OCAK_MART 2024

SİBER TEHDİT DURUM RAPORU

STM MÜHENDİSLİK TEKNOLOJİ DANIŞMANLIK

thinktech STM Teknolojik Düşünce Merkezi

SORUMSUZLUK VE FİKRİ MÜLKİYET HAKKI BEYANI
İşbu eserde/internet sitesinde yer alan veriler/bilgiler ticari amaçlı olmayıp tamamen kamuyu bilgilendirmek amacıyla yayımlanan içeriklerdir. Bu eser/internet sitesinde bulunan veriler/bilgiler tavsiye, reklam ya da iş geliştirme amacına yönelik değildir. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. işbu eserde/internet sitesinde sunulan verilerin/bilgilerin içeriği, güncelliği ya da doğruluğu konusunda herhangi bir taahhüde girmemekte, kullanıcı veya üçüncü kişilerin bu eserde/internet sitesinde yer alan verilere/bilgilere dayanarak gerçekleştirecekleri eylemlerden ötürü sorumluluk kabul etmemektedir.
Bu eserde/internet sitesinde yer alan bilgilerin her türlü hakkı STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'ye ve/veya eserde atıf yapılan kişi ve kurumlara aittir. Yazılı izin olmaksızın eserde/internet sitesinde yer alan bilgi, yazı, ifadenin bir kısmı veya tamamı, herhangi bir ortamda hiçbir şekilde yayımlanamaz, çoğaltılamaz, işlenemez.

İÇİNDEKİLER

Sorumsuzluk ve Fikri Mülkiyet Hakkı Beyanı 2
İÇİNDEKİLER 3
ŞEKİLLER 4
GİRİŞ 5
TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK 5
1. Sosyal Mühendislik: İnsan Zafiyetinden Yararlanan Bir Tehdit 5
Sosyal Mühendislik Nedir? 5
Sosyal Mühendislik Nasıl Yapılıyor? 6
Günümüzde Sosyal Mühendislik 6
Nasıl Korunabiliriz? 6
2. Inception Saldırıları 7
Sanal Gerçeklikte Yeni Tehdit: Inception Saldırıları 7
Inception Saldırısı Nedir? 7
Inception Saldırıları Nasıl Gerçekleştirilir? 7
Inception Saldırılarının Riskleri 7
Inception Saldırılarına Karşı Önlemler 7
Inception Saldırıları Hakkında Ek Bilgiler 8
3. C++ ile C'den Rust ile Go'ya: Bellek Güvenliği Odaklı Programlama Dillerine Geçiş 8
4. LockBit: Küresel Ekonomi ve Güvenliğe Karşı Yükselen Tehdit 9
Giriş: 9
LockBit Nedir? 9
LockBit Saldırıları: 10
Sonuç: 11
5. Dijital Tehditlerin Gölgesinde: Phishing ve İnternet Bankacılığı Dolandırıcılığı 11
6. Milyonlarca Kullanıcının Verileri Sızdırıldı 12
7. Ukrayna Saldırısı Öncesinde Viasat'a Yapılan Siber Saldırı 12
8. Değişim ve Siber Güvenliğin Geleceği: NIST CSF 2.0'daki Yenilikler ve Değişiklikler Neler? 13
NIST CSF 2.0'daki Yenilikler Neler? 15
9. Siber Güvenlik Risk Yönetiminde Kullanılan Standartlar 15
Risk Yönetimi 16
Sonuç: 18
DÖNEM KONUSU 18
10. Açık Kaynak Kod Güvenliği: Risklerin Azaltılması ve Güvenli Yazılım Kullanımı 18
11. IoT Cihazların Siber Güvenlik Regülasyonları 20
Honeypot Verileri 22
KAYNAKÇA 25

