyonik sistemlerde uçağın güvensiz bir ortamda bulunma riskine karşı pilot kontrolünde acil silme önlemleri alınarak uçak içerisinde gizli veri kalmaması garanti edilmiş olmaktadır. Ayrıca kriptografik mekanizmaların kurcalama tehditlerine karşı korunması için de önlemler alınmaktadır. Avyonik kritik yazılımların siber güvenlik tehditlerine karşı dayanıklı dayanıklı ve güvenli bir şekilde yüklenmesi için de kriptografik mekanizmalar kullanılmaktadır. Ayrıca sistemin güvenli bir şekilde açılması ve kriptografik olarak ayağa kalkarak aktif olabilmesi için erişim denetimi kontrolleri sağlanmaktadır.

Kriptolojik mekanizmalar için olmazsa olmaz faktör kriptolojik parametreler ve kriptolojik anahtarlardır. Hava platformlarında güvenli anahtar yönetim mekanizması kurgulanmakta ve kriptolojik anahtarların ve parametrelerin güvenli olarak üretilmesi, dağıtımı, hava platformuna yüklenmesi ve saklanması sağlanmaktadır.

Aviyonik sistemlerde geliştirilen kripto yazılımları aviyonik standartlara uygun olarak geliştirilmektedir. Bu kapsamda DO-178 ve DO-254 standartlarına uygun geliştirme ve doğrulama faaliyetleri gerçekleştirilmekte ve çalışmalar sertifikasyon süreçlerine uygun olarak yapılmaktadır.

AVİYONİKTE KUANTUM SONRASI GÜVENLİK

Zaliha YÜCE TOK, Mustafa EVCİL

Havacılık sektörü de diğer birçok sektörle birlikte yeni nesil teknolojilerin entegrasyonu ile büyük bir değişim geçirmektedir. Uçak operasyonlarını daha verimli hale getirmek, pilot yükünü hafifletmek ve daha güvenli bir iletişime yönelik artan taleple aviyonik pazarın çehresi yeniden şekillenmekte 5G, uydu haberleşmesi ve yapay zekâ teknolojilerinin kullanımı artmaktadır. Bu kapsamda dijitalleşme, bağlantılı uçuş, yeni nesil iletişim sistemleri ve navigasyon sistemleri, yapay zekâ destekli otonom uçuşlar ve siber güvenlik entegrasyonu yeni nesil aviyonik süitlerde yerini almaya başlamıştır.

Havacılık sektörü bu dönüşümleri gerçekleştirirken bir başka dönüşümde kuantum bilgisayarlar ile hesaplamada ve dolayısıyla kriptografi alanında gerçekleşmektedir. Hızlı işlem yapma gücüne sahip olan kuantum bilgisayarların açık anahtarlı kriptosistemler özelinde güvenli haberleşme temellerini olumsuz yönde etkilemesi ile birlikte kuantum ataklara dayalı kriptosistemlere geçiş çalışmaları başlamıştır. Bu kapsamda NIST kuantum sonrası kriptografiye yönelik standart çalışmalarını koordine ederek taslak standartta kuantum bilgisayarlarda polinom zamanlı çözülemeyen zor problemlere dayalı kriptosistem önerilerine yer vermiştir. Kuantum bilgisayarların yakın bir gelecekte kullanılmasa bile kuantuma dayanıklı sistemlere geçişin önemli nedenleri vardır. Bunların başında kritik bilgilerin kaydedilerek gelecekte kuantum bilgisayar aracılığı ile şifrelerin yetkisiz kişiler tarafından çözülebilmesi gelmektedir. Başka bir ifadeyle, uzun süreli arşivleme ihtiyacı olan bilgilerin kuantum sonrası güvenli kriptosistemler ile bilgi güvenliği kavramlarını sağlayacak şekilde saklanması ulusal çıkarlar için gereklidir. Bir diğer önemli neden ise sektörlerin yeni bir kriptosisteme ve buna bağlı olarak yeni güvenlik protokollerine geçmesinin çok uzun süreler almasıdır. Yeni nesil aviyonik platformların son gelişmelerle dış dünya ile bağlantılı hale gelmesi kuantum sonrası kriptografinin de kritik bir ihtiyaç olarak aviyonik sistemlere entegrasyonunu zorunlu hale getirmektedir.

Aviyonik sistemlerin dış dünya ile bağlantısının olmaması, tasarım aşamasında siber güvenlikten çok uçuşa elverişliliğe önem verilmesine yol açmıştır. Bu kapsamda geliştirilen birçok sistemde siber güvenlik önlemleri göz ardı edilmiş, var olan güvenlik çözümlerinde ise kuantum ataklara dayanıksız kriptosistemler kullanılmıştır. Protokollere güvenlik eklentileri getirilmiş ancak çoğu kez tam bir güvenlik sağlanamazken aynı zamanda entegrasyonundaki ek maliyetler sebebi ile de uygulanamamıştır. Bu kapsamda güvenlik ihtiyacının en başında platform için güvenli haberleşme altyapılarının ve uçak yer istasyonu güvenli haberleşme sistemlerinin geldiği anlaşılmıştır.

Aviyonik platformlarda güvenliği sağlamak için, uçuşa elverişlilik standartlarını karşılayan aviyonik mimariye özel olarak tasarlanmış çözümler geliştirilmelidir. ARINC-653, gerçek zamanlı, güvenilir, gömülü yazılım sistemlerinin tasarımı ve geliştirilmesi için oluşturulmuş bir standarttır. Özellikle havacılık endüstrisinde yaygın olarak kullanılır. Bu standart farklı kritiklik seviyesindeki yazılımların birbirinden izole şekilde gerçek zamanlı çalışma kriterlerine uygun olarak koşmasına olanak sağlar. Platform üzerinde koşan uygulamaların güvenli haberleşmesine yönelik kullanılacak kriptografik kütüphanelerin Arinc-653 yapısına entegre edilerek RTCA DO-178C seviye A sertifikasyonuna uygun olarak geliştirilmesi gerekmektedir. Bellek kullanımı ve kriptografik işlemlerin aldığı süre gerçek zamanlı gömülü sistemlerin ihtiyaçlarına uygun şekilde belirlenmelidir. Kuatum ataklara dayalı kriptosistemlerin kaynak tüketiminin yoğun olması ve geliştirilecek kriptografi kütüphanelerinin sertifikasyon gereksinimleri aviyonik platformlara entegrasyonlarında dikkat edilmesi gereken en önemli unsurlardır.

Platform içi güvenliğin yanında platformların yer sistemleri ile güvenli haberleşmesi de kritik önem taşımaktadır. ACARS, uçaklar ve yer istasyonları arasında kısa mesajların hava bandı radyo veya uydu üzerinden iletilmesi için kullanılan bir dijital veri bağlantı sistemi olup, modern havacılıkta yaygın olarak kullanılan protokollerden biridir. Ancak, ACARS protokolünün tasarımı sırasında siber güvenlik hususlarının göz ardı edilmesi ACARS'ın saldırılara karşı savunmasız hale gelmesine neden olmuştur. Dünyanın çoğu bölgesinde, ACARS mesajları genellikle herhangi bir şifreleme olmadan düz metin olarak iletilmektedir. Radyo teknolojisinin gelişmesiyle, ACARS mesajları düşük maliyetli radyo donanımları ve açık kaynaklı programlar kullanılarak kolayca saldırganlar tarafından üretilebilir ve taklit edilebilir durumdadır. ACARS güvenliğini sağlamaya yönelik açık anahtar altyapısı ve kimlik tabanlı kriptografinin kullanıldığı çeşitli protokoller önerilmiştir. Aynı zamanda mesajlardaki sabit bit uzunluğa yönelik güvenlik çözümleri de yer almaktadır. ACARS mesaj güvenliği için ARINC 823 standardı oluşturulmuş ve açık anahtar altyapısı kullanılmıştır ancak, bu protokollere yönelik güvenlik açıkları sebebi ile platformlar tarafından uygulanabilir bir çözüm oluşturulamamıştır. Aynı zamanda kuantum ataklara karşı dayanıksız olan bu çözümlerin kuantum sonrası kriptografi altyapısı ile değiştirilmesi de önem arz etmektedir. Bunlara ek olarak, gerçek zamanlı sistemlerde gecikmenin öneminin de ayrıca ele alınması gerekmektedir.

ADS-B, hava araçlarını gerçek zamanlı olarak izlemek için GNSS verilerini kullanan yeni nesil hava taşımacılığı gözetleme teknolojisidir. En basit anlamada uçağının konumunun ve irtifasının iletildiği bir haberleşme sistemidir. Uçak takibini sürdürmek için periyodik yayınlar yapar. Hem sivil havacılıktaki yolcu sayısının hem de hava sahasında aynı anda bulunan hava aracı sayısının hızla artmasıyla, radar tabanlı gözetleme teknolojilerinin yetersiz kalması sonucunda emniyetini iyileştirmek ve hava sahası kapasitesini arttırmak için ortaya çıkmıştır. ADS-B sinyalleri düz metin olarak iletilmekte ve şifreleme, kimlik doğrulama ve imza eksikliği, ADS-B'yi saldırılara karşı savunmasız hale getirmektedir. Oluşan bu güvenlik açığını gidermek için çeşitli kriptolu ve kriptosuz çözümler önerilmiştir. Kriptosuz çözümler ağırlıklı olarak parmak izi ve geniş spektrum yöntemleri kullanılmaktadır. Yazılım parmak izi yönteminde, ağdaki cihazların yazılımsal davranışına göre kimlik doğrulaması yapılmaktadır. Donanım parmak izinde ise, cihazların ürettikleri gerilim vb. donanımsal davranışları kimlik doğrulaması için baz alınmaktadır. Kriptosuz bir diğer çözüm ise geniş spektrum yöntemidir. Bu yöntemle gönderilecek

bilgi, bir bant genişliği boyunca farklı frekanslara bölerek gönderilmektedir. Frekans atlama yöntemi bu yönteme örnek olarak gösterilebilir. Kriptolu çözümlerde ise asimetrik şifreleme ve simetrik şifreleme, güvenli yayın sağlamak için önerilen yöntemlerdendir. Bu yöntemler, ADS-B yayınları engellemeyi veya değiştirmeyi amaçlayan saldırılara karşı büyük bir güvenlik sağlamayı amaçlarken kuantum ataklara dayanıklı olmamaları sebebi ile güvenlik açığı yaratmaktadır.

Trafik Uyarı ve Çarpışma Önleme Sistem (TCAS - Traffic Alert and Collision Avoidance System), hava aracı etrafındaki belirli bir alana başka bir hava aracının girmesi durumunda, pilotlara görsel ve sesli uyarılar sağlayarak gerekli müdahalelerde bulunmalarını sağlayan ve havada çarpışmayı önlemeyi amaçlayan yeni nesil bir güvenlik teknolojisidir. ACARS da olduğu gibi düşük maliyetli radyo çözümleri ile yanlış bilgi içeren TCAS mesajları gönderilebilmekte ve bu tür saldırıların havada çarpışmaya neden olabileceği ortaya çıkmaktadır. Özetlemek gerekirse TCAS özelindeki siber güvenlik düzenlemelerinin açık olmaması, iletişimde imzalama ve şifrelemenin kullanılmaması TCAS cihazına yönelik güvenlik açığı oluşturmaktadır. Bu kapsamda yapılacak çalışmalarda da kuantum ataklara dayanıklı kriptosistemlerin kullanılması büyük önem arzetmektedir.

LDACS (L-band Digital Aeronautical Communications System) havacılıkta gelecekteki iletişim ihtiyaçlarını karşılamayı amaçlayan havayolu trafiği kontrolü ve hava sahası iletişimi için tasarlanmış hava-yere iletişim bağlantısıdır. Protokol kapsamında kuantum ataklara dayanıklı SIKE algoritması iletişimdeki veri aktarımı sırasında ortaya çıkan işlem gücü tüketimi veya bant genişliği kullanımı gibi yüklere çözüm olarak seçilmiştir. Ancak SIKE algoritmasının kırılması ile birlikte ACARS kullanımını devralabilecek bu seçenek ortadan kalkmıştır. Bununla birlikte NIST tarafından önerilen algoritmaların kullanıldığı ve bir önceki iletişim sisteminde eksik olan hava-hava iletişiminde yer aldığı güncellenmiş bir versiyon üzerinde çalışmalar başlamıştır.

Teknolojinin tüm sektörlerde devrim yaptığı bu dönemde aviyonik platformlarda yer alacak sistemlerde güvenliğin en önemli gereksinimlerden biri olacağı anlaşılmıştır. Kuantum sonrası kriptografi geliştirilecek bu güvenlik çözümlerinin temel yapı taşı olacak, bu çözümlerini sistemlerine entegre edebilen üreticiler ise bir adım önde yer alacaktır. Bu nedenle, geleceğin havacılık endüstrisinde başarı için güvenlik odaklı yaklaşımların benimsenmesi kritik öneme sahiptir.

GÜNCEL SİBER GÜVENLİK KONULARI

SİBER GÜVENLİK FARKINDALIĞI

Berkan UFUK

Gelişen teknolojiye adapte olmaya çalıştığımız günümüz dünyasında neredeyse gelen her yenilik yeni bir siber risk barındırıyor. Artık teknolojiye bağımlı hale gelmekte olduğumuz için risklerin de farkında olmak şarttır. Dolayısıyla bilinçli bir kullanıcı olup siber dünyadaki risklerin farkında olarak daha güvenli bir dünyada yaşamak aslında mümkün. "Siber güvenliğin en zayıf zinciri insandır." sözü defalarca kendisinin doğruluğunu kanıtlamıştır. Bilinçsiz bir kullanıcı yüzünden üstün çabalarla ve teknolojilerle korunan bir siber varlığın gizliliği ifşa olabilir, bütünlüğü bozulabilir veya bu varlık erişilemez hale gelebilir. Dolayısıyla, en zayıf zinciri kadar güvenli olan sistemleri korumak insanları bilinçlendirmekten geçmektedir. Güvenlik yalnızca siber güvenlik uzmanlarının değil, herkesin sorumluluğudur. Siber güvenlik farkındalığı, risklerin farkında olmayı ve bu risklere göre davranmayı gerektirir. Farkındalığı yüksek insanlar, tehdit olayları karşısında verinin korunması için daha doğru adımlar atacaktır.

Siber Hijyen: Siber hijyeni sağlamak, siber saldırı riskini azaltmak ve hassas bilgileri korumaktan geçer. Bu, bilinen güvenlik açıklarını gidermek için yazılım ve güvenlik yamalarının düzenli olarak güncellenmesi, güçlü, benzersiz parolalar kullanılması ve fazladan bir güvenlik katmanı eklemek için çok faktörlü kimlik doğrulama mekanizmalarının uygulanması dahil olmak üzere bir dizi en iyi uygulamayı kapsar. Ayrıca, bağlantılara tıklarken veya bilinmeyen kaynaklardan ekleri indirirken dikkatli olmak, kimlik hırsızlığı dolandırıcılıklarının veya kötü amaçlı yazılım bulaşmalarının kurbanı olmayı önlemeye yardımcı olabilir.

Bu yazıda, insan faktörü yüzünden daha önce yaşanmış olan felaketlerden, bu felaketleri önleyebilecek şeylerden ve dünyada siber farkındalık için yapılanlardan bahsedilecektir.

Siber Tehditlerin Evrimi:

Sıfırıncı gün açıklıkları dahil yeni zafiyetler her sene ortaya çıkmaktadır. Geniş ölçekte bakıldığında siber güvenlik tehditleri kimlik hırsızlığından geniş ölçekte desteklenen siber casusluğa kadar farklı

şekillerde olabilmektedir. Teknolojiye bağımlılık arttıkça ve korunması gereken veri miktarı arttıkça genişleyen saldırı yüzeyi siber saldırılara maruz kalma ihtimalini artırmaktadır. Dolayısıyla siber tehditlerin karşısında durmak için bilinçli olmak bir seçenek değil bir şarttır. Çünkü günümüzde insan kaynaklı saldırılar ve kişilere yönelik saldırılar hala çok yaygın bir şekilde gerçekleşmektedir.

Temel İlkeler:

Siber güvenlik farkındalığı doğal olarak insanlara dayanmaktadır. Bir sistemin siber güvenlik duruşunun güçlendirilmesi için o sistemin siber güvenlik önlemlerinin alınmasının yanı sıra sistemin kullanıcılarına siber tehditleri tanıtmak, tehditlerin nasıl önleneceğini öğretmek ve tehditler gerçekleştiği takdirde yapılacakları öğreterek güçlü bir güvenlik duruşu sergilemek gerekmektedir. Bilinçlenmek için en temel yaklaşım standartlardan ve rehberlerden haberdar olmaktır. Bilgisayar sistemlerinin barındırdığı riskleri anlamak ve onlardan kaçınmak için yapılabilecekler hakkında fikir sahibi olmak için standartlar ve rehberler takip edilebilir. Örneğin Ulusal Standartlar ve Teknoloji Enstitüsü (NIST – National Institute of Standards and Technology) bir kurumun bilgi teknolojileri güvenliği programı kapsamında farkındalık ve eğitim programlarının tasarlanması, geliştirilmesi, uygulanması ve sürdürülmesine ilişkin NIST SP 800-50 (Building an Information Technology Security Awareness and Training Program) Standardı'nı yayınladı. Ayrıca, Avrupa Ağ ve Bilgi Güvenliği Ajansı (European Network and Information Security Agency - ENISA), okuyucunun bilgi güvenliği farkındalığını hazırlamasına ve uygulamasına olanak tanıyan, kamu ve özel kuruluşlara pratik ve etkili tavsiyeler sunmayı amaçlayan bir The New Users' Guide: How to Raise Information Security Awareness isimli kullanıcı kılavuzu belgesini geliştirmektedir. Birleşmiş Milletler Avrupa Güvenlik ve İş birliği Teşkilatı tarafından yayınlanan OSCE (Organization for Security and Cooperation in Europe) Guide on Non-military Confidence Building Measures (CBM – Confidence Building Measures) güven artırıcı önlemler ve durumsal farkındalık için bir rehberdir. Bunlarla birlikte kapsamlı eğitim programları, atölye çalışmaları ve simülasyonlarla

sistem kullanıcıları güçlü bir güvenlik farkındalığı için gerekli bilgileri edinebilirler. Ancak, farkındalığın geliştirilmesi için sadece eğitimlerin ve standartların takip edilmesinin yeterli olmadığı çeşitli araştırmalarda ortaya koyulmuştur. Farkındalığın geliştirilmesi için güvenlik farkındalığı kültürünün oluşturulması gerekmektedir. Böylece kolektif sorumluluk duygusu ile birlikte insanlar, şüpheli olayların tespitleri ve bildirimleri konusunda daha istekli olacaktır.

Yapılan Çalışmalar:

Güney Asya'da siber güvenlik farkındalığının az olduğunu tespit eden bir çalışmada [C], siber güvenlik farkındalığını geliştirmek için bir çerçeve programı hazırlanmıştır. Bu çalışmanın işaret ettiği başka bir çalışmaya göre [A], internetteki insanlar tehlikelerin farkında değil ve gizli ve kişisel bilgilerin nasıl korunması gerektiğini bilmiyorlar. Bu yüzden de siber saldırganların hedefi haline gelmektedirler [B]. Farkındalığı artırmak adına çalışma grupları, seminerler, posterler ve uyarıcı metinler koymanın farkındalık artırıcı bir etki oluşturacağı gösterilmiştir.

Başka bir çalışma[D], Makedonya'daki siber güvenlik farkındalığı durumunu analiz etmiştir. Çalışma, siber güvenlik farkındalık eğitimlerinin hedefinin çocuklar, veliler ve öğretmenler olduğunu, eğitimlerin enstitü seviyesinde ve yalnızca mahremiyet odaklı olarak yapıldığını göstermiştir.

Ayrıca çalışmada, uç kullanıcıların ihmal edildiğini ve farkındalık için yeterli eğitimin yapılmadığı gösterilmiştir. Yazıda ayrıca, Makedonya'da yapılan siber güvenlik farkındalığını artırıcı çalışmalardan bahsedilmiştir.

Siber güvenlik farkındalık düzeylerini araştıran bir yazıda [E], siber güvenlik farkındalığı için yapılan

eylemlerin insanların davranışlarını değiştirmede yeterli olmadığını söylemektedir. Bunun sebebinin ise sadece bilgi verilmesinin yeterli olmadığını, insanların davranışlarını değiştirmek için tavsiyelerin insanlar tarafından anlaşılıp uygulanabilmesini ve insanların buna istekli olması gerektiğini ortaya koymaktadır. İnsanların daha güvenli bir dünya için ikna edilebilmesi adına çeşitli tekniklerin işe yarayabilirliği analiz edilmiştir. Siber güvenlik farkındalığını artırmak için bilgilendirme metinlerinin kesinlikle en yararlı yöntem olduğu sonucuna ulaşılmıştır.

Çalışmada varılan sonuçlar şu şekildedir:

- İnsanları, siber güvenlik riskleri yüzünden gerçekleşebilecek kötü durumları göstererek korkutmanın etkili bir taktik olmadığı,
- Farkındalık materyallerinin profesyoneller tarafından hazırlanması gerektiği,
- Farkındalık eğitiminin yalnızca bilgi vermekten ibaret olmadığı, hedefli, uygulanabilir ve geri beslemeli olacak şekilde yapılması gerektiği,
- İnsanlarda siber güvenlik farkındalığı oluşturabilmek için, öğrenme isteğine sahip olup sürekli geri besleme almaları gerektiği,
- Farklı kültürel içeriklerde ve karakteristiklerde vurgulamalar gerektiği.

İnsanlara bilgi güvenliği farkındalığı eğitimi verilmesinin yollarını araştıran bir çalışmaya göre [F] yazı-tabanlı, oyunlaştırılmış ve video tabanlı eğitimlerden en çok tercih edilen eğitim video tabanlı eğitimler olmuştur. Ancak, en başarılı sonuçların farklı türdeki eğitimlerin bir arada verilmesi ile elde edileceği gösterilmiştir.

Başka bir araştırmada [G] siber güvenlik alanında çalışmayan insanlara siber güvenlik farkındalığı aşılayan bir masaüstü oyun geliştirilmiştir. Bu sayede, organizasyonlardaki tüm çalışanların siber güvenlik risklerini anlaması, siber güvenlik saldırı ve savunmaları hakkında fikir sahibi olması amaçlanmıştır.

Siber güvenlik farkındalığı artıran bir çerçeve programı tasarlayan bir çalışmada[H], hedef kitle için tasarlanan oyun oynatılmış ve bu programı uygulayan adayların siber güvenlik farkındalıklarının arttığı gözlemlenmiştir.

Oyunlaştırmanın siber güvenlik farkındalığı geliştirme üzerindeki etkisini araştıran başka bir çalışma [I], siber güvenlik farkındalık düzeyini hangi oyunun en çok artırdığını araştırmıştır. Bunun için farklı oyunlaştırma yöntemleri karşılaştırılmıştır. Bunun için incelenen oyunlar arasından, mobil oyunların etkili olduğunu gözlemlenmiştir.

Başka bir çalışmada [J], siber güvenlik eğitimi, farkındalığı oluşturma ve egzersizi (cybersecurity education, awareness raising and training - CEAT) 80 farklı ülkede araştırma yapılmış ve genel durum ortaya koyulmuştur. İnternet kullanımının yaygın olduğu ülkelerde siber güvenlik farkındalığına diğerlerinden daha fazla önem verilmektedir. Ayrıca, gelirleri daha düşük olan ülkelerde siber güvenlik farkındalığının daha düşük olduğunu sonucu çıkarılmıştır.

Türkiye Yüzyılına İleri Teknoloji Damgası

www.aselsan.com

aselsan

SİBER CAYDIRICILIK: GELECEĞİN GÜVENLİK PARADİGMASI

Ali IŞIKLI

Günümüzde dijitalleşmeyle birlikte, ulusal güvenlik kavramı giderek daha fazla siber alana yayılmaktadır. Bilgisayar sistemlerinin ve internetin yaygın kullanımı, siber saldırıların artmasına ve geleneksel güvenlik tehditlerine yeni boyutlar eklenmesine yol açmaktadır. Bunun yanı sıra siber saldırılar, birçok ülkenin ulusal güvenliğini doğrudan etkileyebilecek kadar ciddi bir tehdit haline gelmiştir. Devletler, casusluk, sabotaj ve altyapıya yönelik saldırılar gibi çeşitli siber tehditlerle karşı karşıya kalmaktadır. Bu tehditlere karşı etkili bir savunma sağlamak için siber caydırıcılık kavramı giderek daha fazla önem kazanmaktadır. Güçlü bir siber savunma kapasitesine yatırım yapmak ve saldırganlara karşı misilleme kabiliyetine sahip olmak, ulusal güvenliğin korunmasında kritik bir rol oynamaktadır.

Siber caydırıcılık, askeri caydırıcılık kavramından esinlenilerek ortaya çıkan bir kavramdır. Askeri caydırıcılık, potansiyel saldırganları, saldırıyı düşünmekten vazgeçmeleri konusunda caydırmayı amaçlayan bir stratejidir. Siber caydırıcılık, bir devletin veya kuruluşun, siber saldırılarla karşı karşıya kalan diğer aktörlere karşı saldırıların olası sonuçlarını önlemek veya azaltmak için kullandığı stratejilerin bir bütünüdür. Bu stratejiler, siber saldırıların engellenmesi, tespit edilmesi, karşı saldırılarla misilleme yapılması veya başka yollarla cezalandırılması gibi çeşitli yöntemleri içerebilir.

Siber caydırıcılığın ana hedefi, potansiyel saldırganları, saldırılarının olası maliyetlerini ve sonuçlarını dikkate alarak saldırıdan vazgeçirmeye teşvik etmektir. Bu, saldırganların olası sonuçları düşünerek eylemlerini gözden geçirmelerini sağlayarak gerçekleştirilir. Siber caydırıcılık, genellikle güçlü siber güvenlik önlemleri, etkili istihbarat toplama ve analiz yetenekleri, hızlı müdahale kapasitesi ve gerektiğinde misilleme kabiliyeti gibi faktörleri içerir.

Siber caydırıcılığın temel unsurlarından biri, güçlü bir siber savunma yeteneğine sahip olmaktır. Bir devlet veya kuruluş, saldırıya karşı etkili bir şekilde savunma sağlayarak saldırganları caydırabilir.

