Siber Güvenlik: Temel İlkelerden Küresel Stratejilere

Ahsen Beyza Özkul

ahsenbeyza@securedebug.com

İÇİNDEKİLER

Giriş

Dijital teknolojiye olan bağımlılığın her geçen gün arttığı bir dünyada, siber güvenlik hayati bir öneme sahip hale gelmiştir. Veri ihlallerinden fidye yazılımlarına kadar uzanan siber saldırılar, hem sıklık hem de karmaşıklık açısından artış göstererek bireyleri, şirketleri ve hükümetleri etkiliyor. Dijital dünya geliştikçe, tehditler de gelişiyor ve bu durum güvenlik önlemlerinde sürekli bir uyum ve yenilik ihtiyacını doğuruyor.

Bu yazı, siber güvenliğin temel prensiplerini inceleyerek yapay zeka ile yönlendirilen saldırılar ve kuantum hesaplama gibi yeni ortaya çıkan tehditleri ele alıyor. Ayrıca, dijital geleceğimizi korumada küresel işbirliğinin önemine dikkat çekiyor. Bu unsurların anlaşılması, giderek daha karmaşık hale gelen dijital dünyada güvenli bir şekilde yol almak ve korunmak için kritik öneme sahiptir.

Siber Güvenlik

Siber Güvenlik ve Altyapı Güvenlik Ajansı'na (CISA) göre: "Siber güvenlik, ağları, cihazları ve verileri yetkisiz erişim veya suç amaçlı kullanımdan koruma sanatı ve CIA üçlüsünü sağlamaya yönelik uygulamadır."

CIA Üçlüsü güvenlik sistemlerinin geliştirilmesi için temel oluşturan yaygın bir modeldir. Zafiyetleri bulmak ve çözümler geliştirmek için kullanılır.

1) Gizlilik (Confidentiality): Bilginin yalnızca yetkili kişiler tarafından erişilebilir olmasını sağlar. Bu, verilerin yetkisiz erişimlerden ve ihlallerden korunmasını içerir.

2) Bütünlük (Integrity): Bilginin doğru ve değiştirilmemiş olduğunu garanti eder. Bu, verilerin yetkisiz değişikliklerden korunmasını ve güvenilir kalmasını sağlar.

3) Erişilebilirlik (Availability): Bilginin doğru ve değiştirilmemiş olduğunu garanti eder. Bu, verilerin yetkisiz değişikliklerden korunmasını ve güvenilir kalmasını sağlar.

Siber Güvenlik Neden Önemlidir?

1) Gizliliğin Dokunulmazlığı: Gizlilik temel bir haktır ve İnsan Hakları Evrensel Beyannamesi (Madde 12), Avrupa İnsan Hakları Sözleşmesi (Madde 8) ve Avrupa Birliği Temel Haklar Şartı (Madde 7) ile güvence altına alınmıştır. Siber güvenlik, bireylerin bu hakkını korur, kişisel bilgilerin yetkisiz erişime karşı korunmasını sağlar.

2) Hassas Verileri Koruma: Verilerin dijitalleşmesiyle birlikte, ticari sırlar, fikri mülkiyet ve diğer hassas bilgilerin korunması hayati önem kazanmıştır.
3) Kritik Altyapıyı Koruma: Elektrik şebekeleri, sağlık tesisleri, ulaşım sistemleri ve iletişim ağları gibi kritik altyapılar, birbiriyle bağlantılı bilgisayar sistemlerine dayanır. Bu sistemlere yapılan siber saldırılar, temel hizmetlerde kesintilere ve bireylerin güvenliğini tehdit eden sonuçlara yol açabilir. Kötü niyetli aktörler, sistemlerdeki zafiyetleri bilerek istismar edebilir, bu da hayati operasyonların aksamasına neden olabilir.
4) Finansal Kaybı Önleme: Siber suçların 2025 yılına kadar dünya genelindeki işletmelere yıllık 10,5 trilyon dolara mal olacağı tahmin ediliyor. Finans sektöründe siber güvenlik, dolandırıcılık ve şantaj gibi yaygın tehditlere karşı kritik bir öneme sahiptir. Bir siber ihlalden kurtulmak, olay müdahalesi, sistem onarımları ve adli incelemeler gibi ciddi maliyetlere neden olabilir.

Siber Güvenlik Nede Daha Kritik Hala Geliyor?