ŞEKİLLER

Şekil 1: Gerçek VR sistemi kullandığını sanan fakat aslında Inception saldırısı tuzağına düşen bir kullanıcı senaryosu örneği 7
Şekil 2: VRChat uygulamasının klonuyla yapılabilecek senaryo örneği 7
Şekil 3. Microsoft'un her yıl CVE atadığı güvenlik açıklarının yüzde 70'i bellek güvenliği ilişkisi 8
Şekil 4. Phishing 12
Şekil 5. Data 12
Şekil 6. NIST CSF 2.0 Yol Haritası 14
Şekil 7. NIST CYBERSECURITY FRAMEWORK (CSF) 2.0 Kaynakları 15
Şekil 8. NIST 800-30 Risk Değerlendirme Süreç Akışı 17
Şekil 9. ISO 27005 Risk Değerlendirme Süreci 17
Şekil 10. NIST 800-30 Risk Değerlendirme Süreci 17
Şekil 11. Açık kaynak kod güvenliği 19
Şekil 12. GitHub üzerinde popüler bir proje örneği 19
Şekil 13. npm audit çıktısı 19
Şekil 14. VSCode üzerinde çalışabilen örnek bir SCA aracı 20
Şekil 15: IoT Cihaz Örnekleri 20
Şekil 16. IoT Güvenlik Zafiyetleri ve Zorlukları 21
Şekil 17: IoT cihazların siber güvenliğe etkileri 21
Şekil 18. IoT cihazların Siber Güvenliğe Etkileri 22
Şekil 19. Gelen saldırıların ülkelere göre dağılımı. 22
Şekil 20. Parola etiket bulutu. 23
Şekil 21. Kullanıcı adı etiket bulutu 24

GİRİŞ

Siber Güvenlik Müdürlüğü tarafından hazırlanan 2024 yılının ilk raporunda yine birbirinden ilginç konularla karşınızdayız. İlk konumuz, siber güvenlik alanının en zayıf halkası olan insan faktörü kullanılarak gerçekleştirilen saldırılar olarak tanımlanan sosyal mühendislik saldırıları. Ardından, özellikle VR gözlükler üzerinde yapay zekâ araçlarıyla oluşturulan gerçekçi sesleri ve görselleri kullanan Inception saldırısını inceliyoruz. Ardından programlama dillerinde ön plana çıkan bellek güvenliği konusuna ışık tutuyoruz.

Özellikle fidye yazılımlarının kullanımının arttığı bu dönemde küresel ekonomiye karşı bir tehdit olan ve sürekli olarak güncellendiği için büyük bir tehlike arz eden LockBit zararlı yazılımı konusunda detaylı bilgiler sunuyoruz. Hemen sonrasında, banka işlemlerinin neredeyse tamamının internet üzerinden yapıldığı günümüzde, internet bankacılığı dolandırıcılıklarında insan faktörünün istismar edilmesini engellemek için ne gibi önlemler alınabileceğini açıklıyoruz.

Son zamanların en sansasyonel sızıntısı olan, yaklaşık olarak 26 milyar kullanıcının etkilendiği ve "Mother of All Breaches" olarak adlandırılan sızıntıya dair ilgi çekici bilgileri sizlerle paylaşıyoruz. Devamında ise Ukrayna savaşı öncesinde Viasat'a karşı yapılan siber saldırının detaylarını konu alıyoruz.

National Institute of Standards and Technology (NIST) tarafından hazırlanan ve siber savunmayı artırmayı amaçlayan Siber Güvenlik Çerçevesi'nin (CSF), NIST tarafından çıkarılan ikinci versiyonunu inceleyip ilk versiyonu ile ikinci versiyonu arasındaki farkları gösteriyoruz. Hemen sonrasında ise siber güvenlik risk yönetiminde kullanılan standartları irdeliyoruz.

Günümüzde, saniyede tahmini olarak 127 yeni cihazın internete bağlandığı koşullarda, daha detaylı incelenmesi gereken IoT cihazların siber güvenlik regülasyonlarını sizlerle inceliyoruz.

Dönem konusu olarak, son günlerde açık kaynak kütüphanelerde çıkan arka kapı haberlerinden sonra açık kaynak kod güvenliğinde risklerin azaltılması ve güvenli yazılımların kullanımıyla ilgili detaylı bilgileri sizlerle paylaşıyoruz.

Son olarak ise her raporumuzda güncellediğimiz Honeypot verilerimize yer veriyoruz.