Bir devlet veya kuruluşun siber caydırıcılık stratejisi genellikle saldırıya uğrama olasılığına ve saldırının potansiyel etkisine dayanır. Örneğin, bir ülkenin askeri altyapısı veya kritik kamu hizmetleri, daha yüksek bir koruma seviyesi gerektirebilirken, bir şirketin ticari sırları veya müşteri verileri için daha farklı bir strateji izlenmelidir.

Siber caydırıcılık stratejileri genellikle karmaşık ve çok yönlüdür. Örneğin, bir ülke, saldırganlara karşı caydırıcılık sağlamak için askeri, diplomatik ve ekonomik araçları bir araya getirebilir.

Siber caydırıcılık stratejileri, çeşitli araçlar ve yöntemler kullanılarak uygulanabilir.

Siber caydırıcılığın temel bileşenlerinden biri, güçlü bir siber güvenlik altyapısının oluşturulmasıdır. Bir devlet veya kuruluşun siber güvenlik kapasitesi, saldırganların siber saldırı girişimlerini engellemek veya etkisiz hale getirmek için kritik öneme sahiptir. Güçlü bir siber güvenlik altyapısı, saldırganların ataklarını tespit etme, durdurma ve yanıtlama yeteneğini artırır.

İkinci olarak, etkili bir istihbarat toplama ve analiz kapasitesi, siber tehditlerin tespit edilmesi ve analiz edilmesi için önemlidir. Bu, potansiyel saldırganların niyetlerini ve kabiliyetlerini anlama ve gelecekteki saldırıları öngörebilme yeteneğine dayanır. İstihbarat toplama ve analiz faaliyetleri, siber caydırıcılık stratejisinin temel bir parçası olarak devletlerin veya kuruluşların siber tehditlere yanıt verme kabiliyetini artırır.

Üçüncü olarak, hızlı bir müdahale kapasitesi, bir saldırının tespit edilmesinden sonra hızlı bir şekilde yanıt verme yeteneğini ifade eder. Hızlı bir müdahale, saldırının etkilerini en aza indirgeme ve saldırganların faaliyetlerini sınırlama veya durdurma açısından kritik öneme sahiptir. Bu, hem siber saldırıların hemen durdurulmasını hem de gelecekteki saldırıların önlenmesini sağlar.

Dördüncü olarak, gerektiğinde misilleme kabiliyeti, potansiyel saldırganları siber saldırıların olası sonuçları hakkında ciddi düşünmeye teşvik eder. Siber savunma, siber caydırıcılık stratejisinin sadece bir kısmıdır. Askeri caydırıcılık stratejisinin bir diğer önemli unsuru da saldırganlara karşı misilleme kabiliyetine sahip olmaktır. Bir ülkenin, saldırıya uğraması durumunda karşı saldırı yapabilecek yeteneklere sahip olması, saldırganları düşünmekten caydırabilir. Bu, siber alandaki askeri caydırıcılığın etkili bir şekilde kullanılmasını sağlar. Saldırganların karşılaşacakları muhtemel cezaları vurgulayan net politika ve yasal çerçeveler de siber caydırıcılığın önemli bir parçasıdır Ayrıca, uluslararası iş birliği ve diplomasi de siber caydırıcılığın etkili bir şekilde uygulanmasında önemli bir rol oynar. Bu, siber caydırıcılığın temel bir unsuru olarak, saldırganların saldırılarını dikkate alarak hareket etmelerini sağlar.

Ancak, siber caydırıcılığın bazı sınırlamaları da vardır. Özellikle, siber saldırıların karmaşıklığı ve anonimliği nedeniyle, saldırganların kimliklerini tespit etmek ve doğrudan cezalandırmak genellikle zordur. Ayrıca, uluslararası hukuk ve normlar, siber caydırıcılık stratejilerinin uygulanmasını da sınırlayabilir.

Türkiye, siber caydırıcılık konusunda ciddi bir şekilde çalışmaktadır. Ülke, siber güvenlik altyapısını güçlendirmek ve saldırıları tespit etmek ve engellemek için çeşitli önlemler almaktadır. Ayrıca, Türkiye, uluslararası platformlarda siber güvenlik konusundaki iş birliğini artırmak ve ortak tehditlere karşı birlikte hareket etmek için çaba göstermektedir.

Siber caydırıcılık stratejilerinin etkili bir şekilde uygulanması için sürekli bir çaba gerekmektedir. Teknolojinin sürekli olarak değişmesi ve saldırganların yöntemlerinin gelişmesi, siber güvenlik tehditlerinin de sürekli olarak evirilmesine neden olmaktadır. Bu nedenle, siber caydırıcılık stratejilerinin sürekli olarak gözden geçirilmesi ve güncellenmesi önemlidir.

Gelecekte, siber tehditlerin daha da karmaşık hale gelmesi beklenmektedir. Yapay zekâ, bulut bilişim ve nesnelerin interneti gibi yeni teknolojiler, siber saldırganlara daha fazla fırsat sunabilir. Bu nedenle, siber caydırıcılık stratejilerinin sürekli olarak güncellenmesi ve geliştirilmesi önemlidir.

Bununla birlikte, uluslararası iş birliği de siber tehditlerle mücadelede önemli bir rol oynamaktadır. Ülkeler, siber güvenlik konusunda bilgi ve deneyim paylaşımını teşvik etmeli ve ortak savunma stratejileri geliştirmelidir. Bu, siber saldırılara karşı daha etkili bir savunma sağlayabilir ve askeri caydırıcılığın başarısını artırabilir.

Siber caydırıcılık, geleceğin güvenlik paradigmasını şekillendiren önemli bir kavramdır. Geleneksel güvenlik tehditlerine ek olarak, siber alandaki tehditlerle başa çıkmak için etkili bir strateji ve iş birliği gerekmektedir. Türkiye'nin de bu alandaki çalışmaları, ülkenin siber güvenlikteki başarısını artırmak ve uluslararası alanda daha güçlü bir konum elde etmek için önemlidir.

SİBER SALDIRI METODOLOJİSİ

Evren ESER

Günümüzde internetin ve teknolojik altyapıların yaygınlaşması, siber saldırıları dijital dünyanın en büyük tehditleri haline getirmiştir. Siber saldırganlar, bilgisayar sistemlerini, ağları ve dijital altyapıları hedef alarak, hassas verilere erişim sağlayabilir, hizmet kesintilerine neden olabilir, finansal kayıplara ve hatta can kayıplarına yol açabilirler. Siber saldırıların karmaşıklığı ve çeşitliliği sürekli arttığından dolayı, bu saldırılara karşı etkili önlemler almak da giderek zorlaşmaktadır. Siber saldırı metodolojisini anlamak, bu saldırılara karşı güvenliği sağlamak için kritik bir adımdır. Bu yazıda, siber saldırıların planlanması, yürütülmesi ve sonlandırılmasına kadar geçen süreçte yer alan temel aşamalar ve bu aşamalarda kullanılan başlıca teknikler ayrıntılı bir şekilde ele alınmıştır. Ayrıca, etkili bir siber güvenlik stratejisi geliştirmek için izlenmesi gereken adımlara ve gerekli önlemlere de yer verilmiştir.

Siber saldırı metodolojisi, bilgisayar sistemleri, ağlar ve dijital altyapılar üzerinde gerçekleştirilen saldırıların planlanması, yürütülmesi ve sonlandırılması süreçlerini kapsayan bir dizi adımdan oluşur. Bu metodoloji genellikle saldırganların hedeflerine ulaşmak için izledikleri stratejik ve taktiksel adımları tanımlar. Keşif, erişim sağlama, komuta kontrol, yetki yükseltme, yanal hareket, bilgi toplama ve çıkartma ve iz silme aşamaları siber saldırı metodolojisinin başlıca aşamalardır.

1. Keşif Aşaması

Saldırganların hedef sistem, ağ veya organizasyon hakkında mümkün olduğunca çok bilgi topladığı kritik bir süreçtir. Keşif aşamasında toplanan bilgiler, saldırı planının ve stratejisinin belirlenmesine yardımcı olur. Yeterli ve doğru bilgi toplamak, saldırganın hedef sistemdeki zayıf noktaları daha iyi anlamasını sağlar ve saldırının başarılı olma olasılığını artırır. Keşif aşaması pasif keşif ve aktif keşif olmak üzere iki ana kategoriye ayrılır.

Pasif keşif, hedef sistemlerle doğrudan etkileşime girilmeden hedef hakkında bilgi toplama sürecidir. Bu aşamada saldırganların tespit edilme olasılığı düşüktür. Saldırganlar dikkat çekmeden organizasyon, çalışanlar ve sistemler hakkında bilgi toplarlar. Başlıca pasif keşif kaynakları şunlardır:

- **Sosyal Medya ve Diğer Çevrimiçi Kaynaklar:** Sıklıkla kullanılan sosyal medya platformlarında, haber sitelerinde ve diğer kamuya açık kaynaklarda arama yaparak organizasyon ve çalışanları hakkında bilgi toplama yöntemidir. Toplanılan bu bilgiler arasında çalışanların isimleri, e-posta adresleri, telefon numaraları, organizasyon yapısı, organizasyon bilişim sitemlerinde kullanılan teknolojiler gibi bilgiler bulunabilir.

- **Arama Motorları:** Anahtar kelimeler ve çeşitli teknikler kullanılarak, arama motorları üzerinden hedef organizasyonun teknoloji platformları, personel bilgileri, kurumsal ağ giriş sayfaları, iç ağ portal bilgileri gibi değerli bilgiler bulunabilir. Bu yöntemle, hassas bilgiler, bilinen zafiyetleri içeren sistemler veya yanlış yapılandırılmış sistemler tespit edilebilir.

- Ayrıca WHOIS sorguları alan adının sahibi hakkında bilgiler sağlarken, DNS sorgulamaları ile hedef ağ ile ilgili önemli bilgiler elde edilebilir.

- Çeşitli web sayfaları ve araçlar kullanılarak hedef organizasyonda internete açık bilgisayarların, anahtarlayıcıların (switchlerin), yönlendiricilerin (routerların) işletim sistemleri versiyonları, web sunucuların ise sürümleri tespit edilebilir.

Aktif keşif, saldırganların hedef sistemlerle doğrudan etkileşime girerek bilgi topladığı pasif keşif aşamasına göre daha riskli bir aşamadır. Aktif keşif aşamasında saldırganın varlığı ortaya çıkabilir. Ancak saldırganlar, sistemde kullanılan zafiyetli uygulamalar, kullanıcı listeleri ve ağ topolojisi gibi daha ayrıntılı ve değerli bilgileri elde etmek için bu riski göze alır.

Başlıca aktif keşif teknikleri şunlardır:

- **Ağ Taraması:** Hedef ağdaki aktif cihazları ve açık portları tespit etmek için kullanılan yöntemdir. Nmap gibi ağ tarama araçları, hedefin hangi portlar üzerinde hangi hizmetleri sunduğunu belirlemek için kullanılır. Ağ tarama araçları ile hedef sistemde kullanılan servis sürümleri, işletim sürümü bilgileri, banner bilgileri elde edilebilir, hedef sistemin ağ mimarisi hakkında değerli bilgiler edinilebilir.

- **Zafiyet Taraması:** Hedef sistemdeki potansiyel güvenlik açıklarını belirlemek için kullanılan yöntemdir. Zafiyet taraması sonucunda, sistemde bilinen zafiyetler tespit edilir ve saldırganlar hangi noktaları hedef alabilecekleri konusunda fikir sahibi olur. Zafiyet taraması için otomatik tarama yapan araçlar kullanılabileceği gibi deneyimli saldırganlar otomatik tarama yapan araçların gözden kaçırabileceği açıklıklar için manuel olarak zafiyet analizi de gerçekleştirebilir. Web uygulamaları için özelleşmiş zafiyet tarama araçları; SQL enjeksiyonu, XSS (Cross-Site Scripting) ve CSRF (Cross-Site Request Forgery) gibi yaygın web uygulaması zafiyetlerini keşfetmek için kullanılabilir.

Siber güvenlik uzmanları açısından keşif aşamasını anlamak, potansiyel saldırıları tespit etme ve önleme açısından kritik öneme sahiptir. Pasif keşif sonucunda saldırganlara fayda sağlayacak bilgileri en aza indirmek amacıyla organizasyon bünyesinde siber güvenlik farkındalığı eğitimleri düzenlenmelidir. Ayrıca saldırı tespit ve önleme sistemleri (IDS/IPS) gibi siber güvenlik önlemleri kullanılarak saldırganın aktif keşif aşamasında elde edebileceği bilgiler en aza indirilmelidir ve saldırganın işine yarayacak bilgileri elde etmesi önlenmelidir.

2. Erişim Sağlama Aşaması

Saldırganların keşif aşamalarının sonucunda topladığı bilgiler vasıtası ile geliştirdikleri saldırı stratejilerini uygulayarak hedef sisteme erişim elde etmek için gerçekleştirdiği faaliyetleri kapsar. Saldırganların hedef sistem üzerinde kontrol sağlaması bu aşama sonucunda gerçekleşir. Erişim sağlama aşamasında genellikle şu yöntemler kullanılabilir:

- **Sosyal Mühendislik Saldırıları:** Pasif keşif sonucunda elde edilen hedef organizasyon çalışan isimleri, e-posta adresleri, görevleri, ilgi alanları vb. bilgiler kullanılarak yapılan saldırılardır. Başlıca sosyal mühendislik saldırıları şu şekilde sıralanabilir.

Phishing (Oltalama): Kullanıcılara sahte e-postalar veya mesajlar göndererek onları zararlı yazılım indirmeye veya hassas bilgileri paylaşmaya ikna etme yöntemidir. Phishing saldırılarında genellikle gerçek gibi görünen sahte web siteleri veya dosya ekleri içeren e-postalar kullanılır.

Pretexting (Ön Metin): Saldırganın belirli bir senaryo oluşturarak kurbanı manipüle etmesi yöntemidir. Örneğin, saldırgan kendisini organizasyonun bilgi-işlem destek personeli olarak tanıtıp, kullanıcının parolasını elde etmeye çalışır.

Baiting (Yemleme): İçinde zararlı yazılım bulunan USB Bellek gibi bir fiziksel bir cihaz kullanıcının bulabileceği bir yere (evinin otoparkı vb.) bırakılarak kullanıcının bu cihazı bulup hedef sistemde kullanması beklenir.

- **Zafiyet Sömürme (Exploitation):** Hedef sistemde kullanılan servislerin, yazılımların, işletim sistemlerinin zafiyetlerinden faydalanarak sisteme giriş yapılmasıdır. Yazılımların bilinen açıklıklarını hedef alan istismar kitleri (exploit kit) internette kolayca bulunabilir. Ayrıca zafiyet sömürme için özelleşmiş programlar ile saldırıya uygun yükler (payload) hazırlanabilir. Sal-

dırganların yazılımların henüz keşfedilmemiş ya da geliştiricilerin henüz çözüm üretmediği açıklıkları kullanarak sisteme eriştiği sıfırıncı gün (zero-day) saldırıları da bu kapsamdadır. Sıfırıncı gün saldırıları, özellikle savunmasız sistemler üzerinde yüksek başarı oranına sahiptir.

- **Kötü Amaçlı Yazılımlar (Malware):** Virüs, solucan (worm), Truva atı (trojan) gibi kötü amaçlı yazılımlar hedef sistemlere bulaşarak saldırganların bu sistemlere erişim sağlamasına sebep olurlar. Yine hedef sisteme bulaşıp sistemdeki verileri şifreleyerek kullanıcının bu verilere erişimini engelleyen ve saldırganların fidye talep etmesini sağlayan fidye yazılımları (ransomware) da bu kategoriye dahil edilebilir.

- **Parola Kırma Saldırıları:** Özellikle kullanıcıları karmaşıklık seviyesi yüksek parolalar kullanmaya zorlamayan sistemlerde etkili olan ve saldırganların yaygın olarak kullanılan parolaları sistematik olarak deneyerek sisteme erişmesine sebep olabilen yöntemidir.

Erişim sağlama aşaması, saldırganların hedef sistemde kalıcı bir yer edinme çalışmalarının merkezinde yer alır. Saldırganların bu aşamada amaçlarına ulaşması, saldırının diğer aşamalarını mümkün kılar. Dolayısıyla, bu aşamanın anlaşılması ve etkili savunma stratejilerinin uygulanması, sistem güvenliği için hayati önem taşır. Organizasyon içi sosyal mühendislik farkındalığı eğitimleri, sistemlerle etkileşim için güçlü parola politikaları ve çok faktörlü kimlik doğrulaması, sistemlerin ve yazılımların düzenli olarak güncellenmesi ve güvenlik yamalarının uygulanması, saldırı tespit ve önleme sistemlerinin aktif edilmesi, antivirüs yazılımlarının kullanılması gibi önlemler sistemlere yetkisiz erişimi engelleyebilecek ana önlemler olarak sıralanabilir.

3. Komuta Kontrol Aşaması:

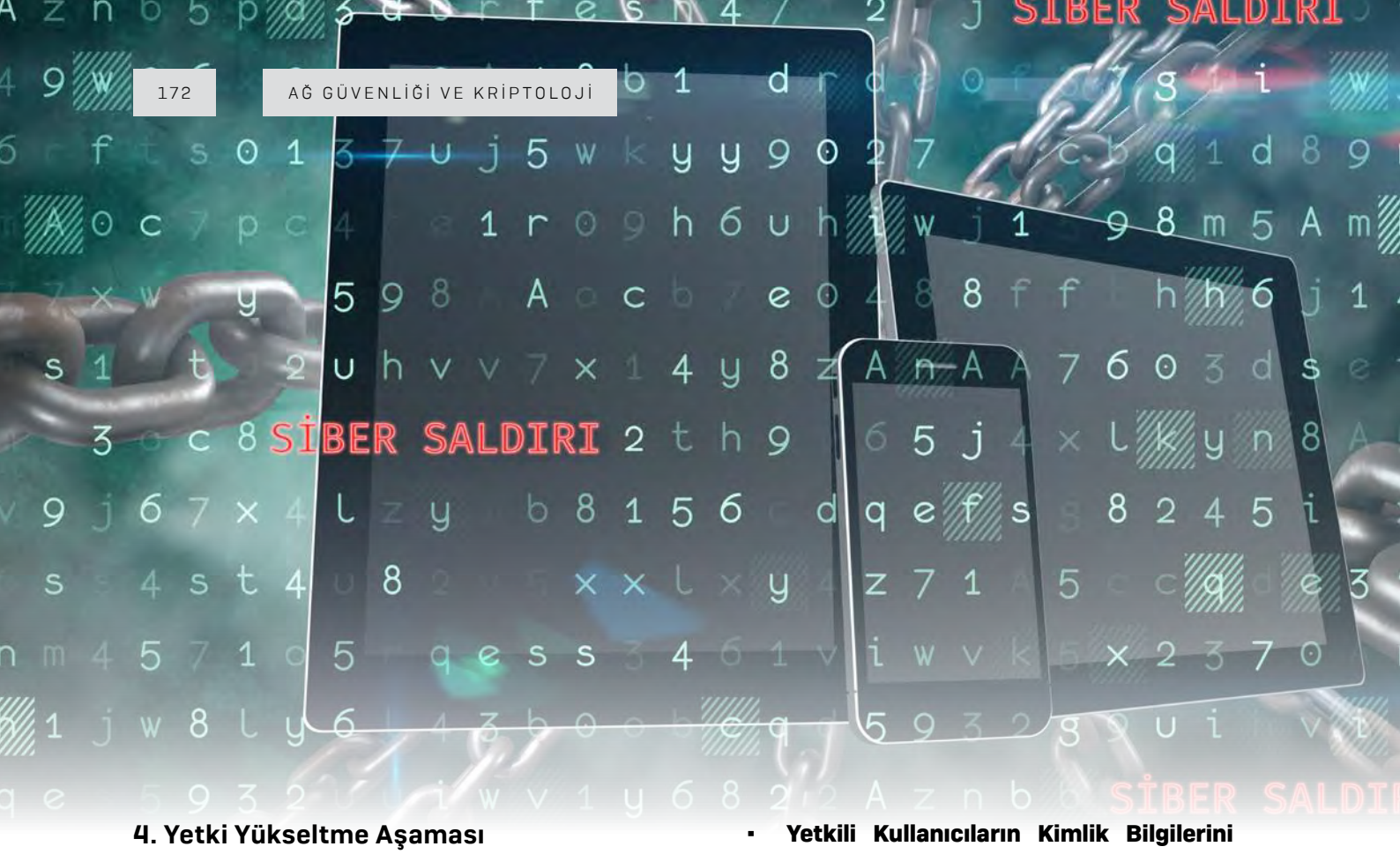
Bu aşamada saldırgan, ele geçirilen sistemlerle iletişim kurarak onları kontrol etmeye çalışır. Saldırganlar genellikle tespit edilmekten kaçınmak için olağan trafiği taklit etmeye çalışır. Saldırganın tespit edilmemek için kullandığı başlıca yöntemler şunlardır:

- **Uygulama katmanı protokolleri:** Halihazırda sistemde kullanılan ssh, rdp, smb gibi uygulama protokolleri kullanarak hedef sistemi yönetebilirler.

- **Proxy:** Saldırganlar, hedef sisteme olan ağ trafiğini yönlendirmek ve kontrol etmek için bir bağlantı proxy kullanabilirler. Bu tür proxy'ler komuta ve kontrol iletişimini yönetmek, eşzamanlı giden ağ bağlantılarının sayısını azaltmak, bağlantı kaybı durumunda esneklik sağlamak veya şüphe oluşturacak trafik oluşturmamak için en sık kullanılan araçlardır. Saldırganlar, kötü amaçlı trafiğin kaynağını daha da gizlemek için birden fazla Proxy kullanarak, Proxy zinciri (Proxy chain) oluşturabilirler.

- **Protokol Tüneli:** Saldırganlar, fark edilemeden hedef sistem ile olan iletişimlerini ayrı bir protokol içine tünelleyebilir. Tünel oluşturma, bir protokolün diğer bir protokolün içine kapsüllenmesidir. Ssh tünelleme, http tünelleme en sık kullanılan protokol tünelleme yöntemleridir.

Komuta kontrol aşaması, saldırganların hedef sistem üzerinde komutlarını iletebilmesi, veri toplayabilmesi ve uygulama yükleyebilmesi için gereken altyapıyı oluşturur. Komuta Kontrol iletişiminin başarılı bir şekilde kurulması ve sürdürülmesi, saldırının etkinliğini ve kalıcılığını artırır. Güvenlik önlemleri olarak ağ trafik analizi, anomali tespit sistemleri göz önünde bulundurulmalıdır.



4. Yetki Yükseltme Aşaması

Saldırganların hedef sistemde düşük seviyeli erişim elde ettikten sonra, daha yüksek seviyeli izinler ve ayrıcalıklar elde etmeye çalıştıkları bir süreçtir. Bu aşama, saldırganların hedef sistem üzerinde tam kontrol sağlamalarını amaçlar. Yetki yükseltme aşaması, genellikle hedef sisteme erişim sağlanıp, sistem dikkatlice analiz edilip sistemdeki varsa zafiyetli yazılımlar, işletim sistemi dosyaları, hatalı yapılandırılmış kullanıcı ve dosya izinleri istismar ederek gerçekleştirilir.

Bu aşamada Linux ve Windows hedef sistemlerde sırasıyla LinPeas ve WinPeas gibi otomatikleştirilmiş tarama araçları kullanılabilir. Bu araçlar hedef sistemde yetki yükseltmeye sebep olabilecek zafiyetleri detaylı olarak sıralar. Başlıca yetki yükseltme teknikleri şu şekilde sıralanabilir.

- **Yerel Yetki Yükseltme (Local Privilege Escalation):** İşletim sistemi, uygulamalar veya hizmetlerdeki güvenlik açıklarının istismar edilmesi, hatalı veya eksik yapılandırılmış dosya izinleri, Unix tabanlı sistemlerde, SUID (Set User ID) veya SGID (Set Group ID) bitlerine sahip programlar, zamanlanmış görevlerin hatalı yapılandırılması gibi zafiyetler saldırganların yetkilerini yükseltmelerine sebep olabilir.
- **Yetkili Kullanıcıların Kimlik Bilgilerini Elde Etme:** Hedef sistemde bulunan konfigürasyon dosyaları, parola dosyaları, kayıt defteri anahtarları, kullanıcı veritabanları yanı sıra sistemin belleğinde saklanan parola özet değerleri, (hash value) veya oturum belirteçleri (token) saldırganın yetkisini yükseltmek için kullanabileceği başlıca kaynaklardır. Bunlar dışında saldırganın sisteme kuracağı keylogger ya da ağ trafiğini dinleme sonucunda elde edeceği bilgiler de yetki yükseltme aşamasında kullanılabilir.

Yetki yükseltme aşamasının başarılı bir şekilde gerçekleştirilmesi saldırganlara sistemde tam bir kontrol sağlar. Saldırganlar sistemdeki tüm verilere erişebildiği gibi, sistemde tespit edilmeden uzun süreli kalıcılık sağlamak için çalışmalar yapabilir, hedef ağda bulunan diğer sistemlere ulaşmak için uygulamalar yükleyebilir, verileri sızdırabilir, kayıt ve log dosyalarını değiştirip izlerini yok edebilirler. Siber güvenlik önlemleri açısından düşünürsek önceki aşamalar için tasarlanan önlemlere ek olarak, sistemleri, dosyaları ve kullanıcı haklarını doğru yapılandırmak, kullanıcılara ve hizmetlere sadece ihtiyaç duydukları minimum yetkileri vermek (en az ayrıcalık ilkesi) kritik öneme sahiptir.

5. Yanal Hareket Aşaması

Yanal hareket (Lateral Movement) aşaması, bir siber saldırganın bir ağa sızdıktan sonra ağ içerisindeki diğer sistemlere veya cihazlara erişim sağlamak için yaptığı faaliyetleri kapsar. Bu aşama, saldırganın belirli bir hedefe ulaşmak, hassas verilere erişmek veya kontrolü ele geçirmek için ağdaki yatay yayılımını ifade eder.