1) Siber uzay, siber güvenlikten daha hızlı büyüyor
    a. Siber uzay, ilk olarak william gibson tarafından 1984'teki "neuromancer" kitabında kullanılan bir kelimedir. Kelimenin kendisi "bilgisayar ağları üzerinden iletişimin gerçekleştiği ortam" anlamına gelir. Siber uzay, farklı bilgisayar sistemlerini bağlayan dinamik ve sanal alan olarak tanımlanır. Beyindeki sayısız nöron gibi, siber uzayda da bilgisayar sistemleri arasında sayısız bağlantı ve ağ vardır.

2) Yapay zeka gelişmeleriyle, siber suçlular daha gelişmiş hale geliyor siber saldırılar her gün yeni biçimler alıyor.

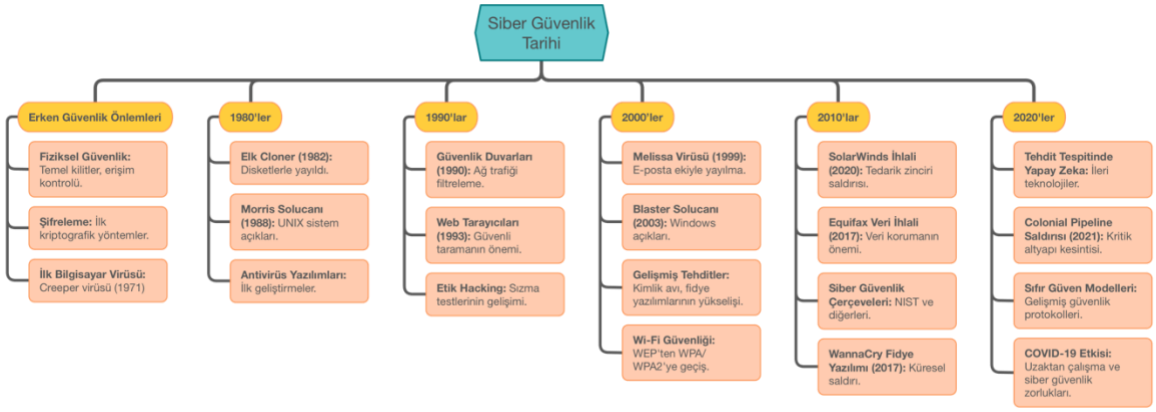
3) Daha fazla veri dijitalleşirken, IOT (Nesnelerin İnterneti) ile daha fazla verinin korunması gerekiyor.

Siber Güvenlik Tarihi

1) Siber güvenlik, erken ana bilgisayarlar için temel fiziksel güvenlikle başladı ve ağların ortaya çıkmasıyla parolalar, şifreleme ve erişim kontrolleri ile gelişti. İlk bilgisayar güvenliği olayı, dijital tehditlerin başlangıcını işaret eden Creeper virüsü (1971) idi.
2) 1980'lerde, kişisel bilgisayarların ve internetin yükselişi, Elk Cloner ve Morris Solucanı gibi erken virüsleri tanıttı ve bu da antivirüs yazılımlarının ve daha iyi uygulamaların geliştirilmesine yol açtı. 1990'lar, güvenlik duvarlarını ve etik hacklemeyi zafiyetleri ele almak için getirdi.
3) 2000'lerde, solucanlar, Truva atları ve kimlik avı gibi tehditlerin artışı, çok faktörlü kimlik doğrulama, VPN'ler ve izinsiz giriş tespit sistemlerinin benimsenmesine yol

açtı. Kablosuz ağları güvence altına almak için ileri düzey şifreleme yöntemleri tanıtıldı.

4) 2010'lara gelindiğinde, WannaCry fidye yazılımı ve Stuxnet gibi saldırılar, NIST gibi kapsamlı çerçevelere duyulan ihtiyacı ve siber güvenlik eğitiminin önemini vurguladı.
5) 2020'de, COVID-19 nedeniyle uzaktan çalışmaya geçiş, uzaktan ortamların güvence altına alınmasına odaklanmayı artırdı, VPN'ler, güvenli işbirliği araçları ve ileri düzey uç nokta güvenliği kullanımına yol açtı. SolarWinds ihlali, tedarik zinciri güvenliğinin önemini vurguladı ve sıfır güven modellerinin benimsenmesini hızlandırdı.