Bu rapor, bilişim dünyasındaki güvenlik tehditlerini ve koruma stratejilerini anlamak isteyen herkes için önemli bir kaynak olacak. Güvenlik bilincini artırmak ve siber tehditlere karşı daha iyi hazırlıklı olmak için bu raporu incelemenizi tavsiye ederiz. Güvende kalın!

TEKNOLOJİK GELİŞMELER VE SİBER GÜVENLİK

1. Sosyal Mühendislik: İnsan Zafiyetinden Yararlanan Bir Tehdit

Sosyal Mühendislik Nedir?

Sosyal mühendislik, özel bilgi, erişim veya veri elde etmek için insan zafiyetlerinden yararlanan bir saldırı tekniğidir. Bu tür saldırılar, teknik becerilere ihtiyaç duymadan, insan zafiyetlerinden ve güven duygusundan yararlanarak yapılır. Saldırılar, yüz yüze ve diğer etkileşim yollarıyla ve çeşitli şekillerde gerçekleştirilebilmektedir. En çok kullanılan bazı yöntemler şunlardır:

- **Phishing (Oltalama):** Saldırganlar kendilerini meşru kuruluşlar gibi göstererek e-postalar aracılığıyla alıcıların kişisel verilerini veya kimlik bilgilerini elde etmeye çalışır.
- **Vishing (Telefon Dolandırıcılığı):** Saldırganlar bireylerin hassas bilgileri ifşa etmelerini sağlamak amacıyla telefon görüşmelerini kullanır.
- **Baiting (Yemleme):** Saldırganlar, USB bellek gibi taşınabilir medya cihazlarını veya yazılım programlarını, kullanıcıların ilgisini çekecek şekilde halka açık alanlarda bırakır. Kullanıcılar bu cihazları bilgisayarlarına taktıklarında veya programları çalıştırdıklarında, bilgisayarlarına virüs veya casus yazılım bulaşabilir.
- **Smishing (SMS Dolandırıcılığı):** Saldırganlar, kullanıcıları kandırmak ve onlardan bilgi sızdırmak için sahte metin mesajları gönderir.
- **Whaling:** Bir oltalama saldırısı türüdür ve aynı zamanda kullanıcının cihazıyla iletişim kurarak kişisel bilgilerine erişim sağlar.
- **Business Email Compromise (Yönetici Dolandırıcılığı):** Saldırganın organizasyon içinde finansal işlerle ilgili güvenilir bir yönetici gibi davrandığı bir sosyal mühendislik yöntemidir.
- **Pretexting (Bahane Uydurma):** Kullanıcıları değerli ve hassas verileri paylaşmaya ikna etme olasılığı yüksek olan inandırıcı senaryolar veya önceden hazırlanmış bahaneler oluşturmayı içeren bir sosyal mühendislik yöntemidir.
- **Honeytrap (Bal Tuzağı):** Özellikle çevrimiçi tanışma sitelerinde veya sosyal medyada ilişki arayan bireyleri hedefleyen bir sosyal mühendislik tekniğidir.

- **Tailgating/Piggybacking (Arkasına Saklanma):** Bir saldırganın fiziksel bir tesisin erişimini, kendisinden önce giren kişinin kapıyı açmasını veya kendisine erişim sağlamasını isteyerek elde ettiği bir fiziksel ihlal yöntemidir.
- **Watering Hole (Su Çukuru):** Saldırganın bir organizasyonun sık sık kullandığı web sitelerini tahmin ederek veya gözlemleyerek bir veya daha fazlasını kötü amaçlı yazılımla enfekte ettiği bir sosyal mühendislik yöntemidir.
- **Diversion Theft (Yön Değiştirme Hırsızlığı):** Bu tür bir saldırıda, saldırganlar bir teslimat veya kurye şirketini kandırarak yanlış teslim alma veya bırakma konumuna gitmesini sağlayarak işlemi durdurur.

Bu saldırı çeşitleri aynı zamanda birden fazla amaca yönelik olabilir. Saldırgan, verileri bozarak, tahrip ederek, silerek veya değiştirerek hedef sisteme zarar verip olumsuz etkiler yaratabilir. Alternatif olarak, sadece verilere erişim sağlamak isteyen bir saldırgan, hedef sistemi değiştirmeden, yalnızca bilgi, erişim, para gibi değerli varlıkları çalmayı amaçlayabilir[1].