Yanal hareket aşaması genelde şu şekilde açıklanabilir:

Saldırgan, ağda hangi cihazların mevcut olduğunu, hangi servislerin çalıştığını ve hangi açıkların bulunduğunu, ağdaki kullanıcı hesaplarını, servis hesaplarını ve bu hesapların haklarını öğrenir. Elde ettiği hesap bilgileri ile diğer sistemlere erişmeye çalışır. Çeşitli araçlar kullanılarak bellekte bulunan parola hash'leri ve diğer kimlik bilgilerini toplar. Saldırgan ele geçirdiği hash, bilet (ticket) bilgileri ve jetonları (token) tekrar kullanılarak yan sistemlere erişim sağlar. PowerShell, PsExec, RDP gibi Uzaktan Yönetim Araçlarını kullanılarak diğer sistemlerde kontrolü ele geçirir ve yönlendirir. Diğer sistemlerde de yetki yükseltme, kalıcılık, veri sızdırma, yan hareket gibi amaçlarına yönelik çalışmalara devam eder.

Yanal hareket aşaması, bir saldırının ağ içinde yayılmasını ve etkisini artırmasını sağlayan kritik aşamadır. Siber güvenlik önlemleri olarak güvenlik duvarları, saldırı tespit ve önleme sistemleri, sistemin kayıtlarının sürekli olarak izlenmesi, ağların bölümlendirilmesi (segmentation) gibi önlemler kritik öneme sahiptir.

6. Bilgi Toplama ve Çıkartma Aşaması

Bilgi toplama ve çıkartma (Data Exfiltration) aşaması, siber saldırganların hedef sistemden hassas ve değerli bilgileri elde edip bu bilgileri dışarıya sızdırdığı aşamadır. Bu aşamada, saldırının nihai amaçlarından olan veri hırsızlığı genellikle gizli bir şekilde gerçekleşir. Saldırganların hedefinde genellikle kullanıcı adları, parolalar, kişisel bilgiler, finansal veriler, ticari veriler, e-posta yazışmaları, müşteri bilgileri gibi önemli bilgiler yer almaktadır.

Bilgi toplama süreci şu tekniklerle gerçekleştirilir:

Saldırganlar genellikle dosya sistemlerini veya veritabanlarını, RAM'de bulunan geçici verileri ya da ağ üzerinden geçen verileri analiz ederek hassas verilere ulaşırlar. Bu verileri çıkartmak için de çeşitli yöntemlere başvururlar.

- **Ağ Üzerinden Çıkartma:** Hassas verilerin e-posta ekleri olarak gönderilmesi, FTP/SFTP gibi dosya transfer protokollerin kullanılması, bir web sunucuya verilerin yüklenmesi, yaygın kullanılan bulut depolama hizmetlerini kullanarak verilerin çıkarılması en yaygın yöntemdir.
- **Şifreleme ve Gizleme:** Saldırganlar, hedef sistemdeki verileri komuta kontrol kanalı üzerinden DNS Tünelleme, HTTP tünelleme gibi normal trafik içerisine gizleyerek çıkarabilirler. Çıkartılan verilerin şifrelenerek gönderilmesi ise tespit edilmesi ve analiz edilmesini zorlaştırılır.

Bilgi toplama ve çıkartma aşaması, siber saldırının en kritik ve zarar verici aşamalarından biridir. Bu nedenle, bu aşamaya karşı güçlü bir savunma hattı oluşturmak ve proaktif önlemler almak, kurumların bilgi güvenliğini korumada hayati önem taşır. Önceki aşamalarda siber güvenlik önlemlerine ek olarak Veri Sızdırma Koruma (Data Leak/Loss Protection) politikalarının etkinleştirilmesi çok önemlidir.

7. İz Silme Aşaması

İz silme aşaması, siber saldırganların hedef sistemde gerçekleştirdikleri faaliyetlerin tespit edilmesini önlemek için izlerini sildikleri aşamadır.

İz silme aşamasında kullanılan teknikler ve yöntemler şu şekilde açıklanabilir:

- **Kayıt (Log) Temizleme ve Manipülasyon:** Saldırgan, sistemdeki faaliyetlerinin izlerini silmek veya değiştirmek için sistem ve uygulama kayıt dosyalarını silerek, saldırganın faaliyetlerini belgeleyen kayıtların ortadan kaldırılmasını sağlar. Bazen de saldırgan; güvenlik ekiplerinin, olay akışını doğru anlamasını zorlaştırmak için kayıtlara yanıltıcı bilgiler ekler, mevcut kayıtları değiştirir veya zaman bilgilerini manipüle eder. Bu şekilde saldırgan, sistemdeki faaliyetlerinin izlerinin bulunmasını neredeyse imkansız hale getirebilir.

- **Anti-Forensic Araçlar ve Teknikler:** Saldırgan, adli analiz süreçlerini zorlaştırmak için anti-forensic araçlar ve teknikler kullanır. Disk temizleme araçları, bellek temizleme araçları saldırı izlerini silmek için çoğunlukla kullanılır.

Bu aşamada, saldırganların faaliyetlerini önlemek için kapsamlı Log Kaydı ve İzleme araçları, Uç Nokta Tespit ve Müdahale (EDR) araçları göz önünde bulundurulabilir. Ayrıca sistemlerin, uygulamaların ve kullanıcıların ürettiği kayıtlar için merkezi kayıt sunucuları kullanılabilir. Bu sunucular ağ üzerindeki tüm cihazlardan ve uygulamalardan gelen kayıt verilerini toplamak, depolamak, analiz etmek, raporlamak için özelleşmiş sanal ya da fiziksel sunuculardır.

Sonuç olarak, siber saldırı metodolojisi, siber tehditleri ve saldırgan davranışlarının daha iyi anlaşılması ve önlenmesi açısından kritik bir öneme sahiptir. Siber saldırı metodolojisinin iyi analiz edilmesi siber güvenlik ekiplerine daha kapsamlı ve etkili bir savunma stratejisi geliştirme imkânı tanır. Siber tehditlerin sürekli geliştiği, karmaşık hale geldiği ve çeşitlendiği dijital dünyada tehditlere karşı hazırlıklı olmak için saldırı metodolojisini çok iyi anlamalı, saldırganların bakış açısını öğrenmeli ve bu şekilde güçlü bir savunma hattı oluşturmalıyız.

DEVSECOPS

Dr. Adnan KILIÇ

DevSecOps, güvenlik uygulamalarını DevOps sürecine entegre eden bir metodoloji ve kültürdür. DevSecOps, geliştirme (Dev), güvenlik (Sec) ve operasyonların (Ops) birleşimidir ve yazılım geliştirme yaşam döngüsünün (SDLC) her aşamasına güvenliği entegre etmeyi amaçlar. Tasarımdan geliştirmeye, testten dağıtıma ve yazılım teslimatına kadar yazılım geliştirme sürecinin tüm aşamalarında otomasyon, izleme ve sıkı entegrasyonu vurgular.

DevSecOps'un önemi, işletmelerin müşteri talebini karşılamak ve rekabetçi kalmak için sürekli teslimat döngülerine giderek daha fazla bağımlı hale gelmesiyle önemli ölçüde artmıştır. Bu yüksek tempolu ortamda, genellikle geç aşama değerlendirmeleri ve kontrolleri içeren geleneksel güvenlik yaklaşımları artık geçerli değildir. Güvenlik ihlalleri ve zafiyetler, mali ve itibar açısından yıkıcı etkilere sahip olabilir, bu da erken ve entegre güvenlik önlemlerinin kritik hale gelmesini sağlar.

Yazılım Geliştirme Metodolojilerinin Evrimi

Yazılım geliştirme metodolojilerindeki gelişim ve ilerleme teknolojinin evrimini ve yazılım uygulamalarının değişen taleplerini yansıtır. Bu tarih, katı, doğrusal yaklaşımlardan daha esnek, yinelemeli metodolojilere doğru bir kaymayı işaret eder; iş birliği ve uyum yeteneğini vurgular.

Şelale modelinden Agile, DevOps ve DevSecOps'a geçiş esneklik, iş birliği ve değişime hızlı uyum gibi, günümüzün hızlı tempolu ve teknoloji odaklı dünyasında hayati öneme sahip özelliklere öncelik veren metodolojilere doğru daha geniş bir hareketi yansıtır.

Şelale (Waterfall) Modeli

Şelale modeli, yazılım geliştirme ve proje yönetimine yönelik doğrusal ve ardışık bir yaklaşımdır. Süreç birkaç aşamadan oluşur ve sürekli olarak aşağı doğru (bir şelale gibi) akar. Bu aşamalar genellikle gereksinim, analiz, tasarım, derleme, doğrulama ve test, dağıtım ve bakımı içerir. Yeni aşama başlamadan önce bu aşamadan önce gelen her aşama tamamlanmalıdır. Bu yöntem, çok açık hedefleri ve sabit gereksinimleri olan projeler için tercih edilir.

Çevik (Agile)

Çevik, sürekli teslimat, takım iş birliği, müşteri geri bildirimi ve değişikliklere hızlı yanıt verebilme yeteneğini vurgulayan esnek, yinelemeli bir yazılım geliştirme yaklaşımıdır. Proje, genellikle birkaç hafta süren sprintler veya yinelemeler olarak adlandırılan küçük, yönetilebilir birimlere bölünür. Çevik metodolojiler, sık denetim ve adaptasyonu teşvik eden disiplinli bir proje yönetimi sürecini, takım çalışmasını, organizasyonu ve sorumluluğu teşvik eden bir liderlik felsefesini, yüksek kaliteli yazılımların hızlı teslimatını sağlayan mühendislik uygulamaları setini ve geliştirmeyi müşteri ihtiyaçları ve şirket hedefleriyle hizalayan bir iş yaklaşımını teşvik eder. Scrum, Kanban ve Extreme Programming (XP), en popüler çevik metodolojileri arasındadır.

DevOps

DevOps, yazılım geliştirme yaşam döngüsünü kısaltmayı ve yüksek yazılım kalitesi ile sürekli teslimat sağlamayı amaçlayan bir uygulama ve kültür hareketidir. DevOps yalnızca otomasyondan ibaret değildir. Aynı zamanda geliştirme (Development - Dev) ve operasyon (Operation - Ops) ekiplerini entegre ederek altyapının otomatize edilmesini amaçlar. İş akışlarının otomatize edilmesi ve uygulama performansının sürekli olarak ölçülmesi yoluyla verimliliği artırmayı da içerir. Yazılım geliştiriciler, kalite güvencesi ve IT operasyonları arasındaki iletişim ve iş birliğinin önemini vurgular. DevOps, yazılım geliştirme ve teslimatında birleşik bir yaklaşımı teşvik etmeyi amaçlar.

DevSecOps

DevSecOps, güvenlik uygulamalarını DevOps sürecine entegre ederek DevOps yaklaşımını genişletir. Güvenlik kontrollerini ve süreçlerini DevOps akışına yerleştirerek temel güvenlik görevlerini otomatize etmeyi amaçlar. IT ve güvenlik arasındaki geleneksel boşlukları kapatmayı ve kodun hızlı, güvenli teslimatını sağlar. DevSecOps modelinde, güvenlik, projenin başlangıcından emekliğe ayrılmasına kadar olan tüm yaşam döngüsü boyunca paylaşılan bir sorumluluk olarak kabul edilir. Bu metodolojiler, geleneksel yazılım geliştirme ve proje yönetimi yaklaşımlarından daha uyarlanabilir, işbirlikçi ve teknoloji odaklı uygulamalara doğru bir kaymayı yansıtır. Her biri farklı türdeki projeler ve kurumsal ortamlar için uygun olan güçlü yönleriyle öne çıkar.

DevSecOps'un Temel İlkeleri

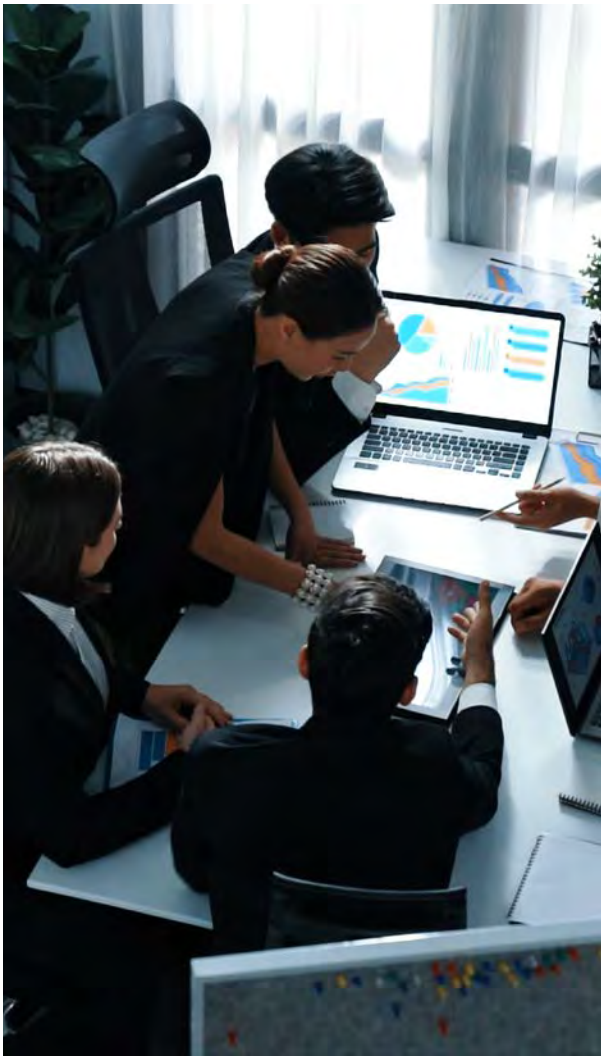
DevSecOps, yazılım geliştirme ve operasyonlarının tüm yönleri üzerinde derinlemesine ve geniş kapsamlı güvenlik uygulamalarını entegre eder. Uygulamaların yaşam döngüsünün başından itibaren yaşam döngüsü boyunca güvenliği yerleştirerek, DevSecOps hızlı yayın döngüleri ile güvenli geliştirme arasındaki boşluğu kapatmayı amaçlar. DevSecOps ilkeleri sadece güvenliği daha erken ("sola kaydırma") ve yaşam döngüsü boyunca sürekli olarak ("sağa kaydırma") dahil etmekle ilgili değildir.

Bu temel ilkelerin bazılarını dayandıkları kavramlar ile birlikte aşağıdaki gibi açıklayabiliriz:

1) Güvenlik, Ortak Bir Sorumluluktur

Güvenlik, DevSecOps'ta herkesin sorumluluğundadır. Güvenlik, ayrı bir güvenlik ekibinin tek sorumluluğu olmaktan çıkıp, geliştiricilerin, operasyon personelinin ve kalite personelinin günlük iş akışlarının ayrılmaz bir parçası haline gelir.

İş birliği ve İletişim: Ekipler arasındaki bariyerleri kaldırmak için geliştiricilerin, operasyonların ve güvenlik personelinin sorunsuz bir şekilde birlikte çalışmaları sağlanır.



2) Güvenliği Sola Kaydırma

"Güvenliği sola kaydırma" ilkesi, gereksinim toplama ve tasarım aşamalarından başlayarak, geliştirme yaşam döngüsünün erken aşamalarında güvenlik önlemlerini entegre etmeyi ifade eder.

Tasarımıyla Güvenli: Uygulamaların tasarım ve mimarisine güvenlik düşünceleri dahil edilerek, geliştirme başlamadan önce risklerin ele alınması hedeflenir.

Güvenlik Testlerinin Otomasyonu: Sürekli entegrasyon (Continuous Integration, CI) hattının bir parçası olarak Statik Uygulama Güvenlik Testi (SAST), Dinamik Uygulama Güvenlik Testi (DAST) ve Etkileşimli Uygulama Güvenlik Testi (IAST) gibi otomatik güvenlik testleri uygulanır.

3) Güvenliği Sağa Kaydırma

"Güvenliği sağa kaydırma", üretime ve dağıtımdan sonra güvenliğe odaklanmayı içerir. Canlı ortamlarda ortaya çıkabilecek yeni zafiyetlerin belirlenmesi ve hafifletilmesi için hayati önem taşımaktadır.

Gerçek Zamanlı Tehdit Tespiti: Potansiyel güvenlik tehditleri üzerine gerçek zamanlı uyarılar sağlayan izleme araçları devreye alınır.

Sürekli Güvenlik Güncellemeleri ve Yama Yönetimi: Zafiyetlere maruz kalmayı azaltmak için güvenlik güncellemelerini ve yamalarını sürekli olarak teslim eden otomatik sistemler uygulanır.

4) Otomasyon ve Entegrasyon

DevSecOps'taki otomasyon, geliştirme aşamalarından bakım aşamalarına kadar uzanır, insan hatasının azaltılmasını ve güvenlik politikalarının tutarlı uygulanmasını sağlar.

CI/CD Entegrasyonu: Her derleme işleminin dağıtılmadan önce güvenlik ihlalleri için otomatik olarak test edilmesini sağlamak üzere güvenlik araçları Sürekli Entegrasyon / Sürekli Dağıtım (CI/CD) hatlarına doğrudan entegre edilir.

Konfigürasyon Yönetimi: Konfigürasyonları yönetmek için kod kullanmak, çevreler arasında güvenlik ayarlarını standartlaştırmaya yardımcı olur ve konfigürasyon sapmasını azaltır.

5) Risk Yönetimi

DevSecOps'ta risk yönetimi, potansiyel etkilerine dayanarak riskleri tanımlamayı, değerlendirmeyi, önceliklendirmeyi içerir ve zamanında ele alınmalarını sağlar.

Proaktif Risk Değerlendirmesi: Potansiyel güvenlik tehditlerini ve zafiyetlerini düzenli olarak değerlendirerek, risk seviyelerine göre önceliklendirilmesidir.

Olay Yanıtı: Potansiyel güvenlik ihlallerini hızlı ve etkin bir şekilde ele almak için olay yanıt planları geliştirilir ve düzenli olarak güncellenir.

6) Sürekli İyileştirme

Siber güvenlik tehditleri sürekli olarak değişmektedir, bu da güvenlik uygulamalarının sürekli olarak yeniden değerlendirilmesini ve iyileştirilmesini gerektirir.

Geri Bildirim Döngüleri: Operasyonlar ve üretimden geliştirmeye geri bildirim mekanizmaları uygulamak, uygulamaların güvenlik özelliklerini iyileştirmeye yardımcı olur.

Eğitim ve Farkındalık: Tüm takım üyelerinin en son güvenlik tehditleri ve en iyi uygulamalar konusunda bilgili olmalarını sağlamak için eğitim programları düzenlenir.

7) Uygunluk ve Yönetişim

DevSecOps, düzenleyici gereksinimlere uyumu sağlamak ve yönetişim standartlarını sürdürmek için hayati önem taşır.

Otomatik Uygunluk Kontrolleri: Geliştirme ve dağıtım süreçleri boyunca güvenlik standartlarına ve yönetmeliklere uyumu doğrulamak için otomatik araçlar kullanılır.

Denetim İzi: Sisteme yapılan tüm değişiklikler için kapsamlı günlükler tutulur, sorunlar oluştuğunda kapsamlı soruşturmalar yapmak kolaylaşır.

Bu ilkeler, uygulamaların yaşam döngüsü boyunca, analizden geliştirmeye, dağıtımdan işletmeye kadar güvenliğin sürekli göz önünde olduğu sağlam bir DevSecOps stratejisinin temellerini oluşturur.

Güvenli Yazılım Geliştirme Yaşam Döngüsü (SSDLC)

Güvenli Yazılım Geliştirme Yaşam Döngüsü (SSDLC), güvenlik önlemlerini doğrudan Yazılım Geliştirme Yaşam Döngüsü'ne (SDLC) entegre eden bir yaklaşımdır. Güvenliği sürecin erken aşamalarında ve sürekli olarak dahil ederek, güvenliğin yazılım geliştirme sırasında bir son düşünce olmaktan çıkıp temel bir yön haline gelmesini sağlar. Bu proaktif yaklaşım, zafiyetleri önemli ölçüde azaltır ve nihai ürünün güvenlik duruşunu iyileştirir.

SSDLC'nin Aşamaları

SSDLC, SDLC'nin geleneksel aşamalarını yansıtır ancak belirli güvenlik görevleri ve kontrol noktaları içerir. Güvenliğin nasıl entegre edildiğine dair her aşamanın özetini aşağıdaki gibi açıklayabiliriz:

1) Gereksinim Analizi

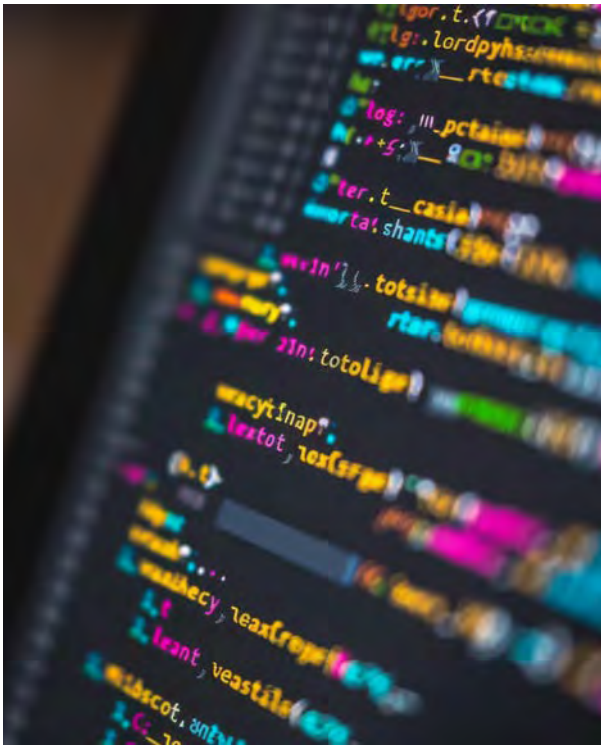
Güvenlik Gereksinimleri: Fonksiyonel gereksinimlerin yanı sıra güvenlik gereksinimleri tanımlanır. Bu, güvenlik yönetişim standartlarını belirlemeyi, uygunluk ihtiyaçlarını belirlemeyi ve güvenlik hedeflerini tanımlamayı içerebilir.

Risk Değerlendirmesi: Sistemi etkileyebilecek potansiyel tehditleri ve zafiyetleri anlamak için genel bir risk değerlendirmesi yapılır.

2) Tasarım

Tasarımdaki potansiyel tehditleri tanımlamak, kategorize etmek ve analiz etmek için tehdit modellemesi yapılır. Bu, baştan itibaren önlemleri tasarlamaya yardımcı olur.

Güvenli Mimari: En iyi güvenlik uygulamalarını içeren güvenli bir mimari plan geliştirilir, örneğin en az ayrıcalık, derinlemesine savunma gibi güvenli tasarım ilkeleri ve kalıpları kullanılır.



3) Uygulama

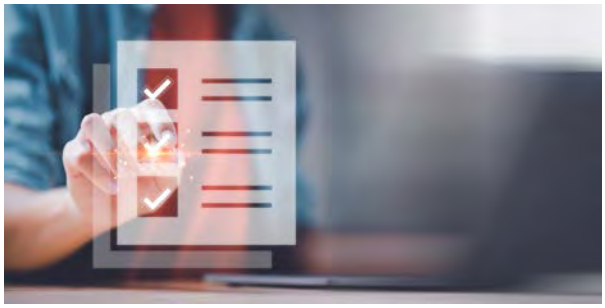
Güvenli Kodlama Pratikleri: SQL enjeksiyonu, siteler arası betik çalıştırma (XSS) ve arabellek taşmaları gibi yaygın, kodlamadan kaynaklı zafiyetlerinden kaçınmak için güvenli kodlama yönergeleri uygulanır. Güvenlik kusurlarını tespit etmek için kod analiz araçları kullanılır.

Kod İncelemesi: Güvenlik sorunlarını belirlemeye odaklanarak düzenli kod incelemeleri yapılır. Bu, manuel olarak veya otomatik araçlar aracılığıyla yapılabilir.

4) Test

Güvenlik Testi: Kapsamlı güvenlik testi entegre edilir, bunlar arasında Statik Uygulama Güvenlik Testi (SAST), Dinamik Uygulama Güvenlik Testi (DAST) ve sızma testi bulunur.

Düzeltme: Test sırasında belirlenen güvenlik zafiyetleri düzeltilir ve düzeltilip düzeltilmediğinden emin olmak için yeniden test yapılır.



5) Dağıtım

Güvenli Dağıtım Uygulamaları: Yazılımın yayınlanması sırasında güvenliği korumak için güvenli dağıtım uygulamaları takip edilir. Bu, tüm güvenlik ayarlarının doğru şekilde uygulandığından emin olmak için konfigürasyon yönetimini içerir.

Değişiklik Yönetimi: Herhangi bir değişiklik için güvenlik etki analizini içeren katı bir değişiklik yönetim süreci uygulanır.

6) Bakım

Sürekli İzleme: Tehditleri gerçek zamanlı olarak tespit etmek ve yanıt vermek için sürekli izleme araçları kullanılır.

Yama Yönetimi: Yeni keşfedilen zafiyetleri ele almak için devam eden bir yama yönetimi süreci geliştirilir ve uygulanır.

7) Tasfiye

Güvenli Veri Tasfiyesi: Yazılımın ömrünün sonunda veya artık gerekli olmadığında tüm hassas verilerin ve kaynakların güvenli bir şekilde tasfiye edilmesi sağlanır.

Güvenlik Entegrasyonu

Güvenliği, SSDLC'nin her aşamasına entegre etmek, birkaç önemli uygulama içerir:

Güvenlik Otomasyonu: Mümkün olduğunda, güvenlik testleri ve izlemesi gibi güvenlik görevleri otomatize edilir. Otomasyon, tutarlılığı sağlar ve insan hatasını azaltır.

Sürekli İyileştirme: SSDLC yinelemelidir. Her sürümden sonra, güvenlik performansı üzerine geri bildirim toplanır ve bir sonraki döngüde güvenlik uygulamalarını iyileştirmek için kullanılır.

Eğitim ve Farkındalık: Tüm takım üyeleri güvenlik tehditleri ve önlemleri konusunda eğitimli ve bilgili tutulur. Bu, geliştiricileri güvenli kodlama uygulamaları konusunda eğitmeyi içerir.