Başlıca Siber Güvenlik Disiplinleri

1) Ağ Güvenliği: Bu, ağ altyapısının tamamını saldırılardan ve yetkisiz erişimlerden korumayı içerir.
2) Uygulama Güvenliği: Uygulamaları zafiyetlerden ve tehditlerden korumaya odaklanır. Uygulama güvenliği, tasarım, geliştirme ve dağıtım dahil olmak üzere tüm geliştirme aşamalarında uygulanabilir ve uygulanmalıdır.
3) Bilgi Güvenliği: Geniş anlamda, bilgiyi yetkisiz erişimden koruyan güvenlik prosedürleri ve araçlar setidir. Bilgi güvenliği, altyapı ve ağ güvenliği, denetim ve test dahil olmak üzere çeşitli BT alanlarını kapsar.
4) Bulut Güvenliği: Dış ve iç tehditleri ele almak için tasarlanmış prosedürler ve teknolojilerdir. Bulut altyapısı, tüm sektörlerde ve birçok dikeyde modern bilişimin neredeyse tüm yönlerini destekler.
5) IoT (Nesnelerin İnterneti) Güvenliği: IoT cihazları, güvenlik kameraları ve akıllı ev aletleri gibi bağlı nesnelerdir. IoT güvenliği, bu cihazları ağ tehditlerinden korumayı içerir.
6) Uç Nokta Güvenliği: Uç nokta güvenliği, masaüstü bilgisayarlar, dizüstü bilgisayarlar ve mobil cihazlar gibi cihazları siber güvenlik tehditlerinden korumayı içerir. Bu uç noktalar, siber suçluların kurumsal ağlara erişmesi için potansiyel giriş noktaları olabilir.

Siber Güvenlik Tehditleri

Verilerin CIA'sını (Gizlilik, Bütünlük ve Erişilebilirlik) tehlikeye atmayı amaçlayan kötü niyetli faaliyetlerdir. Bu tehditler veri ihlallerine, finansal kayıplara ve itibar zararlarına yol açabilir. Bu tehditler bireysel hackerlar veya organize suç gruplarından gelebilir.

1) Kötü Amaçlı Yazılım (Malware): Herhangi bir programlanabilir cihazı, hizmeti veya ağı zarar vermek veya kötüye kullanmak için tasarlanmış bir yazılımdır.
    - Virüsler, Truva Atları, Solucanlar, Botnetler
    - Örnek: 2017'deki Wannacry Fidye Yazılımı saldırısı. Wannacry, birçok bilgisayarın zarar görmesine ve İngiltere veya NHS gibi sağlık hizmetlerinin büyük ölçüde etkilenmesine yol açtı.
    - Savunma Yöntemleri: Antivirüs programları ve düzenli tarama yapma. Cihazların güncel tutulması, güvenlik açıklarının düzenli olarak kapatılması. Ayrıca, bazı ağ güvenliği önlemleri, örneğin Güvenlik Duvarları ve IDS'ler, kötü amaçlı yazılımların önlenmesine yardımcı olabilir.
2) Phishing (Oltalama)(Kimlik Avı): Bildirilen güvenlik olaylarının %80'inden fazlasını oluşturur. Oltalama saldırganları, güvenilir bir varlık gibi davranarak hassas verileri elde eder.
    - Örnek: Bankalardan veya güvenilir kuruluşlardan gelen e-postalar.
    - 2016'daki John Podesta e-posta saldırısı, o yılki ABD başkanlık seçimlerini etkiledi.
3) Parola Saldırıları: Kullanıcının parolasını elde etmek veya çözmek amacıyla yapılan saldırılardır.
    - Örnek: Kaba Kuvvet Saldırıları, Sözlük Saldırıları, Klavye Kayıtçıları.
    - LinkedIn 2012 Saldırısı
4) DDoS Saldırıları (Dağıtılmış Hizmet Engelleme): Bir ağı aşırı trafik ile doldurarak hizmeti kesintiye uğratmayı amaçlar
    - GitHub 2018 Saldırısı (Saldırı çok büyük olmasına rağmen, GitHub bu saldırıyı bir dakika içinde DDoS koruma hizmetleri kullanarak hafifletebildi.)
5) MitM Saldırısı (Orta Nokta Saldırısı): İki taraf arasındaki iletişimi, tarafların bilgisi olmadan kesip değiştirmeyi ifade eder.