Sosyal Mühendislik Nasıl Yapılıyor?

Çoğu sosyal mühendislik saldırısı, saldırgan ile kurban arasında gerçek iletişime dayanır. Saldırgan, verileri ele geçirmek için bilinen zorlama yöntemlerini kullanmak yerine, kullanıcıyı gönüllü olarak açıklamalar yapmaya yönlendirmeyi amaçlar.

Sosyal mühendislik saldırılarının aşamaları genellikle aşağıdaki gibidir:

- **Hazırlık:** Saldırgan sizin veya parçası olduğunuz daha geniş bir grubun geçmişi hakkında bilgi toplar.
- **Sızma:** İlişki kurarak veya bir etkileşim başlatarak, güven kazanmaya başlar.
- **Kurbandan Faydalanma:** İstediği bilgileri kurbana hissettirmeden alır.
- **Bağlantıyı Kesme:** Saldırıyı tamamlar.

Bu süreç bazen tek bir e-posta, bazen de haftalar süren bir dizi sosyal medya sohbeti olarak gerçekleşebilir. Ancak en nihayetinde süreç, kurbanın bilgilerini paylaşması veya zararlı yazılımlara maruz kalması ile sonuçlanır.

Günümüzde Sosyal Mühendislik

Günümüz dünyasında vazgeçilmez bir rol oynayan yapay zekâ, sosyal mühendislik saldırılarının güçlenmesinde son derece etkili olmaktadır.

Son araştırmalar, saldırganların bugün yapay zekâ araçlarını tamamen benimsediklerini ve başarılı sonuçlar elde ettiklerini göstermektedir. Güvenlik uzmanları, oltalama saldırılarının yapay zekânın benimsenmesiyle birlikte arttığını ve bu konuda kullanılan e-postaların daha iyi ve sofistike hâle geldiğini belirtmektedir. Özellikle son bir yıl içinde yapay zekâ kullanılarak yapılan oltalama e-posta saldırılarının yüzde 135 arttığı gözlemlenmiştir.

Yapay zekânın ilk gündeme geldiği dönemlerde, siber güvenlik uzmanları şüpheli gördükleri e-postaların yazım denetiminin yapılmasını önermekteydi. Birçok saldırgan, anadili İngilizce olmayan toplumlardan geldiği ve yeterli İngilizce dil becerilerine sahip olmadığı için e-postalarında bariz dil hataları yapabiliyordu. Ancak yapay zekâ kullanımının yaygınlaşmasıyla birlikte saldırganlar, gelişmiş bir içerik yazarı ve yazım denetleyicisinin yardımını alma olanağına kavuştukları için daha inandırıcı e-postalar oluşturabilmektedir.

Sonuç olarak, birçok güvenlik uzmanı, yapay zekâ destekli siber tehditlerin ilerleyen zamanlarda daha tehlikeli bir hâl alabileceğini belirtmektedir. 1700'den fazla siber güvenlik uzmanıyla yapılan bir anketin raporuna göre, en büyük iki endişe artan hacim ve oltalama saldırılarında üretken yapay zekâ araçlarının kullanılmasıyla hassas verilerin sızdırılmasıdır[2],[3].

Nasıl Korunabiliriz?

Sosyal mühendislik saldırılarını tespit etmeye yardımcı olabilecek birkaç ipucu söz konusudur:

- Farkındalık Eğitimi:
  - Çalışanlara sosyal mühendislik teknikleri hakkında düzenli olarak eğitim verilmelidir.
  - Bu eğitimler, potansiyel tehditlerin tanınması ve uygun tepkilerin öğrenilmesi için önemlidir.
- Bilinmeyen kaynaklardan gelen e-posta veya telefon çağrıları dikkatlice değerlendirilmelidir.
- Şüpheli içerikler veya beklenmeyen talepler konusunda dikkatli olunmalı ve sorgulanmalıdır.
- Güçlü Kimlik Doğrulama:
  - İki faktörlü kimlik doğrulama gibi güçlü kimlik doğrulama yöntemleri kullanılmalıdır.
  - Bu, hesapların yetkisiz erişime karşı korunmasına yardımcı olur.
- Bilgi Paylaşımında Dikkat:
  - Kişisel veya hassas bilgilerin paylaşımı öncesinde doğrulama yapılmalıdır.
  - Bilgiyi talep eden kişinin kimliği ve gerekçesi dikkatlice incelenmelidir.
- Güvenlik Yazılımı ve Güncellemeler:
  - Güvenlik yazılımı ve sistemler düzenli olarak güncel tutulmalıdır. Bu, bilgisayar korsanlarının ve kötü amaçlı yazılımların girişini engellemeye yardımcı olur.
- Şirket içinde güvenlik politikaları ve prosedürler belirlenmeli ve uygulanmalıdır.