SSDLC yaklaşımını takip ederek, organizasyonlar yazılım ürünleriyle ilişkili güvenlik zafiyetleriyle ilgili riskleri büyük ölçüde minimize edebilir. Ayrıca,

güvenliği geliştirme sürecine entegre etmek, düzenleyici gereksinimlere uyumu sadece kolaylaştırmakla kalmaz, aynı zamanda müşterilere güvenlik konusundaki taahhüdü göstererek güven inşa eder.

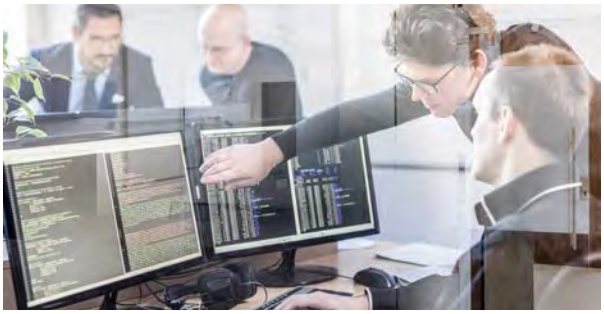
DevSecOps ve SSDLC Arasındaki İlişki

DevSecOps ve SSDLC, güvenliğin yazılım geliştirmede temel bir bileşen olarak yer alması gerektiği ihtiyacına yanıt olarak ortaya çıkmıştır. İkisi arasındaki ilişki, birbirlerini nasıl tamamladıkları ve güçlendirdikleri üzerinden anlaşılabilir:

Felsefi Uyum: Hem DevSecOps, hem de SSDLC, güvenliğin başlangıçtan itibaren entegre edilmesi ve yazılımın yaşam döngüsü boyunca sürdürülmesi gerektiği ilkesine dayanır. DevSecOps, SSDLC'nin gerçek dünya, sürekli dağıtım ortamında başarılabilir olmasını sağlayan kültürü ve uygulamaları getirir.

Pratik Uygulama: DevSecOps, SSDLC tarafından öngörülen güvenlik önlemlerini uygulamak için pratik araçlar (araçlar, uygulamalar, kültür) sağlar. Örneğin, DevSecOps'ta kullanılan otomasyon araçları, geliştirme aşamalarının her birinde SSDLC tarafından zorunlu kılınan güvenlik kontrollerini otomatize edebilir.

Birbirlerini Güçlendirme: SSDLC'yi bir DevSecOps çerçevesi içinde uygulayarak, organizasyonlar güvenliğin sadece planlanmadığını, aynı zamanda etkin bir şekilde uygulandığını gözlemleyebilir. DevSecOps uygulamaları olan sürekli entegrasyon ve sürekli teslimat (CI/CD), değişikliklerin hızlı ve güvenli bir şekilde dağıtılmasını sağlar, bu da güvenlik güncellemelerinin ve yamalarının mümkün olan en kısa sürede uygulanmasını garanti eder.



Sürekli İyileştirme: Her iki çerçeve de güvenlik sorunlarını proaktif bir şekilde belirlemeye ve ele almaya yardımcı olan sürekli izleme ve geri bildirim döngülerini savunur. Bu sürekli iyileştirme yaklaşımı hem güvenlik uygulamalarını hem de geliştirme uygulamalarını geliştirmeye yardımcı olur.

Tehdit Modellemesi ve Risk Değerlendirmesi

Tehdit modellemesi ve risk değerlendirmesi, güvenli bir yazılım geliştirme yaşam döngüsünün (SSDLC) kritik bileşenleridir. Bu süreçler, geliştirme sürecinin erken aşamalarında potansiyel güvenlik tehditlerini ve zafiyetlerini belirlemek ve riskleri önceliklendirerek yazılım dağıtılmadan önce en önemli tehditlerin ele alınmasını sağlamak için tasarlanmıştır.

Tehdit Modellemesi Nedir?

Tehdit modellemesi, bir uygulamaya veya sisteme yönelik potansiyel tehditleri, zafiyetleri ve potansiyel saldırıları belirlemek, sıralamak ve önceliklendirmek için proaktif bir yaklaşımdır. Tehdit modellemesinin ana amacı, sistem doğası, potansiyel saldırganların tahmini profili, olası saldırı vektörleri ve bir saldırganın en çok arzu ettiği varlıklar göz önünde bulundurularak hangi kontrollerin veya savunmaların dahil edilmesi gerektiği konusunda geliştiricilere ve güvenlik ekiplerine sistematik bir analiz sağlamaktır.

Tehdit Modelleme Yöntemleri

1) STRIDE: Microsoft tarafından geliştirilen STRIDE, tehditleri altı türde sınıflandırır: Sahtecilik (Spoofing), Tahrifat (Tampering), İnkâr (Repudiation), Bilgi İfşası (Information Disclosure), Servis Kesintisi (Denial of Service) ve Yetki Yükseltme (Elevation of Privilege). Bu, bir sistemi etkileyebilecek tehdit türlerini anlamaya yardımcı olur.

2) PASTA: Yedi adımlı, risk merkezli bir metodolojidir. İş hedeflerini ve teknik gereksinimleri entegre etmeye, gerçek dünya verilerine dayanarak potansiyel saldırı vektörlerini analiz etmeye odaklanır.

Risk Değerlendirmesi Nedir?

SSDLC bağlamında risk değerlendirmesi, bir olayın olasılığına ve potansiyel etkisine dayanarak riskleri tanımlamak, niceliklendirmeve önceliklendirme sürecidir. Bir sistemin veya uygulamanın zayıf yönlerini istismar edebilecek olası tehditleri ve zafiyetleri belirlemeyi amaçlar.

Geliştirme Aşamaları Boyunca Risk Değerlendirme Teknikleri

Gereksinim Toplama Sırasında: Sistemin işlevsel gereksinimleriyle birlikte güvenlik gereksinimleri tanımlanır. Potansiyel güvenlik sorunlarını öngörmek için yüksek seviyeli tasarım ve mimariye dayalı bir başlangıç risk değerlendirmesi yapılır.

Tasarım Sırasında: Tasarımı analiz etmek ve potansiyel zafiyetleri belirlemek için tehdit modeli kullanılır. Her tehdit hem etki hem de oluşma olasılığı göz önünde bulundurularak risk seviyesine göre değerlendirilir.

Uygulama Sırasında: Kodlama süreci boyunca riskler sürekli olarak değerlendirilir ve hafifletilir. Geliştiriciler kod yazarken gerçek zamanlı olarak zafiyetleri tespit etmek için Statik Uygulama Güvenlik Testi (SAST) araçları kullanır.

Test Sırasında: Dinamik Uygulama Güvenlik Testini (DAST) ve sızma testini içerecek şekilde kapsamlı güvenlik testleri entegre edilir ve daha önce belirlenen tüm risklerin ele alındığından emin olunur.

Dağıtım Sonrası: İşletme ortamındaki değişiklikler veya ortaya çıkan tehditler tarafından getirilen yeni riskleri belirlemek ve yanıt vermek için sürekli izleme ve periyodik güvenlik değerlendirmeleri yapılır.

Tehdit modellemesi ve risk değerlendirmesini SSDLC'ye dahil etmek, sadece proaktif olarak riskleri belirlemeye ve hafifletmeye yardımcı olmakla kalmaz, aynı zamanda güvenlik uygulamalarını organizasyonun risk toleransı ve iş hedefleriyle hizalar. Bu stratejik yaklaşım, güvenliğin sadece teknik bir ek değil, genel geliştirme ve işletme stratejisinin ayrılmaz bir parçası olduğunu gösterir.

DevSecOps'ta Güvenlik Otomasyonu

DevSecOps'ta güvenlik otomasyonu, geliştirme ve işletme hattına hem sistemli hem de ölçeklenebilir bir şekilde güvenlik süreçlerini entegre etmektir. DevSecOps'ta otomasyon, verimliliği artırır, insan hatasını azaltır ve güvenliğin tüm geliştirme ve işletme sürecinin sürekli, ayrılmaz bir parçası olduğundan emin olur.

Güvenlik Otomasyonu için Araçlar ve Teknolojiler

1) Statik Uygulama Güvenlik Testi (SAST): SAST araçları, uygulama çalışmadan önce ele alınabilecek güvenlik zafiyetlerini tespit etmek ve raporlamak için kaynaktaki kodu analiz eder.

2) Dinamik Uygulama Güvenlik Testi (DAST): DAST araçları, web uygulamalarına yönelik saldırıları taklit ederek uygulamanın çalışır durumdayken zafiyetlerini bulur.

3) Etkileşimli Uygulama Güvenlik Testi (IAST): Hem SAST hem de DAST öğelerini birleştiren IAST araçları, ajanlar veya sensörler kullanarak uygulamaları içeriden analiz eder ve güvenlik kusurlarını gerçek zamanlı olarak raporlar.

4) Yazılım Bileşen Analizi (SCA): SCA araçları, özellikle açık kaynak bileşenlerdeki bilinen zafiyetleri taramak için proje bağımlılıklarını tarar.

5) Kod Olarak Altyapı Taraması: Bu araçlar, altyapı-olarak-kod (infrastructure-as-code) şablonlarındaki yapılandırma hatalarını ve uygunluk ihlallerini belirlemeye yardımcı olur.

6) Konteyner Güvenliği: Konteyner güvenlik araçları, konteyner yaşam döngüsü boyunca uygulama konteynerlerini ve içeriklerini güvence altına almak için tasarlanmıştır.

7) Güvenlik Orkestrasyonu, Otomasyonu ve Yanıtı (SOAR): SOAR araçları, birden fazla kaynaktan güvenlik tehditleri hakkında veri toplamayı ve düşük seviyeli güvenlik olaylarına otomatik yanıtlar sağlamayı sağlar.

DevSecOps'ta Karşılaşılan Zorluklar ve Çözümler

DevOps'a güvenliği entegre etmek, yazılımın geliştirme yaşam döngüsü boyunca güvenliğini sağlamak için kritik öneme sahiptir. Ancak, bu entegrasyon, geliştirme, işletme ve güvenlik ekipleri arasındaki hedef ve iş akışlarındaki farklılıklar nedeniyle çeşitli zorluklar doğurabilir.

DevSecOps'ta Karşılaşılan Yaygın Zorluklar

1) Kültürel ve Organizasyonel Direnç: Geliştirme, işletme ve güvenlik ekipleri arasında, sırasıyla hız, istikrar ve güvenlik gibi farklı önceliklere sahip geleneksel bölümler bulunur. Bu, ekiplerin iş akışlarını bozabileceği endişesiyle değişikliklere direnç göstermelerine neden olabilir. Çözüm; güvenlik için paylaşılan bir sorumluluk bilinci oluşturmak üzere kültürel bir değişiklik teşvik etmektir. Ekipler arası anlayışı ve iş birliğini teşvik etmek için eğitim oturumları ve atölye çalışmaları düzenlenmelidir. Her disiplinin karşılaştığı zorluklara empati ve farkındalık oluşturmak için çapraz fonksiyonel ekipler kullanılabilir.

2) Hız ile Güvenlik Arasındaki Çatışma: DevOps'un çevik doğası, sık ve hızlı dağıtımları vurgular, bu da geleneksel güvenlik uygulamalarının kapsamlı ve bazen zaman alıcı doğasıyla çelişir. Çözüm; güvenlik süreçlerini mümkün olduğunca otomatize etmek, hızın üzerindeki etkisini azaltmaktır. Güvenlik kontrollerinin, geliştirme ve dağıtım süreçleriyle eş zamanlı olarak gerçekleşmesini sağlamak için güvenlik araçlarını doğrudan CI/CD hattına entegre edilmelidir.

3) Araç Entegrasyonu ve Otomasyon Zorlukları: Mevcut DevOps hatlarına güvenlik araçlarını entegre etmek ve otomatize etmek teknik olarak zorlayıcı olabilir. Araçlar uyumlu olmayabilir veya işe yarar içgörüler sağlamayabilir, bu da uyarı karmaşıklığına yol açabilir. Çözüm; mevcut geliştirme ve işletme araçlarıyla iyi entegre olan güvenlik araçlarını seçmektir. Otomasyonu destekleyen API'ler ve araçlar sunan araçlar önceliklendirilmelidir. Yanlış pozitifleri azaltmak ve uyarıların anlamlı ve işlevsel olmasını sağlamak için araçlar özelleştirilmelidir.

4) DevOps Ekiplerinde Güvenlik Bilgisinin Eksikliği: DevOps ekipleri genellikle özelleşmiş güvenlik bilgisinden yoksundur, bu da geliştirme yaşam döngüsünün güvenlik duruşunda boşluklara yol açabilir. Çözüm; düzenli güvenlik eğitimi ve farkındalık programları düzenlemektir. Güvenlikle ilgili sorunlar ve rehberlik için iletişim noktası olarak hareket edebilecek DevOps ekipleri içinde güvenlik şampiyonları görevlendirilmelidir.

5) Gelişen Güvenlik Tehditleri: Güvenlik tehditleri hızlı evrim geçirmekte olduğundan en yeni zafiyetler ve saldırı vektörlerini güncel olarak takip edebilmek zor olabilir. Çözüm; yeni tehditleri tespit edebilen sürekli izleme araçları uygulamaktır. Güvenlik tehdit istihbaratı hizmetlerine abone olunabilir ve en son güvenlik eğilimleri ve tehditleri hakkında bilgi sahibi olmak için topluluk ve endüstri forumlarına katılım sağlanabilir.

DevSecOps'un Gelecek Eğilimleri

DevSecOps, organizasyonların yazılım geliştirme ve işletme aşamalarına güvenliği entegre etmenin önemini giderek daha fazla fark etmeleriyle hızla evrim geçirmektedir. Teknolojiler ilerledikçe ve dijital manzara daha karmaşık hale geldikçe, DevSecOps'ta kullanılan metodolojiler ve araçlar da gelişmektedir.

DevSecOps'ta Yükselen Teknolojiler ve Metodolojiler

Yapay Zekâ ve Makine Öğrenimi: Yapay zekâ (AI) ve makine öğrenimi (ML), karmaşık karar verme süreçlerini otomatize ederek DevOps içindeki güvenliği artırmak için giderek daha fazla kullanılmaktadır. AI ve ML, potansiyel güvenlik tehditlerini veya zafiyetlerini bunlar istismar edilmeden önce gösterebilecek desenleri belirlemek için büyük miktarda veriyi analiz edebilir. Bu teknolojiler, güvenlik olaylarına yanıt verme sürecini de otomatize edebilir.

Öngörücü Analitik: Öngörücü analitik, geçmiş verileri kullanarak gelecekteki olaylar hakkında tahminler yapmayı içerir. DevSecOps bağlamında, öngörücü analitik, eğilim verilerine ve geçmiş olaylara dayanarak potansiyel güvenlik ihlallerini ve zafiyetleri öngörebilir. Bu proaktif yaklaşım, ekiplerin en yüksek riskli alanlara odaklanmalarını ve ihlaller meydana gelmeden önce önlem almalarını sağlar.

Güvenlik için Blokzincir: Blokzincir, yazılım dağıtımlarının ve denetimlerinin bütünlüğünü ve izlenebilirliğini artırmak için merkezi olmayan doğası ile kullanılabilir. DevOps hattının her adımının değiştirilemez ve şeffaf olmasını sağlayarak, müdahale ve iç tehdit risklerini azaltabilir.

Sunucusuz Mimari Güvenliği: Sunucusuz mimariler daha popüler hale geldikçe, bu ortamları güvence altına almak benzersiz zorluklar çıkarabilir. Sunucusuz kurulumlardaki güvenlik endişelerini ele almak için örneğin üçüncü taraf hizmetlerin ve dinamik olay odaklı mimarilerin güvenliğini sağlamak adına yeni araçlar ve uygulamalar geliştirilmektedir,

DevSecOps'un Evrimi için Tahminler

Artan Otomasyon: DevOps uygulamaları olgunlaştıkça ve güvenlikle daha sıkı bir şekilde entegre oldukça, güvenlik testlerinde ve uygunluk kontrollerinde otomasyon seviyesi artacak, bu uygulamaları daha verimli ve insan hatasına daha az açık hale getirecektir.

Bulut Güvenliği ile Daha Fazla Entegrasyon: Daha fazla organizasyon bulut ortamlarına geçtikçe, DevSecOps, bulut tabanlı kaynaklar ve uygulamaların güvenliğini artırmak için bulut yerel güvenlik araçlarını ve yeteneklerini doğrudan DevOps iş akışına entegre etmeye daha fazla odaklanacaktır.

Uygunluk Otomasyonuna Artan Odak: Artan düzenleyici gereksinimlerle, DevSecOps hattında uygunluğun otomasyonu hayati önem taşıyacaktır. Organizasyonlar, sürekli uygunluk ve gerçek zamanlı raporlama sağlamak için teknolojiden yararlanacaktır.

DevSecOps Standartlarının Geliştirilmesi: DevSecOps uygulamaları için endüstri genelinde standartlar ve çerçeveler muhtemelen ortaya çıkacak, organizasyonların etkili DevSecOps stratejileri uygulamalarına yardımcı olmak için rehberlik ve kıstaslar sağlayacaktır.

YAZILIM TEDARİK ZİNCİRİ GÜVENLİĞİ

Ahmet Anıl DÜNDAR

Günümüzde geliştirilen yazılımlarda açık kaynakların, üçüncü taraf yazılım ve kütüphanelerin kullanımı giderek artmaktadır. 2023 yılında GitHub üzerindeki tüm projelere yapılmış olan katkı (contribution) sayısının yaklaşık 4,2 milyar civarında olduğu, mevcut proje sayının 420 milyona ulaştığı ve açık kod depoları (repository) sayısının 284 milyonu geçtiği düşünülmektedir.[1] Bu durum göz önüne alındığında, yazılım sektöründe açık kaynak kodlu ve üçüncü taraf yazılımların, kütüphanelerin yaygın bir şekilde kullanıldığını söylemek yanlış olmayacaktır. Bu da yazılım geliştirme ekiplerinin, yazılım geliştirme yaşam döngüsü içerisinde, belli bir kapasitede ve bir dereceye kadar açık kaynak kullandığı anlamına gelmektedir. Ekip bir yazılım sağlayıcısı olarak çalışıyorsa, uygulamaları oluşturmak için güvenilen açık kaynak, üçüncü taraf ve ticari bileşenler kullanacaktır. Bu durum da yazılım geliştiricileri ve onların çalıştığı şirketleri/projeleri bir tedarik zincirinin parçası yapmaktadır. Ancak, tedarik zincirinin yalnızca yazılım geliştirme ekibiyle sınırlı kalmadığını, geliştirme ve teslimat faaliyetlerinin ötesine geçerek uygulamaların son kullanıcısına kadar uzandığını unutmamak gerekir. Tedarik zinciri, bir uygulamaya dokunan veya oluşturulmasında, geliştirilmesinde ve dağıtımında rol oynayan her şeyi içerir. Ayrıca, geliştirme ekipleri tarafından oluşturulan özel kod ve bileşenlerin yanı sıra bu yazılımı oluşturmak ve son kullanıcıya sunmak için kullanılan altyapıyı da içermektedir.

Yazılım tedarik zincirini anlayabilmek için ASELSAN'da geliştirilen veya faaliyet gösteren herhangi bir proje ile örneklemek netlik kazandırabilir. Bir projede çalışacak ekibin belirlenmesi, ekibin kullanılacak malzemelere ve ekipmanlara karar vermesi, bunların tedarik edilmesi için gereken işlemlerin yapılması, yine proje için gereken yazılımsal desteğin alınması ve tüm bu süreçlerin farklı ekipler tarafından yürütülüp farklı ekipler tarafından koordineli bir şekilde yapılması projeyi başarılı bir şekilde

sonlandırmaya yarayacaktır. Tüm tasarım ve üretim sürecine dahil olunduğunda risklerin ortaya çıkabileceği ve gözlemlenebileceği birçok yer ortaya çıkacaktır. Tedarik zinciri doğası gereği nihai ürünün ve onun kullanıcılarının, süreçte yer alan her bileşenden, kişiden, faaliyetten, malzemeden, karardan ve prosedürden etkilenmesidir. Bu iş akışının herhangi bir kısmındaki zayıflık risk doğurur ve bu riski azaltmanın en etkili yöntemi tedarik zincirinin tamamını tamamen anlamaktır. En basit ifadeyle bir kuruluş, tedarik zincirine ilişkin büyük resmi göremeden veya parçaları tam olarak birleştiremeden tüm riskleri göremez veya tam olarak yönetemez. Aynı durumlar yazılım tedarik zinciri için de geçerlidir.

Yazılım tedarik zincirleri, özet olarak yazılımın geliştirildiği, teslim edildiği ve kullanıldığı geniş bir ekosistem olarak değerlendirilebilir. Yazılım tedarik zinciri aslında iki ana elemana sahip gibi görünse de (geliştiriciler ve kullanıcılar veya üreticiler ve tüketiciler) alt kısımda daha da dallanan bir yapı oluşturmak mümkündür. Bu bağlamda, yazılımı oluşturan, dağıtan ve çalıştıran tüm kişiler, bileşenler, kütüphaneler, araçlar ve sistemler yazılım tedarik zincirinin bir parçasıdır. Yukarıda bahsedildiği gibi açık kaynak, üçüncü taraf yazılım ve kütüphanelerin kullanımının artmasıyla tüm geliştiriciler aslında birer kullanıcı yani tüm üreticiler birer tüketici haline gelmiş olur. Yazılım tedarik zincirinde temel olarak 4 halkadan bahsetmek mümkündür. Bunlar oluşturma/yaratma, derleme, dağıtma ve çalıştırmadır.

Yazılım tedarik zincirine yapılan saldırılar da hem geliştirici hem de kullanıcılar için birer tehlike haline gelmiştir. Asıl amacı yazılım güvenliğini ve bütünlüğünü tehlikeye atmak olan bu saldırıların genelinde güvenlik açıklıklarından yararlanarak kimlik avı saldırıları ve sonucunda kimlik bilgilerinin kötüye kullanımı, yetkisiz erişim, yetkisiz izleme, finansal hırsızlık veya sistemlerin devre dışı bırakılması olabilir. Ayrıca saldırganlar, yazılım tedarik zincirine yazılım daha oluşturulurken veya yazılım üzerine bir yama veya güncelleme geldiğinde de dahil olabilmektedir.

Açık kaynak kodların ve kütüphanelerin varlığı, yazılımda tedarik zinciri güvenliği için bir risk oluşturmaktadır. Her ne kadar, açık kaynak, özel yazılmış bir koddan daha fazla veya daha az riskli olmasa da yeterince güvenli hale getirilmemesi, projenin ve kuruluşun genel güvenliği için büyük risk oluşturur. Geliştiriciler veya altyükleniciler bilerek veya bilmeyerek projelerine açık kaynaklı kodları veya kütüphaneleri ekleyebilir. Tedarik zincirinde açık kaynak bileşenlerini, lisanslarını, güvenlik açıklarını ve bunlarla ilişkili riskleri takip etmek kuruluşun sorumluluğundadır. Ancak yazılım sektörünün büyümesi ve yaratılan uygulamaların derinliğinin artması göz önüne alındığında manuel izleme ve kontrol etme yetersiz kalacaktır.

Günümüzde yazılım geliştiren birçok kuruluş, kaynak kodlarını ve kod altyapılarını kendi havuzlarında saklamaktadır. Bu da oluşturma/yaratma evresinde kuruluşları saldırganlar için bir hedef haline getirmekte ve yalnızca kodları değil tüm CI/CD hattını (pipeline) da tehlikeye atmaktadır. Burada gerçekleştirilebilecek saldırılara örnek olarak kaynaklarda yapılabilecek izinsiz değişiklikler ve kaynak depolarının güvenliğinin ihlal edilmesi verilebilir. Bu yöntemle saldırganlar hem kaynaklara kötü amaçlı davranışlar ve güvenlik açıklıkları ekleyebilir hem de yönetim ara yüzü üzerinden bir saldırı tanımlayabilirler. Derleme aşaması saldırılarına ise değiştirilmiş derleme kaynakları, güvenlik ihlali içeren derleme platformları ve kod depoları (repository) örnek verilebilir. Dağıtım aşamasında ise saldırganlar zafiyetli içeriklerin kullanıcılar tarafından indirilmesini sağlayabilir veya kullanıcıların güvenlik yamaları içeren güncellemeleri indirmesini kasıtlı olarak engellemeye çalışabilir. Son olarak çalıştırma aşamasında ise yanlış kullanıcı yapılandırmasının yapılması, yapılandırmaların düzgün ayarlanmamasından dolayı gereğinden yüksek izinlerin verilmesi, rol bazlı

erişim denetiminin (RBAC) kullanılmaması veya düzgün konfigüre edilmemesi, yeterli güvenlik açığı taraması yapılmaması sistemi son aşamada zafiyetli hale getirebilir ve tüm kuruluşu riske atar.

Yazılım tedarik zinciri güvenliğinin sağlanması için NIST (Ulusal Standartlar ve Teknoloji Enstitüsü, National Institute of Standards and Technology) tarafından yayınlanan SSDF (Güvenli Yazılım Geliştirme Çerçeve Dokümanı, Secure Software Development Framework) ve SLSA (Tedarik Zinciri Seviyesi Yazılım Varlıkları, Supply-chain Levels for Software Artifacts) gibi rehber ve yönlendirici dokümanlar yayınlanmış olup tüm geliştirici ekiplere bu çerçevede eğitimler verilmekte ve öğrenilmiş dersler ve bilgi birikimleri paylaşılmaktadır. Fakat yine de bu rehber dokümanlar ve eğitimler üçüncü taraf ve açık kaynaklı kütüphanelerin veya yazılımların oluşturduğu veya içerdiği tehditleri tamamen ortadan kaldırma konusunda katkı sağlayacak olan bir diğer parça da SBOM (Yazılım Malzeme Listesi, Software Bill of Materials) olarak nitelendirilebilir.

SBOM, bir yazılımın içerdiği tüm bileşenleri ve bu bileşenler arasındaki ilişkileri detaylı bir şekilde listelemeyi amaçlayan bir belgedir. Adeta bir yazılımın "malzemeler listesi" olarak düşünülebilir. SBOM, yazılımın güvenliği, lisans uyumluluğu ve güncellemeleri takip etmek, yazılım tedarik zincirini yönetmek, yazılımın güvenliğini ve güvenilirliğini artırmak için büyük önem taşır. Aynı zamanda, güvenlik açıklıklarının izlenmesi ve bunlara hızlı bir şekilde müdahale edilmesi için de kullanılır.