- 2015 Superfish Olayı

Siber Güvenlik Çerçeveleri

Kuruluşların mevcut siber güvenlik uygulamalarını değerlendirmelerine ve bunları geliştirmelerine yardımcı olan risk bazlı yönergelerdir. Bu çerçeveler, siber güvenlik risklerini yönetmek için yapılandırılmış bir yaklaşım sunar. ISO ve NIST Çerçeveleri, siber güvenlikte en çok başvurulan iki çerçevedir. Her ikisi de benzer amaçlar hizmet etse de, bazı önemli farklılıklar vardır.

1) **ISO 27001:** Bilgi Güvenliği Yönetim Sistemi (ISMS) için gereksinimleri belirleyen uluslararası bir standarttır. Kuruluşun ihtiyaçlarına göre uyarlanmış siber güvenlik uygulamalarını kurmayı, uygulamayı, sürdürmeyi ve geliştirmeyi hedefler.
2) **NIST Cyber Security Framework (CSF):** ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilen bu çerçeve, öncelikli olarak kritik altyapı sektörlerine yöneliktir. Kuruluşların siber güvenlik risklerini tanımlamalarına, korumalarına, tespit etmelerine, yanıt vermelerine ve iyileşmelerine yardımcı olur. NIST CSF, ISO 27001'den daha esnektir ve daha az ayrıntılıdır, bu nedenle kuruluşların uyum sağlaması daha kolaydır.
3) **NIST 800-53:** Federal bilgi sistemleri için güvenlik ve gizlilik kontrollerini sağlayan ayrıntılı bir düzenleyici belgedir. NIST CSF'den daha kapsamlıdır ve geniş bir gereksinim yelpazesi sunar, ancak daha katıdır ve genellikle devlet kurumları için tasarlanmıştır.

4) **Diğer Çerçeveler:**

- **COBIT**: Kurumsal BT'nin yönetimi ve yönetişimi için bir çerçevedir. Kuruluşların risk, kaynak kullanımı ve BT değerini dengelemelerine yardımcı olur.
- **ITIL**: : BT hizmet yönetimine odaklanır ve kaliteli BT hizmetleri sağlamak için en iyi uygulamaları içerir. ITIL Güvenlik Yönetimi, ISO 17799'a dayanır ve güvenliği BT hizmet süreçlerine entegre eder.
- **COSO**: Öncelikli olarak bir finansal kontrol çerçevesidir, ancak risk yönetimini de etkiler ve BT güvenliğinde resmi risk değerlendirmeleri gerektirir.

Siber Güvenlikte Güncel Trendler ve Zorluklar

1) Yapay Zeka (AI) ve Makine Öğrenmesi: Yapay zeka (AI), siber güvenliğin evriminde giderek daha önemli bir bileşen haline geliyor ve siber saldırıların sürekli artan tehdidine karşı gelişmiş, otomatik ve proaktif savunma mekanizmaları sunuyor. Geleneksel siber güvenlik yöntemleri hala önemli olsa da, sofistike saldırılar karşısında genellikle yetersiz kalıyor. AI, büyük veri miktarlarını analiz ederek, kalıplardan ve davranışlardan öğrenerek ve insan müdahalesine ihtiyaç duymadan gerçek zamanlı kararlar vererek bu boşluğu doldurur. AI, siber tehditleri anında tespit edip yanıt verebilir, potansiyel zararları azaltma süresini kısaltır. Ayrıca, zayıf noktaları belirlemede ve potansiyel gelecekteki saldırıları tahmin etmede yardımcı olur. Bu süreçleri otomatikleştirerek, AI siber güvenlik ekiplerinin iş yükünü önemli ölçüde azaltır ve onların daha karmaşık sorunlara odaklanmalarına olanak tanır. Ancak, AI'nin siber güvenlikte bir panasea olmadığı unutulmamalıdır. AI destekli sistemlerin etkinliği, kullanılan veri ve algoritmaların kalitesine büyük ölçüde bağlıdır. Siber suçlular da AI'yi kötü niyetli amaçlar için kullanmaya başladıkça, siber güvenlik alanının AI teknolojilerini geliştirmeye devam etmesi gerekecek

2) Bulut Güvenliği: Bulut bilişim esneklik ve maliyet tasarrufu sağlar ancak benzersiz güvenlik zorlukları getirir:

    a. Zorluklar
        i. Veri İhlalleri: Bulut ortamları, hassas bilgileri çalmak isteyen hackerlar tarafından hedef alınabilir.
        ii. İç Tehditler: Erişimi olan çalışanlar veya yükleniciler, güvenlik sorunlarına neden olabilirler, ister istemez ister kasıtlı olarak.
        iii. Veri Kaybı: Veri, yedekleme çabalarına rağmen, kazara silme veya sağlayıcı kesintileri nedeniyle kaybolabilir.
        iv. Uyumluluk: Uluslararası veri ile özellikle karmaşık olan veri koruma düzenlemelerine uyum sağlamak zor olabilir.