Bu politikalar, sosyal mühendislik saldırılarına karşı savunmada kritik bir rol oynamaktadır[4].

2. Inception Saldırıları

Sanal Gerçeklikte Yeni Tehdit: Inception Saldırıları

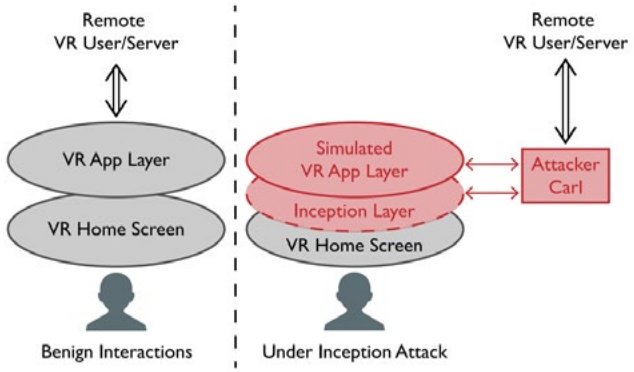
Sanal gerçeklik (VR) teknolojisi son yıllarda büyük bir gelişme göstermiş ve birçok alanda kullanılmaya başlanmıştır. Bu gelişmeyle birlikte, VR sistemlerinin güvenliğinin de artırılması gerekmektedir. Araştırmacılar, VR sistemlerinin "Inception saldırısı" adı verilen yeni bir güvenlik açığına karşı savunmasız olabileceğini keşfettiler[5].

Inception Saldırısı Nedir?

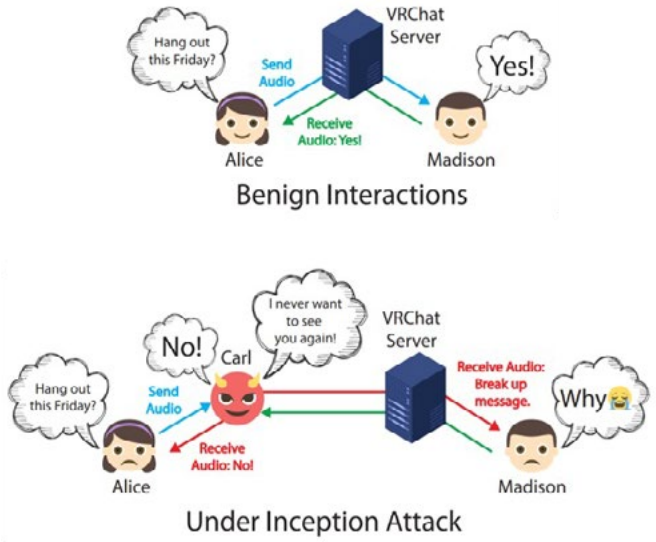
Inception saldırısı, Christopher Nolan'ın "Inception" filminde tasvir edilene benzer şekilde, bir kullanıcının sanal gerçeklik deneyimini onun bilgisi dışında maniple ederek çalışır. Saldırganlar, üretken yapay zekâ araçlarını kullanarak gerçekçi simülasyonlar oluşturup ses ve görselleri gerçek zamanlı olarak değiştirebilir. Bu arada, kullanıcı çevrimiçi etkileşimlerinin kaydedildiğinin veya maniple edildiğinin farkına varamaz.

Inception Saldırıları Nasıl Gerçekleştirilir?