Yazılım dünyasında, birçok farklı bileşen ve kütüphane kullanılır. SBOM, bu bileşenleri ve bunların sürüm bilgilerini, lisanslarını, bağımlılıklarını ve güvenlik durumlarını içeren kapsamlı bir envanter sunar. Bu belge, yazılımın oluşturulmasından dağıtılmasına ve güncellenmesine kadar olan süreçte kullanılabilir.

SBOM, yazılımın yaşam döngüsü boyunca değişebilir ve güncellenebilir.

- Başlangıç Aşaması: Yazılım geliştirme sürecinin erken aşamalarında, SBOM genellikle temel bileşenleri ve doğrudan bağımlılıkları içerebilir. Bu aşamada, SBOM daha genel ve kapsamlı olabilir.
- Geliştirme Süreci: Yazılımın geliştirilme sürecinde, yeni bileşenler eklenebilir veya var olan bileşenlerin sürümleri değişebilir. Bu durumda SBOM güncellenmeli ve yeni eklenen bileşenler veya değişiklikler kaydedilmelidir.
- Test ve Analiz Aşaması: Yazılımın test aşamasında, SBOM, test süreçleri ve sonuçlarına göre güncellenebilir. Özellikle güvenlik testleri yapıldığında, güvenlik açıklıkları tespit edilirse veya yeni bağımlılıklar keşfedilirse SBOM güncellenmelidir.
- Dağıtım ve Sürdürme Aşaması: Yazılım kullanıma hazır hale geldiğinde, SBOM güncellemeleri, dağıtım sırasında yapılan değişikliklere göre yapılmalıdır. Örneğin, yeni bir sürüm çıkarıldığında veya farklı bir ortama taşındığında SBOM güncellenmelidir.
- Güncelleme ve Bakım: Yazılımın yaşam döngüsü boyunca düzenli olarak güncellemeler alır. Her yeni güncelleme veya bakım çalışması, SBOM'un güncel kalmasını gerektirir. Yeni sürümler veya güvenlik düzeltmeleri SBOM'a yansıtılmalıdır.

SBOM'un yaşam döngüsü boyunca düzenli olarak güncellenmesi ve revize edilmesi, yazılımın güvenliğini, lisans uyumluluğunu ve güncel durumunu korumak için önemlidir. Bu belge, yazılım tedarik zinciri yönetiminde ve güvenlik açıklıklarının izlenmesinde kritik bir rol oynar.

SBOM'lar genellikle yazılım bileşenlerini ve ilişkilerini tanımlamak için farklı standartlara ve formatlara sahiptir.

- SPDX (Software Package Data eXchange) Linux Foundation tarafından geliştirilen ve lisans uyumluluğu odaklı olan bir SBOM formatıdır. Yazılımın bileşenlerini, sürümlerini, lisanslarını ve ilişkilerini kapsar.

- CycloneDX, OWASP (Açık Web Uygulaması Güvenlik Projesi, Open Web Application Security Project) tarafından geliştirilen bir SBOM formatıdır. Özellikle güvenlik odaklıdır ve yazılım bileşenlerinin güvenlik açıklıkları hakkında bilgi sağlar. Daha hafif bir yapıya sahiptir ve genellikle güvenlik açıklıklarının izlenmesi için tercih edilir.

- SWID (Yazılım Tanımlama, Software Identification) Tagging, NIST tarafından geliştirilen bir SBOM formatıdır. Bileşenlerin benzersiz tanımlayıcılarını içerir ve yazılımın bileşenlerini belirtmek için kullanılır.

Bu SBOM tipleri farklı odaklara sahiptir. Örneğin, SPDX lisans uyumluluğu ve bileşenler arası ilişkileri vurgularken, CycloneDX güvenlik açıklıklarını vurgular. Yazılım geliştirme sürecinde hangi odakların önemli olduğuna bağlı olarak farklı SBOM formatları tercih edilebilir. CycloneDX formatında oluşturulan SBOM'u, OWASP topluluğu tarafından geliştirilmiş açık kaynaklı bir proje olan Dependency-Track uygulamasına yükleyerek yazılımın içerdiği bileşenleri ayrıntılı olarak gözden geçirilebilir. Dependency-Track'in sunduğu detaylı analizler sayesinde, yazılımın farklı bileşenlerindeki güvenlik açıklıkları hakkında derinlemesine bilgi edinilebilir. Her bileşenin hangi güvenlik açıklıklarına sahip olduğunu, risk düzeylerini ve bu açıklıkların nasıl çözülebileceğini gösteren detaylı incelenebilir raporlar oluşturulmuş olacaktır. Sunulan bu detaylı inceleme ve analiz imkanları, yazılım güvenliğini güçlendirmek adına oldukça değerli bir kaynak olarak öne çıkmaktadır.

SBOM, yazılımın bileşenlerini ve ilişkilerini belirleyerek güvenlik açıklıklarının tespit edilmesine ve izlenmesine yardımcı olur. Dependency-Track gibi araçlar ise bu bilgileri kullanarak yazılımın güvenlik durumunu derinlemesine analiz etmeyi sağlar. Özellikle zafiyetlerin belirlenmesi ve bunlara karşı çözümlerin bulunması, yazılımın güvenliği açısından hayati öneme sahiptir. SBOM ve benzeri araçlar, yazılım geliştirme sürecinde güvenliği artırırken aynı zamanda lisans uyumluluğu ve yazılımın güncel durumunu takip etmekte de büyük yardımcılardır. Bu araçlar sayesinde yazılım geliştiricileri, yazılımlarının güvenliğini sağlama ve sürdürme konusunda daha bilinçli ve etkili adımlar atabilirler.

YAPAY ZEKÂ VE MAKİNE ÖĞRENMESİ: SİBER GÜVENLİKTEKİ FIRSATLAR VE ZORLUKLAR

Hakan MUTLU

Siber güvenlik alanı, zararlı yazılımlar, oltalama (phishing) ve sosyal mühendislik saldırıları, ağ güvenliği tehditleri, kimlik ve erişim yönetimi zorlukları, iç tehditler, veri sızıntıları ve gizlilik ihlalleri gibi çeşitli saldırılar sebebiyle zorluklarla doludur. Fidye Yazılımları, virüsler ve Truva atı gibi zararlı yazılımlar, sistemlere sızarak ciddi hasarlara yol açabilirken, oltalama saldırıları kullanıcıları aldatarak kişisel ve kurumsal bilgileri ele geçirmeyi hedefler. Ağ güvenliği, özellikle ortadaki adam (man-in-the-middle) ve servis kesintisi (Denial of Service - DoS/ Dağıtık Servis Kesintisi Saldırısı – Distributed Denial of Service - DDoS) saldırıları gibi tehditlerle sürekli bir mücadele halindedir. Kimlik hırsızlığı ve yetkisiz erişim, hassas verilere erişim konusunda ciddi güvenlik sıkıntıları yaratır. İçeriden gelen tehditler, kurum içi güvenilir kişilerin bilgiyi kötüye kullanmaları şeklinde ortaya çıkarken, veri sızıntıları ve ihlalleri ise kurumlar için itibar kaybına ve hukuki sorunlara neden olabilir. Ayrıca, bulut bilişim, IoT gibi yeni teknolojilerin benimsenmesi, güvenlik profesyonelleri için yeni zorluklar yaratmaktadır. Tüm bu tehditler, sürekli güncellenen ve gelişen güvenlik stratejilerini zorunlu kılar.

Son yıllarda yapay zeka (AI, Artificial Intelligence) teknolojisinin gelişimi büyük bir hız kazanmıştır. Gelişen donanım teknolojilerinin ve tasarlanan daha karmaşık model ve algoritmaların katkıları ile derin öğrenme, büyük veri setleri altındaki karmaşık ilişkileri çözen modellerin eğitilmesi ile, yapay zekanın doğal dil işleme, görüntü tanıma ve otomatik karar verme gibi alanlarda üstün performans sergilemesini sağlamıştır. Özellikle, dil modelleri ve otonom araçlar gibi uygulamalarda gözlemlenen başarılar, yapay zekanın günlük yaşamımızdaki rolünü arttırmıştır. Yapay zeka ve makine öğrenmesi (ML, Machine Learning), siber güvenlik alanındaki çeşitli zorluklara da yenilikçi çözümler sunarak bu alandaki savunma meka-

nizmalarını güçlendirmektedir. Zararlı yazılımların tespiti ve önlenmesinde, yapay zeka destekli sistemler, dosyaların davranışsal ve statik analizlerini yaparak sıfırıncı gün(Zero Day) açıklıklarını dahi tanıyabilir. Yapay zeka; oltalama ve sosyal mühendislik saldırılarına karşı e-posta ve iletişim trafiğini analiz ederek sahteciliği saptayabilir ve kullanıcı davranışlarındaki anormallikleri izleyerek iç tehditlere dikkat çekebilir. Ağ güvenliği alanında, yapay zeka sürekli ağ trafiğini gözlemleyerek potansiyel saldırıları önceden belirleyebilir ve otomatik müdahale mekanizmaları ile saldırıları durdurabilir. Kimlik ve erişim yönetiminde, dinamik kimlik doğrulama sistemleri ve erişim kontrolleri, kullanıcı aktiviteleri ve biyometrik veriler üzerinden sürekli öğrenme ile daha güvenilir hale gelir. Veri gizliliği korumasında ise, duyarlı verileri otomatik olarak sınıflandırabilir ve şifreleyerek veri ihlallerini önler. Bu teknolojiler, siber güvenlik stratejilerini daha etkin, hızlı ve öngörülebilir kılarak kurumların siber tehditlere karşı daha dirençli hale gelmesine yardımcı olmaktadır.

Fırsatlar

Peki nedir bu yapay zeka? Yapay zeka, insan zekasının bazı işlevlerini taklit edebilen bilgisayar sistemleri ve algoritmalarını ifade eder. Bu sistemler, öğrenme, problem çözme ve karar verme gibi insan zekasına özgü görevleri belirlenmiş mekanizmalar ile gerçekleştirebilir. Makine öğrenmesi (Machine Learning - ML) ise, yapay zekanın bir alt kümesi olarak, verilerden otomatik olarak öğrenme ve bu öğrenmeyi kullanarak kararlar verme yeteneği sağlar. ML, veri setlerinden örüntüler çıkararak ve yeni verileri bu örüntüler açısından değerlendirerek çalışır. Bu teknolojiler, geniş bir uygulama yelpazesinde, basit görevlerden karmaşık problem çözümlerine kadar çeşitli işlemleri otomatize etmekte kullanılmaktadır. Yapay zeka ve makine öğrenmesi, siber güvenlik alanında da pek çok uygulama imkanı sunmaktadır. Ağ ve kayıt anomali tespiti yöntemleri ile ağlarda veya sistemlerde beklenmeyen aktiviteleri saptayarak güvenlik ihlallerini gerçek zamanlıya yakın bir şekilde

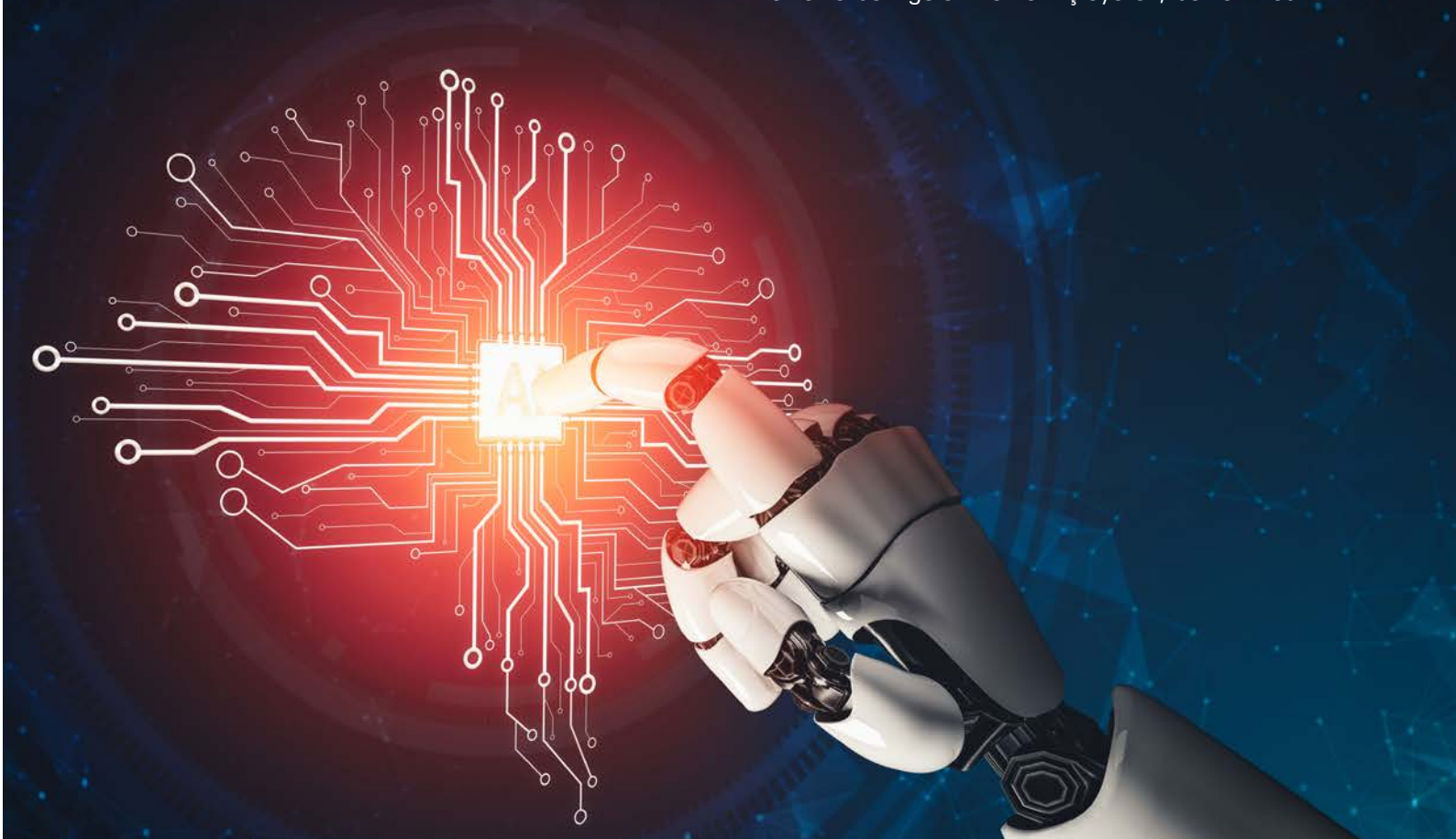
belirler. Örneğin, zaman serisi analizi, kullanıcı ve cihaz aktivitelerinin uzun süreli kayıtlarını inceler, bu verilerden elde edilen örüntüler, herhangi bir sapmanın hızla belirlenmesini sağlar. Davranışsal analitikler ise, kullanıcıların günlük işlemlerini izleyerek oluşturulan profil üzerinden herhangi bir anormalliği tespit eder. Derin öğrenme teknikleri, zararlı yazılımların yapılarını analiz edip sınıflandırmak için kullanılır, böylece bilinmeyen zararlı yazılımları bile tanıyabilirler. Doğal Dil İşleme (NLP, Natural Language Processing), oltalama saldırılarını ve zararlı komutları tespit etmek için e-posta ve diğer metin tabanlı iletişimleri analiz eder. Ayrıca; günlük incelemeleri yapan yapay zeka destekli algoritmalar, sürekli gelişen tehdit manzarasına karşı adapte olabilir, böylece yeni ve evrilmekte olan saldırı vektörlerini tanıyabilir. Bu sistemler, karmaşık ve çok katmanlı güvenlik mimarilerinin geleneksel kural tabanlı tespit yöntemlerinin yanında siber saldırılara karşı proaktif koruma sağlamada önemli rol oynayabilirler. Yapay zeka ve makine öğrenmesi algoritmaları geniş ve sürekli güncellenen zararlı yazılım veri tabanlarından öğrenerek, bilinmeyen veya değişken zararlı yazılımları otomatik olarak tanıma ve sınıflandırma yetenekleri kazanabilir. yapay zeka tabanlı sistemler, zararlı yazılımların davranışsal özelliklerini analiz eder ve bu davranışları normal kullanıcı veya sistem aktiviteleriyle karşılaştırarak şüpheli davranışları ayırt edebilir. Bu, özellikle polimorfik ve metamorfik zararlı yazılımlar gibi sürekli evrilen tehditlere karşı etkili olması beklenmektedir. Ayrıca, dil işleme yöntemlerini kullanan derin öğrenme modelleri, zararlı yazılımın kod yapısını inceleyerek, zararlı olabilecek gizli özellikleri tespit edebilir. Yapay zekanın analizleri gerçek zamanlı olarak gerçekleşmektedir, böylece tehditler hızlı bir şekilde engellenmesi konusunda bu teknolojilerden alınabilecek faydalar literatürde yer almaktadır. Ancak, mevcut yapay zeka tabanlı zararlı yazılım tespiti ve önleme sistemlerinin sınırlamaları da bulunmaktadır. Özellikle, önceden tanımlanmamış tehditlere hızla uyum sağlama kapasitesi kısıtlıdır ve bu sistemler zaman zaman yanlış pozitif(yanlış karar verilmiş tehdit kararı) veya yanlış negatif(yanlış karar verilmiş tehdit değil kararı) sonuçlar üretebilir. Bu durum, sürekli gelişen zararlı yazılım çeşitliliği karşısında etkinliklerini sınırlar ve kritik sistemlerde hatalı uyarılar veya tehlikelerin gözden kaçırılmasına neden olabilir. Bu nedenle, yapay zeka tabanlı güvenlik çözümleri genellikle ikincil sistemler olarak kullanılmaktadır ve sürekli

güncellenmeleri gerekmektedir. İlerleyen süreçte, yapay zekanın sıfırıncı gün saldırılarına karşı bile etkili bir savunma hattı olabilmesi için pek çok çalışma yürütülmektedir. Sıfırıncı gün saldırıları, bilinen bir güvenlik açığından faydalanarak, açığın henüz bilinir hale gelmeden önce gerçekleştirilir. Yapay zeka teknolojileri, siber güvenlikte sıfır gün saldırıları gibi zorlu tehditlere karşı savunma mekanizmaları oluşturmak konusunda henüz tam anlamıyla olgunlaşmamış olmasına rağmen, umut vadeden bir gelişme potansiyeline sahiptir.

Yapay zeka, öğrenme sürecinde büyük veri setlerini analiz ederek birtakım öznitelikler çıkarma ve bu özniteliklere dayanarak tanıma yetenekleri geliştirme konusunda son derece yeteneklidir. Kimlik doğrulama ve erişim kontrolü alanında, biyometrik verilerin ve davranışsal biyometriklerin kullanımıyla önemli katkılar sağlar. Biyometrik veriler, parmak izi, yüz tanıma, iris tanıma vb. gibi fiziksel özellikleri kapsarken, davranışsal biyometrikler, klavye kullanımı, fare hareketleri ve yürüme şekli vb. gibi bireylerin davranışsal özelliklerini analiz eder. Yapay zeka teknolojileri, bu verileri gerçek zamanlı olarak işleyerek, kullanıcının kimliğini doğrulamada ve yetkisiz erişim girişimlerini belirlemede yüksek doğruluk sağlar. Ayrıca, sürekli kullanıcı ve varlık davranış izleme sistemleri, yapay zeka destekli analizlerle, normal dışı davranışları saptayarak güvenlik ihlallerini önceden algılamakta ve dinamik erişim kontrolü sağlamakta kullanılabilir. Bu sistemler, kullanıcıların durumlarına veya ağdaki güvenlik seviyesine bağlı olarak erişim haklarını gerçek zamanlı olarak dinamik bir şekilde ayarlayabilir. Bu yetenekler sayesinde, yapay zeka, siber güvenlikte kimlik doğrulama ve erişim kontrolü süreçlerini daha akıllı ve esnek hale getirerek, kurumları ve bireyleri yetkisiz erişim ve veri ihlallerine karşı koruma potansiyeline sahiptir.

Zorluklar

Ağ güvenliği, kurumların ve bireylerin hassas bilgilerini yetkisiz erişim ve siber saldırılardan koruyarak bilgi güvenliğini ve iş sürekliliğini sağlamak için önemli bir alandır. Yapay zeka teknolojileri, ağ trafiğini sürekli izleyerek ve analiz ederek anormal aktiviteleri veya potansiyel tehditleri gerçek zamanlı olarak tespit edebilir. Bu, özellikle geniş ağ yapısında, IoT (Internet of Things) cihazları gibi çeşitli ve çok sayıda bağlı cihazın yönetilmesi gerektiğinde kritik öneme sahiptir. Yapay zeka, bu cihazlardan gelen verileri işleyerek, beklenmedik



trafik örüntüleri veya şüpheli ağ etkileşimlerini algılayabilir ve güvenlik ihlallerini önleyebilir. Ancak, yapay zekanın ağ güvenliği kullanımı bazı eksiklikler ve zorluklar içerir. Yapay zeka sistemleri bazen yanlış pozitif veya yanlış negatif sonuçlar üretebilir, bu da karmaşık ağ yapılarında ve IoT cihazları gibi çeşitlenen teknolojilerde ciddi sorunlara yol açabilir. Yanlış pozitifler, meşru trafiği tehlikeli olarak işaretleyerek gereksiz uyarılar yaratırken, yanlış negatifler gerçek tehditleri gözden kaçırabilir. IoT cihazlarının sınırlı işlem kapasitesi ve enerji verimliliği, gelişmiş yapay zeka güvenlik çözümlerinin entegrasyonunu zorlaştırabilir ve performans üzerinde olumsuz bir etki yaratabilir. Bu eksiklikler, yapay zekanın ağ güvenliği alanında etkinliğini artırmak için ele alınması ve çözülmesi gereken önemli konulardır.

Günümüzde, dijital dönüşümün hızla ilerlemesi ve veri hacminin artması ile birlikte, veri gizliliği ve koruma daha önce hiç olmadığı kadar önem kazanmıştır. Yapay zeka veri gizliliği ve koruma alanında, kişisel verilerin korunması ve veri sızıntılarını önleme konularında önemli faydalar sunabilir. Yapay zeka tabanlı sistemler, büyük veri kümelerini analiz ederek duyarlı verileri otomatik olarak tanımlayabilir ve bu verileri şifrelemek için politikalar uygulayabilir. Bu süreç, özellikle geniş ölçekli kurumlarda veri sızıntılarının önlenmesi ve veri ihlalleriyle ilgili risklerin azaltılmasında kritik bir rol oynar. Yapay zeka, ayrıca davranışsal analizler yaparak, anormal veri erişimlerini saptayabilir ve potansiyel iç tehditleri veya ihlalleri erken aşamada tespit edebilir. Ancak, yapay zekanın veri gizliliği ve koruma kullanımı bazı eksikliklerle de karşı karşıyadır. Yapay zeka sistemleri, yanlış sınıflandırmalar yapabilir, bu da yanlış veri koruma uygulamalarına yol açabilir. Ayrıca, yapay zeka modellerinin eğitimi için kullanılan verilerin kalitesi ve güncelliği, sistemin genel etkinliğini doğrudan etkiler. Gizlilik açısından, yapay zeka tarafından işlenen verilerin, veri koruma standartları ve yasal düzenlemelere uygun olarak yönetilmesi gerekir, bu da ek güvenlik önlemleri ve düzenli denetimler gerektirir. Bu nedenle, yapay zekanın veri gizliliği ve koruma alanında sunduğu çözümler, bu teknolojinin etkinliğini artırmak ve potansiyel riskleri azaltmak için sürekli olarak değerlendirilmeli ve iyileştirilmelidir.

Üretken Yapay Zeka (Generative AI), yapay zeka alanında son dönemde öne çıkan ve öğrenilen verileri temel alarak yeni ve özgün içerikler oluşturabilen bir teknolojidir. Üretken yapay zeka, öğrenilen veri kümelerine dayanarak yeni içerikler üretebilir ve siber güvenlik alanında yenilikçi uygulamalara imkan tanıyabilir. Özellikle, üretken yapay zekayı kullanarak siber saldırı senaryoları geliştirmek, güvenlik sistemlerinin zorlu testlerden geçirilmesini ve böylece savunmaların güçlendirilmesini sağlayabilir. Bu yöntem ile kırmızı takım (red team) egzersizleri ile mavi takım (blue team) savunmalarının gerçekçi ve karmaşık siber tehditlere karşı nasıl tepki vereceğini simüle edilebilir. Üretken yapay zekayı , gerçek dünya saldırılarına benzer koşullar yaratarak, potansiyel güvenlik açıklarını ortaya çıkarmada ve savunma stratejilerinin proaktif bir şekilde geliştirilmesinde kritik bir rol oynayabilir. Ancak, uygulanabilirliği konusunda bazı zorluklar bulunmaktadır. Örneğin, yüksek kaliteli ve temsil edici veri setlerine olan ihtiyaç, üretken yapay zeka modellerinin eğitimi ve optimizasyonunu karmaşıklaştırabilir. Ayrıca, yanlış pozitiflerin veya yanlış negatiflerin yüksek oranı, gerçek dünya uygulamalarında bu teknolojinin güvenilirliğini sınırlayabilir. Bu nedenlerle, üretken yapay zekanın potansiyelini tam olarak gerçekleştirmek için sürekli teknik gelişmeler ve metodolojik iyileştirmeler gerekmektedir. Buna rağmen, bu teknoloji, özgün saldırı senaryoları oluşturarak kurumların siber saldırılara karşı daha hazırlıklı olmalarını sağlar ve sürekli değişen tehdit ortamında rekabet avantajı yaratabilir.