v. Paylaşılan Sorumluluk: Güvenlik, bulut sağlayıcısı (bulut altyapısını güvence altına alır) ve müşteri (veri ve uygulamaları güvence altına alır) arasında paylaşılır.
vi. Yanlış Yapılandırmalar: Yanlış ayarlar verileri yetkisiz erişime açabilir.

b. Stratejiler

i. Veri Şifreleme: Verileri, yetkisiz erişimden korumak için hem aktarımda hem de dinlenme durumunda şifreleyin.
ii. Erişim Kontrolleri: Hassas bilgilere kimlerin erişebileceğini sınırlamak için güçlü kimlik doğrulama ve rol tabanlı erişim kullanın.
iii. Düzenli Güvenlik Kontrolleri: Potansiyel güvenlik sorunlarını bulmak ve düzeltmek için düzenli değerlendirmeler yapın.
iv. İzleme ve Kaydetme: Şüpheli davranışları hızla fark etmek ve yanıt vermek için bulut faaliyetlerini izleyin.
v. Olay Yanıtı: Güvenlik olaylarına yanıt vermek ve iyileşmek için bir plan oluşturun.
vi. Uyumluluk: Bulut hizmetlerinizin yasal ve düzenleyici gereksinimleri karşıladığından emin olun.
vii. Çalışan Eğitimi: İnsan hatalarını azaltmak için en iyi güvenlik uygulamaları konusunda personeli eğitin.

Hükümetlerin ve Uluslararası İşbirliğinin Siber Güvenlikteki Rolü:

1) Uluslararası Çerçeveler: Tutarlı güvenlik önlemleri için küresel siber güvenlik standartları ve en iyi uygulamaları geliştirmek.
2) Bilgi Paylaşımı: Tehditler ve zayıflıklar hakkında bilgi paylaşarak toplu savunmayı geliştirmek.
3) Sınır Ötesi Hukuk Uygulaması:Sınırları aşan siber suçlara yanıt vermek için uluslararası işbirliği yapmak.
4) Kapasite Geliştirme: Daha az güvenli bölgelerin siber güvenlik kapasitelerini geliştirmelerine yardımcı olmak.
5) Siber Güvenlik Diplomasisi: Siber uzayda sorumlu davranışları belirlemek ve çatışmaları önlemek için küresel tartışmalara katılmak.

Kaynaklar

1. Planet Compliance. (2022, 30 Kasım). *Finansal siber güvenlik: Üçüncü taraf riski*. Planet Compliance. https://www.planetcompliance.com/financial-cybersecurity-third-party-risk/
2. Vedantu. (2024). *Siber uzaya giriş*. Vedantu. https://www.vedantu.com/commerce/introduction-to-cyberspace
3. IBM. (t.y.). *Bulut güvenliği*. IBM. https://www.ibm.com/topics/cloud-security
4. Kaspersky. (t.y.). *Uç nokta güvenliği nedir?* Kaspersky. https://www.kaspersky.com/resource-center/definitions/what-is-endpoint-security
5. Microsoft. (t.y.). *Bilgi güvenliği (Infosec) nedir?* Microsoft. https://www.microsoft.com/en-us/security/business/security-101/what-is-information-security-infosec
6. Institute Data. (2024, 2 Nisan). *Siber güvenliğin 7 türü nedir?* Institute Data. https://www.institutedata.com/blog/what-are-the-7-types-of-cyber-security/
7. Tunggal, A. T. (2024, 25 Nisan). *Siber güvenliğin önemi*. UpGuard. https://www.upguard.com/blog/cybersecurity-important
8. Bayuk, J. [Jennifer Bayuk]. (2019, 22 Ekim). *Siber güvenliğin tarihi* [Video]. YouTube. https://www.youtube.com/watch?v=lvxFE-HO7oc
9. 51Sec. (2018, Aralık). *Siber güvenlik çerçeveleri ve kaynaklar*. 51Sec. https://blog.51sec.org/2018/12/cyber-security-frameworks-resources.html#point14