Inception saldırıları, VR sistemlerindeki çeşitli güvenlik açıklarından yararlanarak gerçekleştirilir. Araştırmacılar, Meta Quest Pro'nun "geliştirici mod" ayarını kullanarak saldırı yapabildiklerini buldular. Bu ayar, VR sistemine uzaktan erişim olanağı sağlar ve saldırganlar bu açığı kullanarak kullanıcının sanal ortamını kontrol edebilir. Aynı zamanda Apple Vision Pro gibi dışarıdan uygulama yüklemenin kısıtlı olduğu daha güvenlikli VR sistemlerinde bile kullanıcılar, uygulama mağazalarından güvenli gözüken uygulamalar indirdiklerinde bu tür saldırılarda tuzağa düşebilirler.



Şekil 1: Gerçek VR sistemi kullandığını sanan fakat aslında Inception saldırısı tuzağına düşen bir kullanıcı senaryosu örneği[6].



Şekil 2: VRChat uygulamasının klonuyla yapılabilecek senaryo örneği[6].

Araştırmacılar VR sistemi kullanıcılarının birbirleriyle konuşabildikleri bir uygulama olan VRChat uygulamasının klonunu yaparak bu açığın nasıl kötü amaçla kullanılabileceğini incelediler. Bu klon uygulama sayesinde araştırmacılar, saldırganların kullanıcıların ekranını görüntüleme ve eylemlerini değiştirme gibi saldırılarda bulunabileceklerini tespit ettiler. Eylemleri saldırgan tarafından değiştirilen kullanıcılar, bu klon uygulamada başka kullanıcılarla konuştuklarında iki taraf da tamamen farklı konuşmalar deneyimleyebilmektedir.

Inception Saldırılarının Riskleri

Inception saldırıları, kullanıcıların kişisel bilgileri ve finansal verileri için büyük bir risk oluşturmaktadır. Saldırganlar, bu bilgileri ele geçirmek için sahte banka uygulamaları veya kimlik avı siteleri oluşturabilirler. Ayrıca Inception saldırıları, siber casusluk ve propaganda yaymak için de kullanılabilir.

Inception Saldırılarına Karşı Önlemler

- **Geliştirici Modu Kullanımının Kısıtlanması:** VR sistemlerinde bulunan geliştirici modu gibi potansiyel güvenlik riskleri taşıyan özelliklerin kullanımı, standart kullanıcılar için kısıtlanabilir veya daha güvenli hâle getirilebilir. Bu, saldırganların sisteme erişmesini engellemeye yardımcı olabilir.
- **Güvenlik Yazılımlarının Kullanımı:** VR sistemlerine özgü güvenlik yazılımları veya uygulamaları geliştirmek veya kullanmak, potansiyel saldırıları tespit etmek ve engellemek için etkili bir yol olabilir. Bu tür yazılımlar, sistemlerin güvenliğini artırmak için düzenli olarak güncellenebilir.

- **Yetkilendirme ve Kimlik Doğrulama:** Kullanıcıların sistemlere erişirken güçlü yetkilendirme ve kimlik doğrulama yöntemleri kullanmaları sağlanabilir. İki faktörlü kimlik doğrulama gibi ek güvenlik katmanları, yetkisiz erişimi engelleyebilir.
- **Ağ Güvenliği Çözümleri:** VR sistemlerinin bağlı olduğu ağlarda güvenlik duvarları, kötü amaçlı trafiği engelleyebilir ve saldırıları önleyebilir. Ağ izleme ve güvenlik protokolleri, potansiyel tehditleri tespit etmek ve önlemek için kullanılabilir.
- **Kullanıcı Eğitimi:** Kullanıcıların, sanal gerçeklik deneyimlerinde dikkatli ve potansiyel güvenlik risklerine karşı bilinçli olmaları için eğitilmesi önemlidir. Kullanıcılar, bilinmeyen kaynaklardan gelen uygulamalardan kaçınmayı ve şüpheli etkinlikleri rapor etmeyi öğrenmelidir.
- **Araştırma ve İnceleme:** Güvenlik araştırmacıları ve sistem geliştiriciler, sürekli olarak yeni tehditleri tespit etmek ve bunlara karşı savunma mekanizmaları geliştirmek için çalışmalıdır. Bu, hızla evrilen saldırı tekniklerine karşı daha iyi bir hazırlık sağlayabilir.