Yapay Zeka Sistemlerine Karşı Yapılan Saldırılar

Peki yapay zeka sistemleri siber saldırılara ne kadar dayanıklıdır? En yaygın tehdit türlerinden biri olan düşmancıl (adversarial) saldırılar, yapay zeka modellerini yanıltmak amacıyla manipüle edilmiş verilerle gerçekleştirilir. Bu tür saldırılar, özellikle görüntü ve ses tanıma sistemlerinde etkili olup, sistemleri yanlış sınıflandırmaya veya hatalı kararlar almaya zorlar. Örneğin, bir görüntü tanıma sistemi, değiştirilmiş bir görüntüyle yanlış etiketleme yapması için kandırılabilir. Bir diğer saldırı türü olan veri zehirleme, eğitim aşamasında kötü niyetli verilerin sisteme sızdırılmasıyla yapay zeka modelinin baştan yanlış öğrenmesine neden olur. Model çalma saldırıları ise, saldırganların eğitimli

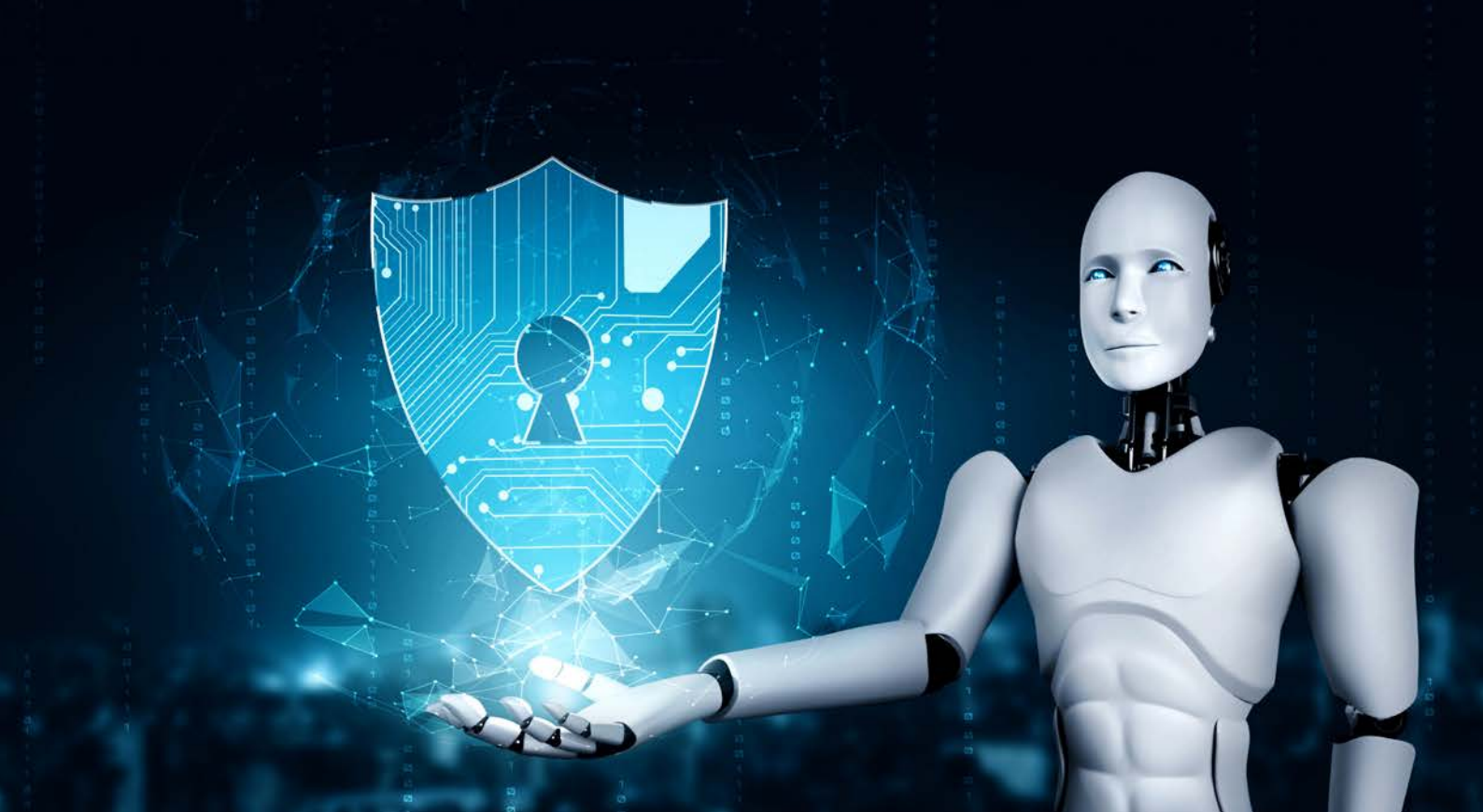
yapay zeka modellerine benzer modeller oluşturarak, onların iç çalışmalarını veya veri yapılarını kopyalayıp yanlış karar verecek şekilde bozulmasıdır.

Yapay zeka sistemlerini savunmak ve bu tür saldırılara karşı dayanıklılıklarını artırmak için alınabilecek çeşitli önlemler bulunmaktadır. İlk olarak, düşmancıl saldırılara karşı savunma için, yapay zeka modellerini düşmancıl örneklerle eğitmek ve test etmek önemlidir. Bu yöntem, modellerin manipüle edilmiş verilere karşı daha dirençli hale gelmesini sağlar. Örneğin, bir görüntü tanıma sistemi, manipüle edilmiş görüntülerle eğitilerek, bu tür saldırılara karşı daha güçlü bir tahmin yeteneği kazanabilir. Veri zehirleme saldırılarına karşı korunmak için, eğitim verilerinin doğruluğunu ve güvenilirliğini doğrulamak gerekir. Veri temizleme işlemleri, anomali tespit teknikleri ve güvenilir veri kaynaklarından yararlanmak, kötü niyetli verilerin sisteme sızmasını önleyebilir. Ayrıca, veri setlerini düzenli olarak gözden geçirmek ve güncellemek, eğitilmiş modelin doğruluğunu ve düşmancıl etkilere karşı güvenliğini artırır. Model çalma saldırılarına karşı, API erişim kontrol mekanizmalarını güçlendirmek, modelinizi kullanan veya erişen kullanıcıların yetkilendirilmesini sağlamak önemlidir. Modelin çıktılarını sınırlayarak ve gereksiz bilgi ifşasını engelleyerek saldırganların model hakkında detaylı bilgi edinmeleri zorlaştırılabilir. Ayrıca, model şifreleme ve kodlama teknikleri, modelin iç yapısını korumak için kullanılabilir. Son olarak, yapay zeka sistemlerinin güvenliğini sürekli olarak izlemek ve değerlendirmek, olası güvenlik açıklarını erken tespit etmekte ve hızlı müdahalede bulunmada hayati rol oynar. Siber güvenlik ekipleri, yapay zeka güvenliğine yönelik en son araştırmaları ve güvenlik uygulamalarını takip ederek, sistemlerini güncel tehditlere karşı korumalıdır. Bu önlemler, yapay zeka sistemlerinin siber saldırılara karşı daha dayanıklı hale gelmesine yardımcı olacak ve güvenliğini sürekli olarak sağlamlaştıracaktır.

Doğal dil işleme araçları, kişisel verilerin işlenmesinde yaygın olarak kullanılmaktadır ve bu da onları potansiyel siber saldırılara açık hale getirir. Özellikle, doğal dil işleme sistemleri kişisel verileri analiz ederken, bu verilerin manipüle edilmiş girdilerle yanıltılması veya kötü niyetli aktörler tarafından ele geçirilmesi ciddi gizlilik ihlallerine yol açabilir. Örneğin; bir saldırgan, doğal dil işleme

sistemine zararlı girdiler sağlayarak sistemi, hassas bilgileri ifşa edecek şekilde manipüle edebilir. Bu tür saldırılar, kullanıcıların kişisel bilgilerinin yanlış sınıflandırılmasına veya yanıltıcı sonuçlar üreterek veri sızıntılarına neden olabilir. Ayrıca, doğal dil işleme uygulamaları, kullanıcı verilerini işlerken, veri zehirleme gibi teknikler kullanarak eğitim verilerine müdahale edilmesi sonucu güvenlik açıklarına maruz kalabilir. Bu durum, yanıltıcı çıktılar üreten ve sonuçta kullanıcıların kişisel bilgilerinin ifşa olmasına yol açan bozulmuş doğal dil işleme modellerine neden olabilir. Bu nedenle, doğal dil işleme sistemlerini güvenli bir şekilde uygulamak ve korumak için veri doğrulama, güvenli veri depolama, erişim kontrolleri ve sürekli güvenlik izlemesi gibi önlemler alınması kritik önem taşımaktadır. Bu önlemler, doğal dil işleme araçlarının güvenilirliğini artırır ve kullanıcı verilerinin korunmasını sağlar.

Yapay zeka teknolojileri, siber güvenlik alanında yenilikler yaratmaya devam ederken gelecekteki trendleri ve zorlukları da şekillendirmektedir. Bu teknolojiler, tehdit algılama, otomasyon ve tepki süreçlerini sürekli iyileştirerek daha etkin bir savunma mekanizması oluşturmayı amaçlamaktadır. Ancak, düşmancıl yapay zeka gibi tehditler, yapay zeka sistemlerini manipüle edebilecek saldırı teknikleri ile karşı karşıya kalındığını gösteriyor. Bu tür saldırılar, yapay zekanın güvenilirliğini ve etkinliğini sınırlayarak, sistemlerin yanıltıcı kararlar almasına neden olabilir. Ayrıca, yapay zeka ve makine öğrenmesi modellerinin eğitimi için gereken yüksek kaliteli ve geniş kapsamlı veri setlerinin yönetilmesi sürekli bir zorluk oluştururken, veri gizliliği, kişisel verilerin korunması ve şeffaflık gibi etik konular da büyük önem taşımaktadır. Bu teknolojilerin büyük veri setleri üzerinde çalışması, özellikle kişisel verilerin yanlış kullanılması veya ifşa edilmesi riskini barındırır. Bu nedenle yapay zeka ve makine öğrenmesi modellerinin eğitimi sırasında kullanılan verilerin gizliliğine ve korunmasına yönelik güçlü protokollerin ve şifreleme tekniklerinin uygulanması, etik standartlara ve yasal düzenlemelere uygunluğun sağlanması kritik önem taşır. Bu zorlukların üstesinden gelmek için sürekli araştırma, gelişmiş algoritmalar ve yeni güvenlik protokolleri geliştirilmesi gerekmekte, böylece yapay zeka ve makine öğrenmesinin siber güvenlikteki potansiyeli daha güvenli ve etkili bir şekilde kullanılabilecektir. Bu çabalar, yapay zeka destekli siber güvenlik çözümlerinin daha daya-



nıklı ve adapte olabilir hale gelmesini sağlayarak, gelecekteki siber tehdit ortamında kurumları korumada önemli bir rol oynamaya devam edecektir.

Toparlayacak olursak yapay zeka ve makine öğrenmesi teknolojilerinin gelişimi, siber güvenlik dahil birçok alanda iş süreçlerini dönüştürmekte ve otomatize etmekte büyük rol oynamaktadır. Bu teknolojiler, tehdit tespiti ve yanıt verme gibi görevleri daha hızlı ve etkin bir şekilde yerine getirerek, güvenlik operasyonlarını güçlendirmekte ve çalışanların yükünü hafifletmektedir. Ancak, yapay zekanın işleri tamamen elimizden alacağı yönündeki endişeler genellikle abartılıdır. Gerçekte, yapay zeka, insanların yerini almak yerine onları desteklemeyi amaçlamaktadır. Yapay zeka, rutin ve tekrar eden görevleri üstlenerek insan çalışanlara daha stratejik ve analitik işlere odaklanma fırsatı sunar. Bu sayede, çalışanlar daha yaratıcı ve yenilikçi roller üstlenerek kariyerlerini ilerletebilir. Bu bakış açısıyla, yapay zekanın "işleri elimizden alma" potansiyeli değil, "işleri dönüştürme" kapasitesine odaklanmak daha doğru olacaktır. Yani, yapay zeka ve makine öğrenmesi teknolojileri, siber güvenlikte ve diğer alanlarda iş süreçlerini ve çalışma yöntemlerini yeniden şekillendirerek insanların daha değerli işler yapmalarını sağlayacak araçlar olarak değerlendirilmelidir.

Hayatı Yenileyen Teknoloji

Modernizasyon Yetenek Çalışmalarımız

Savunma araçlarının hareket kabiliyetlerinin üstün teknoloji inovasyonları ile geliştirilerek modernizasyon çözümlerinin hazırlanmasını sağlıyoruz.

www.aselsan.com

aselsan

SIFIR GÜVEN YAKLAŞIMI İLE AĞ GÜVENLİĞİNİ ANLAMAK

İrem Gül SUBAŞI

Günümüzde siber güvenlik, sürekli evrilen bir alan. Geleneksel ağ güvenliği yöntemleri, modern tehditlere karşı yetersiz kalabiliyor. Bu durum, bizi yeni bir soruyla karşı karşıya bırakıyor. Bu güncel siber tehditler karşısında dijital varlıklarımızın güvenliğini nasıl sağlayabiliriz? İşte bu noktada Sıfır Güven Yaklaşımı devreye giriyor. Sıfır Güven ismindeki bu yaklaşımla geleneksel ağ mimarilerinin "Saldırganları dışarıda tut" ilkesi artık yerini "Saldırganlar zaten içeride, buna göre önlemlerini al" şeklinde bir ilkeye bırakmıştır.

Sıfır güven yaklaşımı, geleneksel ağlarda olduğu gibi, tehdit aktörlerini dışarıda tutmak yerine bu aktörlerin zaten iç ağda bulunabildiğini ve önlemlerin bu tehdide göre alınması gerektiğini söyleyen yaklaşımdır. Geleneksel ağ mimarisi bir kale konseptine benzetilir ve zararlı unsurlar kalenin yani ağın dışında tutulmaya çalışılır. Bunun aksine Sıfır Güven yaklaşımına göre, kullanılan ağ her zaman güvensizdir ve saldırılara açıktır. Sıfır Güven, "Asla Güvenme, Her Zaman Doğrula" ilkesine dayanır. Bu felsefe, ağ içi veya dışı, hiçbir kullanıcıya veya cihaza otomatik olarak güvenilmemesi gerektiğini savunur. Erişim talepleri her defasında yeniden doğrulanmalıdır. Bu yaklaşım, modern siber güvenlik tehditlerine karşı daha etkili bir savunma sunar.

Geleneksel Ağ Güvenliği ve Dezavantajları: Geleneksel ağ güvenliği, büyük ölçüde güvenlik duvarlarına ve içeriden dışarıya güvenlik anlayışına dayanır. Bu sistemler, bir kez içeri girebilen kullanıcılara genellikle geniş erişim imkanı tanır. Ancak bu yaklaşımın bazı dezavantajları vardır:

1. Güvenlik Duvarına Duyulan Varsayılan Güven: Geleneksel yaklaşımlar, güvenlik duvarlarına aşırı bağımlıdır. Bu duvarlar, dış tehditlere karşı bir savunma hattı oluştururken, iç ağdaki tehditleri göz ardı edebilir. Bu, iç tehditlere karşı savunmasızlık anlamına gelmektedir.

2. İçeriden Dışarıya Güvenlik: Geleneksel güvenlik, ağın içindeki kullanıcılara geniş bir hareket alanı tanır. Bu durum, iç tehditlere karşı ciddi bir savunmasızlık yaratır. İçeriden yapılan saldırılar veya ihlaller, geleneksel ağ güvenliğine dayanan sistemler tarafından kolayca tespit edilemez.

3. Statik Güvenlik Protokolleri: Statik kurallar ve politikalar, dinamik tehditlere karşı yetersiz kalabilir. Geleneksel ağ güvenliği, genellikle statik bir tehdit modeline dayanır ve bu, sürekli değişen siber tehdit ortamında etkisiz kalabilir.

Sıfır Güven Yaklaşımının Avantajları:

1. Sürekli Doğrulama: Sıfır Güven yaklaşımı, her erişim talebini sürekli olarak doğrular. Bu doğrulama, güvenlik ihlallerini önlemede geleneksel ağ güvenliğine göre daha etkilidir çünkü sıfır güven yaklaşımında her kullanıcı ve cihaz, her zaman şüphe altındadır.

2. En Az Ayrıcalık İlkesi: En az ayrıcalık ilkesi (Principle of Least Privilege), kullanıcılara yalnızca ihtiyaç duydukları minimum seviyede sisteme erişim hakkı verilmesini tanımlar . Bu ilke ile iç tehditlere karşı daha güçlü bir koruma sağlanır. Kullanıcılar yalnızca görevleri için gerekli olan kaynaklara erişebilir, bu da potansiyel zararın kapsamını sınırlar.

3. Dinamik Güvenlik Politikaları: Sıfır Güven, kullanıcı davranışlarına ve değişen tehditlere göre uyarlanabilir güvenlik politikaları sunar. Bu esneklik, ağın sürekli olarak güncel ve güvenli kalmasını sağlar.

Sıfır güven yaklaşımını benimseyen bir ağ aşağıdaki 5 temel iddiayı savunur:

- Ağın her zaman güvensiz olduğu varsayılır.
- Ağda her zaman iç ve dış tehditler bulunmaktadır.
- Bir ağda güven ilişkisi kurulması için yerellik (aynı ağda bulunuyor olma) yeterli değildir.
- Her cihaz, kullanıcı ve ağ akışının kimlik doğrulaması ve yetkilendirmesi yapılmalıdır.
- Ağ politikaları statik değil dinamik olarak belirlenmeli ve bu politikalar birden fazla kaynaktan alınan verilere dayanarak oluşturulmalıdır.

Temelde ağda iki segment bulunmalıdır. Bunlardan birisi güvenin ilişkilerinin kurulduğu kontrol düzlemi (control plane) ve diğeri güven ilişkilerinin uygulandığı veri düzlemi (data plane)'dir. Veri ve kontrol düzlemi arasındaki etkileşimlerin otomatize ve göreceli olarak hızlı olmadığı bir ağ, sıfır güven yaklaşımını uygulamıyordur. Modern konfigürasyon yönetim sistemleri hem cihaz envanteri tutup hem de veri düzlemi yapılandırmasını otomatize ettiği için sıfır güven yaklaşımının uygulamaya başlanması için mantıklı bir ilk adım olacaktır.

Sıfır güven modeline göre ağ iletişimi önce kontrol düzleminden başlamalıdır. Kullanıcılarla birlikte, kullanıcıların kullandıkları cihazlara da kimlik doğrulaması ve yetkilendirmesi yapılmalıdır. Ancak bu kontrollerden sonra sadece içeriye giriş için belirli bir seviyede erişim yetkisi verilmeli ve bu erişim yetkisi sıfır güven yaklaşımı ile yönetilen ağın güven seviyesine göre (ilerideki bölümlerde anlatılacak) verilmelidir. Kontrol düzleminin kimliği doğrulanan kullanıcıya verdiği yetki, yalnızca kimlik doğrulaması sağlayan cihaz ile sınırlı olmalıdır.

Sıfır güven yaklaşımı, kontrol düzlemi ile veri düzlemi arasına keskin bir çizgi çekmiştir. Böyle bir ağda veri düzlemi ağdaki trafiği işleyen uygulamalar, güvenlik duvarları, yönlendiriciler ve vekil sunucular oluşur. Veri düzlemi bütün sisteme erişim sağlayabildiği için, veri düzlemindeki servislerin kontrol düzleminde yetki sağlamak amacıyla kullanılmasını önlemek büyük önem arz etmektedir.

Veri düzlemi saldırganlar açısından sisteme giriş noktası sayıldığı için, veri düzlemi ile kontrol düzlemi arasındaki arayüzün saldırıya kapalı olması önemlidir. Bu iki düzlem arası trafik şifreli olmalı ve sistemin güvenilir olduğundan emin olmak için halka açık olmayan ortak anahtar altyapısı (non-public PKI) ile kimlik doğrulaması sağlanmalıdır.

Bu güvenlik gereksinimlerinin bulunmasının bir diğer önemli sebebi de kontrol düzleminin bütün ağ için bir güven sağlayıcı olarak görülmesidir. Bütün ağ üzerindeki etkisinin ve erişiminin yüksek olması sebebiyle kontrol düzleminin güvenilirliği oldukça önemlidir.

5 Adımda Sıfır Güven

1. Saldırı Yüzeyini Belirle

Saldırı yüzeyi, yetkisiz bir kullanıcının, saldırganın, sisteme erişim sağlayabileceği noktaları ifade eder. Sıfır güven yaklaşımının uygulanabilmesi için saldırı yüzeyi detaylıca belirlenmelidir.

2. Mikro-Segmentasyon Sağla

Mikro-segmentasyon: Veri merkezinin birbirinden bağımsız küçük mantıksal segmentler olarak bölünmesi ile güvenlik kontrollerini tanımlayan ve her bir segmente servis sağlayan bir ağ güvenliği tekniğidir. Mikro-segmentasyon, IT'ye güvenlik politikalarını birçok fiziksel firewall kurmak yerine ağ sanallaştırma teknolojisi kullanarak uygulama kolaylığı sağlar. Güvenlik kontrollerinin küçük segmentlere ayrı ayrı uygulanıyor olması sebebiyle mikro-segmentasyon, saldırıya karşı direnci arttırır.

3. Çok Faktörlü Kimlik Doğrulama Uygula

Çok faktörlü kimlik doğrulaması kullanıcıdan iki veya daha fazla kimlik doğrulaması sağlamasını bekler. Örneğin kullanıcının oturum açma işlemi sırasında kullanıcı adı ve cep telefonuna gelen kodu girmesi istenebilir.

- Bilinen şey (something you know): Yalnızca kullanıcının bildiği/ bilmesi gereken bilgilerden oluşur. Kullanıcı adı, parola, PIN gibi.

- Sahip olunan şey (something you have): Yalnızca kullanıcının sahip olduğu nesnelerden oluşur. Banka kartı, cep telefonu, güvenlik anahtarı gibi.

- Olunan şey (something you are): Kullanıcının biyometrik özelliklerini kapsayan parametrelerdir. Parmak izi, retina taraması, yüz taraması, ses tanıma gibi.

Çok faktörlü kimlik doğrulama ile oturum açma işlemlerinde ekstra bir güvenlik katmanı sağlanmış olur.

4. En Az Ayrıcalık İlkesi Uygula

En az ayrıcalık ilkesiile veriye ulaşımı kısıtlayarak veri güvenliğinin artırılması hedeflenmektedir. Bir belgenin okuma yetkisinin yalnızca o belgeye erişim sağlaması gerektiği düşünülen kullanıcılara verilmesi, belgeyi değiştirme yetkisinin ise sadece belgeyi oluşturan kullanıcıya verilmesi en az ayrıcalık ilkesine örnek olarak gösterilebilir.

En az ayrıcalık ilkesinde kullanıcıları yetki seviyelerine göre gruplandırmak (yönetici hesabı, kullanıcı hesabı, servis hesabı gibi) gerekmektedir.

5. Tüm Uç Nokta Cihazlarını Doğrula

Doğrulanmamış hiçbir cihaza güvenme. Sıfır güven, "kimseye güvenmeme" ilkesine dayanır. Kurumların kendi sınırları içinde veya dışında hiçbir cihaza veya kullanıcıya otomatik olarak güvenmemesi ve erişim izni vermeden önce her şeyi sıkı bir şekilde doğrulaması gerektiği inancına dayanan bir güvenlik konseptidir. Sıfır güven yaklaşımı cihaz doğrulamaya ve kimlik merkezli kontrolleri genişletmeye yardımcı olur. Cihaz doğrulaması ile verilere erişim sağlamaya çalışan cihazların güvenlik kriterlerini karşılayıp karşılamadığının kararı verilebilir.

Sıfır Güven Mimarisi

Sıfır Güven mimarisinin temel bileşenleri olan Politika Motoru, Politika Yöneticisi, Politika Uygulama Noktası ve Politika Karar Noktası organizasyonlara güvenlik politikalarını oluşturma, yönetme ve uygulama konusunda kapsamlı bir çözüm sunar. Bu bileşenlerin bir araya gelerek çalışması, ağ güvenliğini dinamik, esnek ve etkili kılar.

1. Politika Motoru

Politika Motoru , Sıfır Güven mimarisinin beynidir. Bu bileşen, ağ üzerindeki tüm veri akışlarını ve erişim taleplerini değerlendirir. Politika Motoru, kuruluşun güvenlik politikalarını, kullanıcıların kimlik bilgilerini, cihaz durumlarını ve diğer bağlam bilgilerini kullanarak, hangi kaynaklara erişim izin verilip verilmeyeceğinin kararını verir. Bu süreçte, sürekli olarak risk değerlendirmesi yapar ve erişim politikalarını dinamik bir şekilde uygular.

Kaynağa erişim izni verip vermeme kararından sorumlu bileşendir. Erişim izni vermek, reddetmek ve iptal etmek gibi kararları verir.

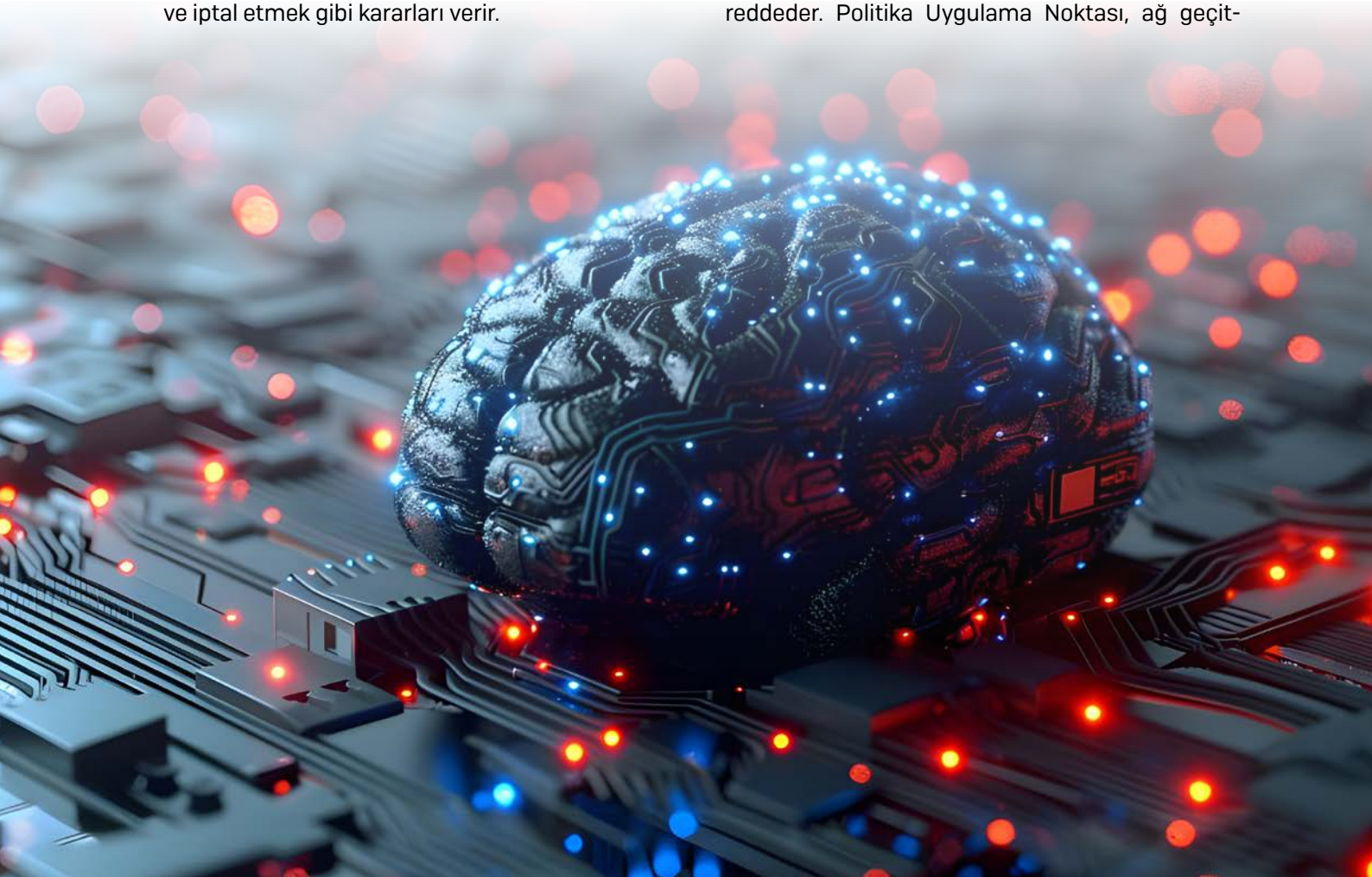
2. Politika Yöneticisi

Politika Yöneticisi, güvenlik politikalarının oluşturulduğu, yönetildiği ve güncellendiği yerdir. Bu bileşen, kuruluşun güvenlik gereksinimlerine, düzenleyici uyumluluk standartlarına ve iş ihtiyaçlarına göre politikaları şekillendirir. Politika Yöneticisi, bu politikaları Politika Motoru'na ileterek, bu politikaların ağ genelinde tutarlı ve etkin bir şekilde uygulanmasını sağlar.

Politika Yöneticisi, ilgili Politika Uygulama Noktası'na verilen komut ile özne(erişim izni isteyen) ve kaynak(erişmek istenilen) arası iletişim yolunun kurulmasından ve kapatılmasından sorumludur.

3. Politika Uygulama Noktası

Politika Uygulama Noktası, Sıfır Güven mimarisindeki uygulama kolu olarak işlev görür. Bu bileşen, kullanıcıların, cihazların veya hizmetlerin ağ kaynaklarına erişim taleplerini alır ve bu talepleri Politika Motoru'na iletir. Ardından, Politika Motoru'ndan gelen kararlara göre erişimi onaylar veya reddeder. Politika Uygulama Noktası, ağ geçit-



leri, sanal özel ağlar (VPN'ler), güvenlik duvarları ve hatta uç nokta cihazları gibi çeşitli yerlerde konumlandırılabilir. Bu noktalar, ağın güvenliğini sağlamak için kritik öneme sahiptir, çünkü erişim kontrolünün gerçekleştiği yerlerdir.

Politika Uygulama Noktası, özne ile kaynak arasındaki bağlantıyı etkinleştirmek, izlemek ve sonlandırmak işlemlerinden sorumludur. İstekleri iletmek için doğrudan Politika Yönetcisi ile iletişim kurar.

4. Politika Karar Noktası

Politika Karar Noktası, erişim taleplerini değerlendirir ve bu taleplere ilişkin kararlar alır. Politika Karar Noktası, Politika Motoru'nun' bir parçası olarak görülebilir. Bu bileşen, kullanıcı kimlik bilgileri, cihaz durumu, uygulama sağlığı ve diğer bağlam bilgilerini analiz eder. Daha sonra, bu bilgileri mevcut güvenlik politikaları ve kuralları ile karşılaştırarak, her bir erişim talebi için izin verilip verilmeyeceğine karar verir. Politika Karar Noktası'nın kararları, Politika Uygulama Noktası tarafından uygulanır.

Sıfır Güven Mimarisinin İşleyişi

Yukarıda tanımları yapılmış olan bu dört bileşen, Sıfır Güven mimarisinin temel yapı taşlarını oluşturur ve birlikte çalışarak güvenli bir ağ ortamı sağlarlar. İşleyiş süreci şu şekildedir:

1. Erişim Talebi: Bir kullanıcı veya cihaz, ağ kaynaklarına erişim talebinde bulunur.

2. Politika Uygulama Noktası: Bu talep, ilk olarak Politika Uygulama Noktası'na ulaşır. Politika Uygulama Noktası, talebi Politika Karar Noktası'na iletmeden önce gerekli kimlik doğrulama ve bağlam bilgilerini toplar.

3. Politika Karar Noktası: Politika Karar Noktası talebi değerlendirir. Bu süreçte, kullanıcının kimliği, cihazın güvenlik durumu, uygulamanın durumu ve diğer bağlam bilgileri göz önünde bulundurulur. Politika Karar Noktası , bu bilgileri mevcut güvenlik politikaları ve kuralları ile karşılaştırır.

4. Karar ve Uygulama: Politika Karar Noktası , erişim talebine izin verilip verilmeyeceğine karar verir ve bu kararı Politika Uygulama Noktası'na iletir. Politika Uygulama Noktası, bu karara göre erişimi onaylar veya reddeder.

5. Politika Motoru ve Politika Yöneticisi: Bütün bu adımlar boyunca, Politika Motoru ve Politika Yöneticisi, güvenlik politikalarının güncel ve uygun olduğundan emin olmak için sürekli olarak çalışır. Politika Motoru, risk değerlendirmesi yaparak ve politikaları dinamik bir şekilde uygulayarak güvenlik duruşunu optimize eder. Politika Yöneticisi ise politikaları sürekli güncel tutar ve organizasyonun ihtiyaçlarına göre ayarlama yapar.

Sıfır Güven yaklaşımının organizasyonlar için siber güvenlik alanında sunduğu avantajları ve güvenlik mimarisinin temel bileşenlerini değerlendirdik. Bu yaklaşım, geleneksel ağ güvenliği zafiyetlerini aşarak sürekli doğrulama, en az ayrıcalık ilkesi, çok faktörlü kimlik doğrulama gibi önlemleri içermesiyle öne çıkıyor. Ayrıca, Sıfır Güven yaklaşımının uygulanması organizasyonlara her an saldırıya açık olduklarını kabul etme ve sürekli olarak güvenlik önlemlerini güncelleme gerekliliğini getirmektedir. Bu, siber tehdit ortamındaki sürekli değişime ayak uydurabilme kabiliyetini artırarak güvenlik duvarlarını aşan bir savunma stratejisi sunar.Bu bağlamda, Sıfır Güven yaklaşımı, organizasyonlara siber güvenlik anlamında gelişen tehditlere karşı daha dirençli olmalarını sağlayan önemli bir çözüm sunar. Güvenlik politikalarının sürekli olarak güncellenmesi ve her erişim talebinin dikkatli bir şekilde değerlendirilmesi, modern siber tehditlere karşı etkili bir savunma sağlar. Bu sayede, Sıfır Güven Yaklaşımı, dinamik ve kapsamlı bir güvenlik sağlama potansiyeli ile organizasyonların güvenliklerini en üst seviyeye çıkarmaktadır.

PAROLANIN HİKAYESİ VE KİMLİK DOĞRULAMA

Dr. Halil Kemal TAŞKIN

Kimlik doğrulama denilince akla gelen en temel yöntem kullanıcı adı ve parola ile kimlik doğrulamadır. Ancak, parola kullanımı her zaman sandığımız kadar kolay olmayabilir. Bunu daha iyi anlayabilmek için kimlik doğrulama sürecini bir geliştiricinin gözünden ele almak faydalı olacaktır: Bir sistemimiz var ve kullanıcılar sisteme kayıt olarak erişim sağlıyorlar. Kullanıcıların kimliklerini doğrulamak için sadece kullanıcının sahip olduğu ve saklama sorumluluğu kendilerinin olacak şekilde bir değer kullanmaları gerekecek. Bu değere parola diyeceğiz.

Kullanıcının parolasını belirlemek için iki temel yöntemden bahsedebiliriz. İlki, kayıt esnasında kullanıcıdan bir parola girmesini istemek, diğer yöntem de kullanıcı kayıt başvurusunu yaptıktan sonra kullanıcı için bir parola üreterek, üretilen parolayı kullanıcıya bildirmek olacaktır.

Kullanıcıya parolanın iletildiği durumu ele alalım. Bu işlem doğrudan ekranda gösterme, e-posta ile gönderme, SMS ile gönderme vb. yöntemlerle olabilir. Sonrasında, kullanıcı bu parola ile sisteme giriş yaptığında ya bu parolayı kullanmaya devam edebilir ya da ilk girişte yeni parola belirlenmesi istenebilir. Yaygın olarak ikinci uygulama kullanılmaktadır.

Her iki durumda da, yani parolayı kullanıcının belirlemesi ya da sistemin kullanıcı için rastgele bir parola üretmesi durumunda, bu değerin veritabanında nasıl saklanacağı siber güvenlik açısından önem kazanıyor. Veritabanının bir saldırgan tarafından ele geçirilmesi durumunda tüm parolalar da ele geçirilmiş olacak ve saldırgan da hesaplara erişebilir hale gelecek. Peki bunun nasıl bir zararı olabilir? Yine iki alternatif üzerinde duralım. İlki, saldırganın veritabanına eriştiğinin sistem yöneticileri tarafından fark edilmemesi. Bu durumda saldırgan istediği hesaplara erişim sağlayabilecektir. Bu da sadece parola kullanmanın tek başına yeterli olmadığını vurgulamak için güzel bir örnek olarak verilebilir.

İkinci senaryoda, varsayalım ki saldırgan hemen tespit edildi ve sistemdeki tüm parolalar sıfırlandı. Kullanıcılara da bildirim gönderilerek saldırının engellendiği, parolaların sıfırlandığı bilgisi iletiliyor. Ancak, gerçek hayatta durum biraz daha farklı olabiliyor, özellikle kullanıcı açısından bakıldığında sürecin davranışsal boyutu devreye giriyor. Kullanıcılar aynı parolayı birden fazla yerde kullanmış olabiliyor. Giderek artan dijital varlıklarımızı göz önüne aldığımızda, aynı şekilde sahip olduğumuz kullanıcı adı ve parola sayısı da artıyor. Her bir hesap için ayrı parolalar üretmek, özellikle de "karmaşık" parolalar üretmek zorlayıcı hale gelebiliyor. Bunun için de parola yöneticisi yazılımlar ya da parolasız kimlik doğrulama teknolojilerinin kullanımından bahsetmek mümkün.

Bahsettiğimiz senaryolar üzerinden çıkaracağımız sonuç **veritabanında parola saklanmaz** olacaktır.

Parola değerini olduğu gibi saklamak yerine, kullanıcının giriş aşamasında yazdığı parolanın kayıt aşamasında oluşturduğu parola ile aynı olup olmadığını doğrulayacak ve parola bilgisini içermeyecek bir değer saklamalıyız. Bu değere "parola doğrulama değeri" diyelim. Parola doğrulama değerinin sahip olmasını beklediğimiz özellikler aşağıda listelenmiştir.

- Paroladan üretilmeli.
- Aynı parola için farklı değerler üretilebilmeli.
- Üretilen değerden parolaya erişmek zor olmalı.
- Bir paroladan üretilmiş parola doğrulama değerini, parola bilgisi (ve ihtiyaç duyulabilecek diğer değerler) olduğunda tekrar üretmek mümkün olmalı.

Bu şartları sağlayacak şekilde bir parola doğrulama değeri üretecektemel çözüm kriptografik özet fonksiyonlar olacaktır.

Bir özet fonksiyon, rastgele uzunluktaki bir değeri sabit uzunluktaki bir değere dönüştürür. Ancak bu özet fonksiyonun kriptografik olarak kabul edilmesi için bazı özellikleri sağlaması gerekmektedir.

Bunları temel olarak aşağıdaki gibi listeleyebiliriz:

- Verilen bir değer için özet fonksiyonunu hesaplamak kolay olmalıdır.
- Bilinen bir özet değerine ait metni bulmak zor olmalıdır.
- Bilinen bir metin ile aynı özet değerini üretecek ikinci bir metin bulmak zor olmalıdır.
- Aynı özet değerine sahip iki metin bulmak zor olmalıdır.

Kriptografik özet fonksiyonların sahip oldukları özellikler sayesinde birbirine çok yakın parolaların bile özet değerleri birbirinden istatistiksel olarak farklı olacaktır. Bu doğrultuda, veritabanında saklamamız gereken değerler parola doğrulama değerleri olmalı. Parola doğrulama değerlerini aslında özet fonksiyon çıktıları olarak ifade edebiliriz ancak parolaların sadece özet değerini hesaplayarak saklamak yeterli midir? (Cevap tabi ki hayır.)

Bu durumdan başlayarak sırayla farklı başlıkları değerlendirelim:

Parolanın Özet Değerini Saklamak

Kullanıcının kayıt aşamasında parolasını girdiğini varsayalım. Parolanın özet değerini hesaplandı ve veritabanına yazıldı. Artık veritabanında parolanın özet değeri mevcut. Güvenlik bakış açısı ile problemleri düşünelim:

1. Aynı parolalar aynı değerlere sahip olacak. Dolayısıyla veritabanına erişim sağlandığında aynı parolayı kullanan kullanıcılar kolaylıkla tespit edilebilecek.

2. Popüler özet fonksiyonlar için (SHA1, MD5 vb.) Internet üzerinde birçok önceden hesaplanmış hazır listeler mevcut. Eğer tahmin edilebilen bir parolanız var ise, bu listeler kullanılarak parolaların çözülmesi mümkün olabilmektedir. Internet üzerinde arama yaparak ücretli ve ücretsiz birçok hazır listeye ulaşmak ve sorgu yapmak mümkün.

Kaba Kuvvet ve Sözlük Saldırıları

Özet değerlerinden parolayı ele geçirme/bulma konusu ile ilgili olarak, yaşanan siber saldırılar sonucu ele geçirilen parolalardan en çok kullanılanlara Internet üzerinde farklı listelerden ulaşmak mümkün. Bu listeler içindeki parolaların özet değerlere karşılık gelip gelmediğini test etme işlemine sözlük saldırısı denilmektedir. Benzer şekilde, belirli bir alfabe içindeki tüm karakterleri kullanarak sırayla deneme işi de kaba kuvvet saldırısı olarak adlandırılmaktadır. Kaba kuvvet ve sözlük saldırılarının bir ileri adımı olarak gökkuşağı (rainbow) tablosu saldırılarından bahsedebiliriz. Rainbow tablosu, bir özet fonksiyon algoritması için önceden hesaplanmış değerlerin olduğu tablodur. Rainbow tabloları zaman-bellek ödünleşimi (time-memory trade-off) doğrultusunda kaba kuvvet saldırılarının istatistiksek olarak iyileştirilmiş bir halidir.

Salt (Tuz) Kullanımı

İngilizcede salting (tuzlama) olarak geçen bu işlem aslında yemek tarifi benzerliğinden geliyor. Nasıl yemeğe katılan tuz miktarı yemeğin lezzetini değiştiriyorsa, özet fonksiyonlarda kullanılacak salt değeri de aynı metinden farklı özet değeri üretimini sağlıyor.

Aynı paroladan farklı değerler elde etmenin çeşitli avantajları olacaktır. Bunlar:

- Aynı parolayı kullanan farklı kullanıcıların veritabanında görünen özet değeri de farklı görünecektir. Dolayısıyla, aynı parola kullanan kullanıcıları tespit etmek mümkün olmayacaktır.
- Önceden hesaplanmış hazır tabloların (sözlük, rainbow) kullanımını engelleyecektir ya da zorlaştıracaktır.

Artık, oluşturulan özet fonksiyon değeri ile birlikte salt değerini de saklamak gerekecektir. Çünkü kullanıcı giriş yaparken parolasını girdiğinde veritabanında yazılı değerin aynısını elde edebilmek için parola ile birlikte bu salt değerine de ihtiyaç olacaktır. Bu durumda parola doğrulama değerimiz özet fonksiyon değeri ve kullanılan salt değeri olacaktır. Salt değerinin uzunluğu, tekrarlı kullanımı gibi durumlara dikkat edilmelidir. Salt değerinin kısa olması yapılacak parola kırma saldırılarının başarısını artıracaktır.

Salt değerinin tekrarlı ya da her kullanıcı için farklı şekilde kullanılıp kullanılmayacağı da önemlidir. Örneğin, veritabanına özel sabit bir salt belirleyip, tüm parolalarda bu salt değerinin kullanılması tercih edilebilir. Ancak, böyle bir durumda bir siber saldırı sonucu salt değeri ele geçirilirse o veritabanına özel hesaplanmış tablolar oluşturularak parola kırma saldırıları gerçekleştirilebilir. Dolayısıyla, salt değerinin her kullanıcıya özel ve rastgele oluşturulması daha uygun bir çözüm olacaktır. Hatta hem her kullanıcıya özel rastgele bir salt hem de veritabanına özel merkezi bir salt değerinin birlikte kullanımı gibi senaryolarda gündeme gelebilir.

Parolayı Şifrelemek

Özet fonksiyonların dışında şifreleme algoritmaları ile de parolaları veritabanında saklamayı düşünebiliriz. Bu durumda çözülmesi gereken yeni bir problem daha ortaya çıkacaktır: Şifreleme için kullanılacak anahtarın saklanması.

Eğer parolalar veritabanında şifreli saklanıyorsa, şifreleme için kullanılan anahtar (ve varsa salt) değeri aynı ise, aynı parolalar aynı çıktıları üretecektir. Bu da veritabanına erişim sağlayan bir saldırganın kolaylıkla aynı parolayı kullanan kullanıcıları tespit etmesini sağlayacaktır. Parolaların şifrelenmesi durumunda, artık hem veritabanını hem de parolaların şifrelenmesi için kullanılan anahtar(lar)ı korumak gerekecektir. Dolayısıyla, atak yüzeyine yeni bir element daha eklenmiş olmaktadır. Ayrıca, şifreleme kullanımı durumunda anahtara erişim sağlanması ile parolalara açık olarak erişme ihtimali de mevcuttur. Sonuç olarak, parolayı şifreleyerek saklamak çok anlamlı bir çözüm gibi görünmeyebilir.

Çözüm: Anahtar Türetme Fonksiyonları

Özet fonksiyonların en temel özelliklerin birisi hızlı çalışmalarıdır. Dolayısıyla, salt değeri bilinen bir özet fonksiyon çıktısına da parola kırma araçları ile oldukça hızlı sözlük saldırıları yapılabilecektir. Bunu yavaşlatmak için kullanılacak çözümü Anahtar Türetme Fonksiyonu (KDF: Key Derivation Function) olarak ifade edebiliriz.

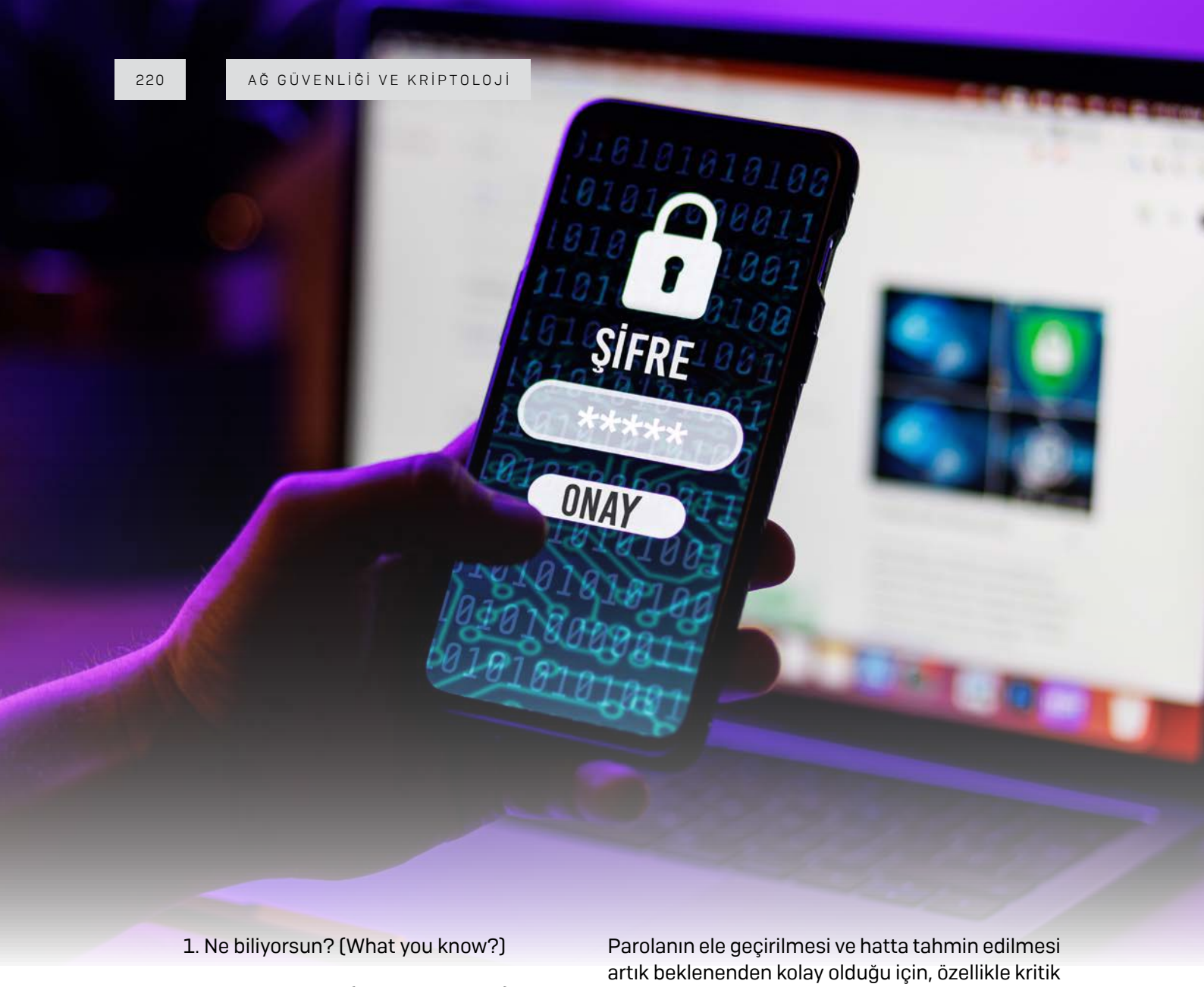
KDF'ler kullanıcıların girdiği parolaların şifreleme algoritmalarının anahtarları olarak kullanılmasında ve parolaların veritabanlarında saklanmasında oldukça kullanışlı çözümler sağlıyorlar. Temel olarak KDF'ler bir özet fonksiyonun belirli parametreler doğrultusunda tekrarlı olarak çalışması sonucu çıktı üretirler. Özellikle GPU ve ASIC tabanlı sistemler ile de yüksek başarımlı parola kırma işlemleri yapılabildiği durumlarda, bunlar için de dayanıklı çözümler sunmaktadır. Örneğin, bir özet fonksiyon algoritması çok az bellek kullanımı yaparken, özel olarak tasarlanmış KDF'ler bellek yoğun işlem yapıları sayesinde parola kırma saldırılarının hızını azaltmaktadır. Popüler bazı KDF'ler PBKDF2, Bcrypt, Scrypt ve Argon2 olarak ifade edilebilir.

Her ne kadar parola kullanımı ve saklanması için teknik olarak uygun önlemler alınabilse de, sadece parola ile kimlik doğrulama yapılması yetersiz kalabilmektedir. Bu doğrultuda, kimlik doğrulama için parola kullanımına ek olarak kullanılabilecek bileşenler de mevcuttur.

Web Üzerinde Akıllı Kart ile Kimlik Doğrulama

Web, hayatımızın vazgeçilmez bir parçası haline geldi ve kullandığımız uygulamalar giderek daha fazla Web teknolojilerini kullanır hale gelmektedir. Bununla birlikte, farklı kimlik doğrulama yöntemlerinin uygulanması güvenlik süreçlerinin temelini oluşturmaktadır.

Kimlik doğrulama başlı başına bir çalışma alanı olarak ele alınabilmekte ve çok farklı çözümlerin sunulabilmektedir. En yaygın kimlik doğrulama yönteminin rahatlıkla kullanıcı adı ve parola ile sistemlere giriş olduğunu söyleyebiliriz. Daha genel olarak baktığımızda kimlik doğrulama için kullanılabilecek ilave bilgileri bize verecek soruları aşağıdaki gibi listeleyebiliriz.



1. Ne biliyorsun? (What you know?)

2. Neye sahipsin? (What you have?)

3. Nesin? (What you are?)

Üçüncü madde ile başlarsak, bu soruya cevap olarak parmak izi, yüz tanıma vb. biyometrik doğrulama yöntemlerini verebiliriz. Hatta davranışsal analiz yöntemleri (parolayı yazma hızınız, kelimeleri klavyede yazma şekliniz vb.) ile yapılan doğrulamaları da bu kapsama alabiliriz. İlk soru ise temel olarak parola/PIN kullanımını ifade etmektedir. İkinci soru ise sahip olduğumuz varlıklar olarak tanımlanabilir. Bunlar fiziksel ya da sanal olabilir. Örneğin, bir akıllı kart ya da tek kullanımlık parola üreteci vb. cihaz olabilir. Bununla birlikte, SMS ya da tek kullanımlık parola (OTP: One-time Password) yöntemleri ile elde edilen parolalar da bu kapsamda değerlendirilebilir.

Parolanın ele geçirilmesi ve hatta tahmin edilmesi artık beklenenden kolay olduğu için, özellikle kritik işlemlerde sadece parola kullanmak güvenli olarak görülmemektedir. Yukarıdaki üç kimlik doğrulama yöntemini birlikte kullanma fikrini düşündüğümüzde karşımıza oldukça iki kavram çıkacaktır: 2FA ve MFA.

İki aşamalı doğrulama (2FA: Two-factor Authentication) ve Çok aşamalı doğrulama (MFA: Multi-factor Authentication), parolanın yanında ilave olarak doğrulanacak değerler için temel tanımları vermektedir. Eğer parola ile birlikte yukarıda belirttiğimiz diğer iki yöntemden en az biri kullanılıyorsa, yani bir adet farklı doğrulama yöntemi uygulanacaksa buna 2FA, eğer birden çok yöntem uygulanacaksa MFA olarak ifade edilmektedir. Günlük hayatta çoğunlukla 2FA yöntemini kullanılıyor olsa da bu doğrulama yönteminin geneli MFA olarak ifade edilebilir.

Akıllı Kartlar ve Web Tarayıcılar

"Neye sahipsin?" sorusuna cevap olarak verilebilecek akıllı kartları ele alalım. Akıllı kartları, üzerinde kriptografik işlemler yapabildiğimiz, fiziksel müdahalelere ve kopyalamaya dayanıklı (içindeki gizli bilgileri çıkarması ve değiştirmesi zor olan) ortamlar olarak ifade edebiliriz. Kriptografik işlemleri, anahtar/sertifika üretme ve depolama, simetrik ve asimetrik kriptografik algoritma operasyonları (şifreleme, şifre çözme, elektronik imza) ve rastgele sayı üretme gibi çeşitlendirebiliriz.

Hem çok aşamalı doğrulama adımı olarak hem de farklı kriptografik ihtiyaçlar doğrultusunda Web tarayıcı ve akıllı kart etkileşimine ihtiyaç duyulmaktadır. Bu etkileşim çeşitli seviyelerde ifade edilebilir:

1. Web tarayıcı uygulamasının akıllı kart ile haberleşmesi.

2. Web sitesinin doğrudan akıllı kart ile haberleşmesi.

3. Web sitesi ile akıllı kartın ortak bir oturumda buluşması.

Akıllı kartları günlük hayatımızda farkında olmasak da sıklıkla kullanıyoruz. Hatta hemen hemen hepimiz cebimizde en az bir adet akıllı kart taşıyoruz. Başta yeni kimlik kartlarımız olmak üzere, kredi/banka kartlarımız, telefon SIM kartları ve elektronik imzalar bu kapsamda değerlendirebilir. Bir uygulamanın akıllı kart ile haberleşmesinde belirli katmanlar vardır. Uygulama ile kart arasındaki haberleşme ISO 7816, PKCS#11, PCSC gibi standartlarla sağlanmaktadır. Web tarayıcılar ve akıllı kartlar arasındaki haberleşme ile ilgili olarak PKCS #11 standardı kullanılmaktadır. PKCS #11 sayesinde, kullandığımız akıllı kartın marka ve modelinden bağımsız olarak kartın fonksiyonlarına erişmek mümkün olmaktadır. Her akıllı karta ait PKCS#11 sürücüleri akıllı kartı üreten firma tarafından yayınlanmaktadır. Dolayısıyla ilgili akıllı kartın kullanılabilmesi için üretici firmanın yayınladığı sürücüler temin edilmelidir. Benzer şekilde, yazılım geliştirme süreçlerine entegrasyon için de yine üretici tarafından sağlanacak olan yazılım geliştirme kitleri (SDK) yayınlanabilmektedir.

Web Tarayıcı Uygulaması ve Akıllı Kart Haberleşmesi

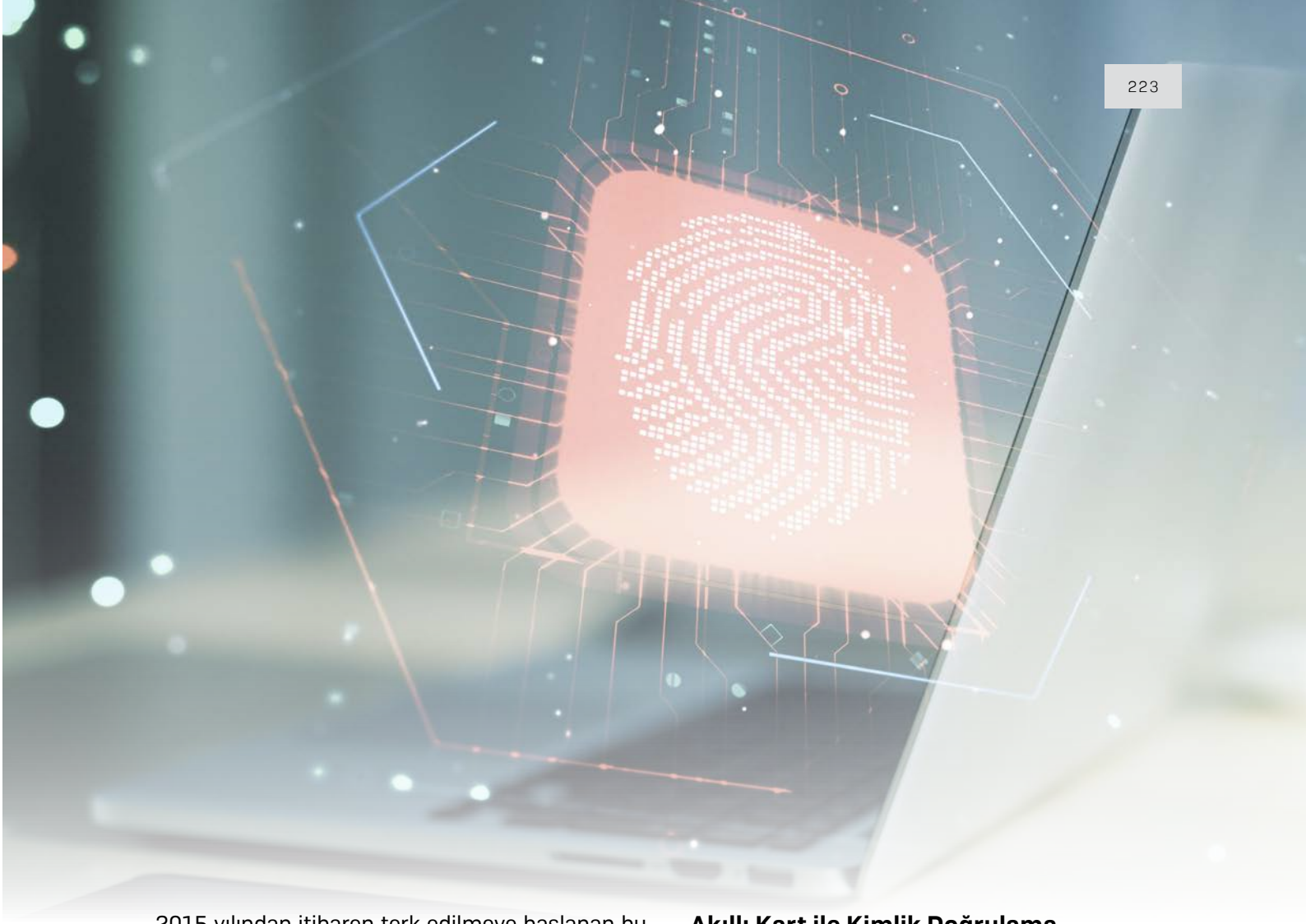
Günümüzde TLS protokolünde kimlik doğrulama çoğu zaman tek taraflı kullanılmaktadır. Sadece istemcilerin sunucuyu doğrulaması sağlanıyor. Ancak, sunucu hangi istemcinin bağlandığını bu aşamada bilmiyor. Bu noktada, TLS'i çift taraflı kullanmak da mümkündür. Bu protokol mTLS (Mutual TLS) olarak adlandırılmakta ve sunucunun da TLS el sıkışması aşamasında istemcinin kimliğini doğrulamasını sağlamaktadır. mTLS yapılandırması özellikle sıfır-güven güvenlik modellerinde de sıklıkla tercih edilmektedir. mTLS'i gerçekleştirmek için istemci taraflı sertifika kullanmak gerekmekte ve bu sertifikayı saklamak için bir akıllı kart kullanmak en uygun çözümlerden birisi olarak karşımıza çıkmaktadır.

Uygun bir kart okuyucu ve kullanılan akıllı kartın PKCS#11 sürücüsü ile web tarayıcı uygulamasına akıllı kartı eklemek mümkündür. Dolayısıyla, akıllı kart üzerindeki sertifikaları artık web tarayıcı uygulaması mTLS el sıkışması için gerekli olan yerde kullanacaktır. Ancak, bu haberleşme TLS seviyesinde gerçekleştiği için, uygulama katmanının haberi olmayacaktır. Dolayısıyla, eriştiğiniz web uygulamasının akıllı kartınız ile herhangi bir etkileşimi olmayacaktır, tüm iletişim web tarayıcı uygulama tarafından yapılacaktır.

Web Sitesi ve Akıllı Kart Haberleşmesi

Web sitelerinin doğrudan akıllı kart ile haberleşmesi ise oldukça eskiye dayanan ve çoğu zaman başarısızlıkla sonuçlanan bir geçmişe sahiptir.

Web tarayıcı uygulamasında açtığımız bir web sitesinin doğrudan akıllı karta erişebilmesi belirli izinler gerekmektedir. Bu durumu, daha genel bir bakış açısı ile web sitesinin USB'den bağlanan bir cihaza erişiminin sağlanması olarak ifade edebiliriz. Web tarayıcı uygulamaları web sitelerinin belirli kısıtlar altında izole olarak çalışmasını sağlarlar. Bu izolasyondan çıkılması için bir tür eklenti sistemi ile bu durumu aşmak gerekmektedir. Tarayıcılarda eklenti desteğinin en eskilerinden birisi olarak 1995 yılında tanıtılan NPAPI arayüzünün bunun için güzel bir örnek olduğunu söyleyebiliriz.



2015 yılından itibaren terk edilmeye başlanan bu arayüz ile Adobe Flash Player, Oracle Java Runtime ve Microsoft Silverlight gibi birçok teknolojiyi web sitelerinin doğrudan sayfa içinde çalıştırması sağlandı.

Web sitesi içerisinde çalıştırılabilen bu eklentiler sayesinde web sitesi işletim sistemi üzerinde belirli yetki ve erişimlere sahip olabiliyordu. Akıllı kart erişimi ile ilgili en yaygın olarak Java ile geliştirilen eklentiler kullanıldı. Web sitesi içerisinde çalışan Java uygulaması üzerinden PKCS#11 ile akıllı karta erişilerek ihtiyaç duyulan (elektronik imza üzerinden kimlik doğrulama ya da belge imzalama gibi) işlemler yapılabiliyordu.

Ancak, bu teknolojilerin web siteleri içine entegre edilmesi uzun vadede hem güvenlik hem de performans problemlerine sebep oldu. Günümüzde NPAPI arayüzünün yaygın kullanımı bulunmamaktadır. NPAPI'nin alternatifleri olarak ActiveX ve PPAPI gibi teknolojiler de kullanılmıştır. Günümüzde bu teknolojilerin hiçbirisi aktif olarak kullanılmamakla birlikte kısmen destek sunmaya devam eden web tarayıcı uygulamalar mevcuttur.

Akıllı Kart ile Kimlik Doğrulama

Bir diğer yandan, akıllı kart ile kimlik doğrulamanın nasıl yapıldığına kısaca değinelim. Akıllı kartlarda yüklü olan bir sertifika olduğunu ve bununla elektronik imza atılabildiğini varsayalım. Erişmek istediğimiz web sitesi akıllı kartımızı kullanarak kimliğimizi doğrulamak istediğinde, akıllı karta erişim sağlayarak belirli bir metin için elektronik imza oluşturur. Oluşturulan elektronik imzalı metnin web sitesinin sunucusunda uygun kriptografik kontroller ile doğrulanması sonucu kimlik doğrulama tamamlanır ve ilgili oturum yetkisi verilir.

PKCS#11 ile sağlanan kriptografik yetenekler kimlik doğrulama dışında farklı amaçlar için de kullanılabilmektedir. Bununla birlikte,, sadece kimlik doğrulama için özelleşmiş bir protokol de geliştirilmiş ve tarayıcılara entegre edilmiştir. Google ve Yubico firmaları tarafından 2014 yılında başlatılan ve günümüzde FIDO tarafından devam ettirilen kimlik doğrulama protokollerinin ilki olan Universal 2nd Factor (U2F) çözümü, kimlik doğrulamada 2FA aşaması için web tarayıcı uygulamaların doğrudan desteği ile web sitelerinde USB

kimlik doğrulama tokenlarının kullanılmasını sağlamıştır. Günümüzde, U2F protokolü yerini WebAuthn ve CTAP2 protokollerini destekleyen FIDO2 projesine bırakmıştır. Her ne kadar FIDO2 uyumlu çözümler kimlik doğrulama için web siteleri ile uygun donanımları buluşturan bir standart olsa da, PKCS#11 destekli akıllı kartları kullanma ihtiyacı çeşitli kriptografik yeteneklerinden dolayı halen devam etmektedir.

Web Sitesi ve Akıllı Kartın Ortak Oturum Üzerinden Haberleşmesi

Web siteleri ile akıllı kartları haberleştirebileceğimiz güncel yöntemleri aşağıdaki gibi listeleyebiliriz:

1. Benzersiz bir numara ile oturum eşleştirme
2. Akıllı kartın takılı olduğu istemcide yerel sunucu başlatma
3. Web sayfası üzerinden masaüstü uygulama başlatma

Son maddeyi ele alırsak, Microsoft ClickOnce ve Java Web Start gibi teknolojilerle web sayfaları üzerinden masaüstü uygulamaların çalıştırılmasının sağlanmasıyla akıllı kartın masaüstü uygulama üzerinde web sayfası ile etkileşimi sağlanmakta ve akıllık kart yetenekleri kullanılmaktadır. Çalıştırılan masaüstü uygulama PKCS#11 ile akıllı karta erişerek gerekli işlemleri yapmaktadır. Ancak, farklı platformlara uyumluluğun zor olması ve tarayıcılara özel eklenti kurulumu gereksinimlerinin de etkisiyle bu teknolojiler de günümüzde artık kullanılmamaktadır. Diğer iki yöntem ise günümüzde aktif olarak kullanılmaktadır.

İlk yöntem, web sitesinin ve akıllı kart ile haberleşecek masaüstü uygulamanın birbirinden bağımsız olarak çalışması ve anlık olarak oluşturulacak bir benzersiz oturum numarası üzerinden iki tarafın birbiri ile buluşması olarak ifade edilebilir.

Web sitesine erişip akıllı kart ile giriş yap seçeneği seçildiğinde, web uygulaması bir masaüstü uygulama indirmenizi ve çalıştırmanızı talep edecektir. Web sayfasında görüntülenecek bir oturum kodunun çalıştırılan masaüstü uygulamaya girilmesi ile web sayfası oturumu ve masaüstü uygulama arasında eşleşme sağlanacaktır. Masaüstü uygulama PKCS#11 ile akıllı karta erişip gerekli işlemleri yaptıktan sonra sunucuya bilgileri iletecek ve web sayfası oturumu buna uygun olarak devam edecektir. Günümüzde Elektronik İmza ile giriş yapılan birçok web sayfasın bu yöntemi kullanmaktadır.

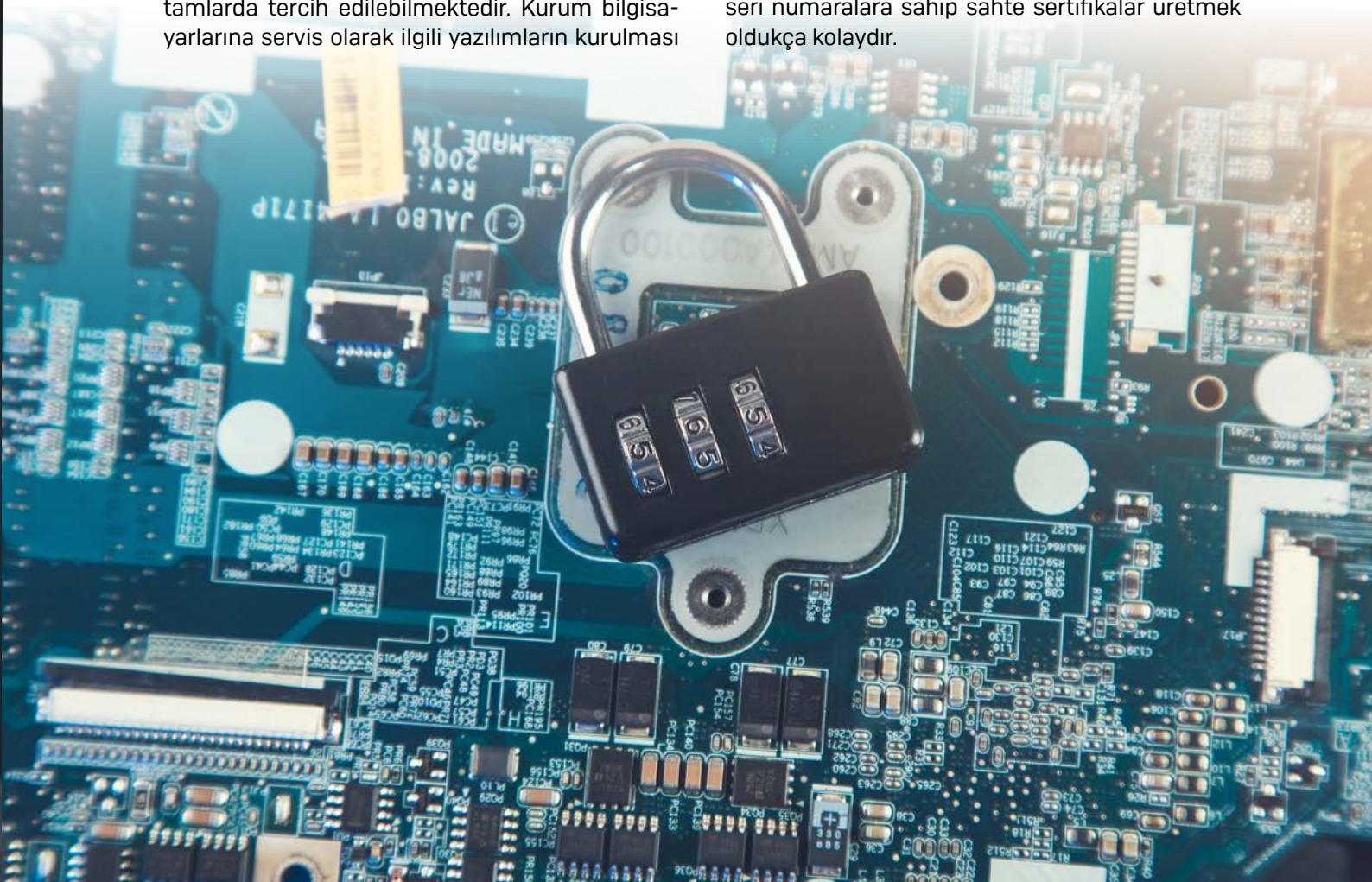
İkinci yöntem ise, akıllı kartın takılı olduğu istemci bilgisayara bir yazılım kurularak yerel bir web servis oluşturulması ve bu web servisin PKCS#11 üzerinden akıllı karta erişim sağlayarak web sitesi ile akıllı kart arasında haberleşmeyi sağlayan servis olarak kurulmasıdır. Erişim sağlanmak istenen web sitesi yüklenirken, yerel olarak kurulan web servisin yerel adresini bileceği için sayfa içerisinde bu adrese istek yaparak akıllı kart ile haberleşmeyi sağlayacaktır. Bu yöntem, daha çok kurumsal ortamlarda tercih edilebilmektedir. Kurum bilgisayarlarına servis olarak ilgili yazılımların kurulması ve web sitelerinin bu servisle haberleşmesi sayesinde akıllı kart işlemleri sağlanmaktadır.

Akıllı Kart Kullanımında Yapılan Bazı Yanlışlar

Akıllı kartları kullanırken kriptografik özelliklerini doğru kullanmak önem arz etmektedir. Akıllı kart ile kimlik doğrulama yapılırken yaşanabilecek bazı yanlış kullanım senaryoları aşağıda listelenmiştir:

1. Akıllı Kartın Kriptografik Özelliklerini Kullanmamak

Akıllı kart kullanarak kimlik doğrulama yapmak isteyen bir web sitesinin akıllı kartın kriptografik yeteneklerini (elektronik imza ve sunucu taraflı kriptografik doğrulama) kullanarak bu işlemi gerçekleştirmesi gerekmektedir. Ancak, akıllı kart kontrolünün kart seri numarası ve/veya sertifika seri numarası üzerinden yapılması kriptografik yeteneklerin kullanılmaması anlamına gelmektedir. Seri numaralar kolaylıkla kopyalanarak aynı seri numaralara sahip sahte sertifikalar üretmek oldukça kolaydır.



2. Akıllı Kartın PIN Kodu Doğrulamasını Harici Olarak Yapmak

PKCS #11 üzerinden yapılan kart haberleşmesinde kartın PIN kodu doğrulaması yapılarak işlemler gerçekleştirilmektedir. Kullanıcının yazdığı PIN kodunun veritabanı gibi yerlere ayrıca kaydedilerek depolanması ve bu değerler üzerinden kontrol edilmesi ihtiyacı yoktur. Kullanıcıdan gelen PIN kodu değerinin doğrudan kart üzerinde PIN kodu doğrulaması yapılarak kontrolü sağlanmalıdır. Ayrıca, akıllı kartın PIN kodunun uygulama harici başka bir yerde değiştirilmesi sonucu kartın doğrulanmasında sorun yaşanacaktır ve iş akışına yönelik de sorun oluşacaktır.

3. Kart ve Kullanıcı Eşleştirmesini Sertifika Dışında Veritabanı Ortamında Yapmak

Hangi kullanıcının hangi sertifikaya sahip olduğu bir veritabanı üzerinde eşleştirme yapılarak değil, her kullanıcıya verilen sertifikaların içinde o kullanıcıya ait bilgilerin verilmesi ile sağlanmalıdır. Bu da üretilen sertifikaların kriptografik olarak geçerliliğin kontrolünün sağlanmasını gerektirecektir. Açık Anahtar Altyapısının doğru kurgulanması için bu adım da önem arz edecektir.

Güncel Trend: Parolasız Kimlik Doğrulama

Parolaların ele geçirilmesi kaynaklı yaşanan birçok siber güvenlik olayı sonrasında parola kullanmadan kimlik doğrulama yapmanın alternatif yöntemleri araştırılmaya başlandı. Bunun sonucu olarak yeni bir çözüm kategorisi karşımıza çıktı: Parolasız kimlik doğrulama.

FIDO2 protokolü de bu işlemi sağlayan protokollerden birisi. Parolasız çözümlere bakıldığında, sadece fiziksel olarak erişim olan bir cihaz (akıllı telefon vb.) ile eşleşme yapılarak kimlik doğrulama işlemi bu cihaz üzerinden yapılmaktadır. Daha önce bahsedilen 2FA/MFA işlemlerinin parola olmayan adımlarını, cihaz bazlı eşleştirme ile birlikte kullanarak işlem tamamlanmış olmaktadır. Kimlik doğrulama için bir cihaz eşleşmesi olduğundan dolayı bu cihazın çevrimdışı ve çevrimiçi olması senaryolarına göre farklı çözümler üretmek mümkün olmaktadır.

Hayata
Değer
Katan
Teknoloji
aselsan
Sürdürülebilirlik Vizyonumuz
Küresel pazarda yarattığımız değerler ile sürdürülebilir büyümesini koruyan, rekabet gücü ile tercih edilen, stratejik ortak olarak güven duyulan, çevreye ve insana duyarlı bir milli teknoloji firması olma vizyonuyla, çalışmalarımıza devam ediyoruz.
www.aselsan.com
aselsan

BİZİM HİKAYEMİZ, BÜYÜK TÜRK MİLLETİNİN BAĞIMSIZLIK AŞKININ, BİRLİK VE BERABERLİĞİNİN,
TEKNOLOJİ VE İNOVASYONLA HARMANLANMIŞ DESTANSI BİR YOLCULUĞUDUR.
MİMARI SİZ.
TEMİNATI BİZ.
BAĞIŞ İÇİN OKUTUNUZ
TÜRK SİLAHLI KUVVETLERİNİ GÜÇLENDİRME VAKFI
aselsan
TÜRKHAVACILIK UZAYSANAYİİ
ROKETSAN
HAVELSAN
İSBİR
aspilsan
DÖVİZ İLE NAKİT BAĞIŞ HESAPLARI
TÜRKİYE İŞ BANKASI - SWIFT ISBKTRIS - USD
TR85 0006 4000 0024 2383 9100 00
T.C. ZİRAAT BANKASI - SWIFT TCZBTR2A - USD
TR44 0001 0017 4506 0317 4150 52
TÜRKİYE İŞ BANKASI - SWIFT ISBKTRIS - EURO
TR28 0006 4000 0024 2384 0800 00
T.C. ZİRAAT BANKASI - SWIFT TCZBTR2A - EURO
TR81 0001 0017 4506 0317 4150 65
TÜRK LİRASI İLE NAKİT BAĞIŞ HESAPLARI
GARANTİ BANKASI - TL
TR71 0006 2000 1140 0006 2970 83
TÜRKİYE İŞ BANKASI - TL
TR84 0006 4000 0014 2380 8100 00
VAKIF KATILIM BANKASI - TL
TR68 0021 0000 0001 9870 0000 01
HALK BANKASI - TL
TR37 0001 2009 4520 0016 0019 87
T.C. ZİRAAT BANKASI - TL
TR07 0001 0017 4506 0317 4150 39
ZİRAAT KATILIM BANKASI - TL
TR13 0020 9000 0005 7968 0000 01
www.tskgv.org.tr
tskgv_resmi
tskgv_resmi
tskgvresmi
@tsk_gv