Bu önlemler, Inception saldırıları gibi karmaşık güvenlik tehditlerine karşı daha dirençli ve güvenli bir sanal gerçeklik ortamı oluşturabilir. Ancak hiçbir önlem tek başına yeterli olmayabilir. Bu nedenle kapsamlı bir güvenlik stratejisi benimsenmelidir.

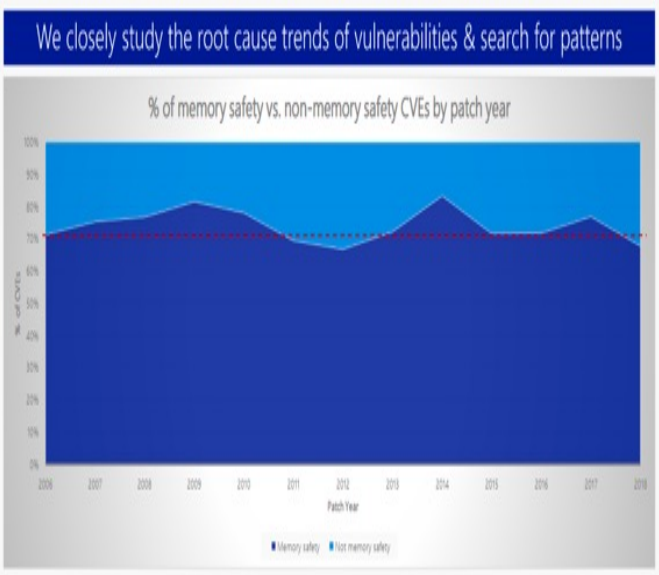
Inception Saldırıları Hakkında Ek Bilgiler

- Inception saldırıları, VR sistemlerinin yanı sıra artırılmış gerçeklik (AR) sistemlerini de etkileyebilir.
- Inception saldırılarının önlenmesi için siber güvenlik eğitimi önemlidir. Kullanıcılar, VR ve AR ortamlarında karşılaşabilecekleri güvenlik riskleri hakkında bilinçlendirilmelidir.
- Inception saldırıları, VR ve AR teknolojilerinin gelişmesiyle daha da karmaşıklaşabilir. Bu nedenle, bu alandaki araştırmaların ve geliştirmelerin devam etmesi önemlidir.

3. C++ ile C'den Rust ile Go'ya: Bellek Güvenliği Odaklı Programlama Dillerine Geçiş

Dijitalleşme ivmesinin artışı, teknolojik yeniliklerin yanı sıra siber güvenlik tehditlerinin de evrim geçirmesine neden olmaktadır. Bu dinamik ortam, hem kurumlar hem de bireyler için siber güvenlik zorluklarını daha da karmaşık hâle getirmekte, yazılım geliştirme süreçlerinde güvenliğin baştan itibaren entegre edilmesinin önemini artırmaktadır.

Bellek güvenliği zafiyetleri, yazılım güvenliğinde sıkça karşılaşılan temel sorunlardan birini oluşturmakta ve saldırganlara sistemleri kötüye kullanma imkânı sunmaktadır.



Şekil 3: Microsoft'un her yıl CVE atadığı güvenlik açıklarının yüzde 70'i bellek güvenliği ilişkisi[7].

Bellek güvenliği zafiyetleri, yazılım güvenlik açıklarının önemli bir kısmını teşkil etmektedir. Bu tür zafiyetler, yalnızca teknik bir mesele olmanın ötesinde, kurumların ve kullanıcıların güvenliğini doğrudan etkileyen kritik bir konu hâline gelmiştir. Bu bağlamda, güvenlik açıklarını minimize etmek ve daha güvenli yazılım ürünleri geliştirmek amacıyla, bellek güvenliği zafiyetlerinin etkili bir şekilde ele alınması büyük önem taşımaktadır[8].

Bellek güvenliği sorunları, yazılım güvenliği açıklarının önemli bir bölümünü oluşturmaktadır. Bu sorunlar, sistemlerin kötü amaçlı saldırılara maruz kalmasına neden olabilir. Bellek güvenliği zafiyetleri, yazılımın beklenmeyen şekillerde davranmasına yol açabilir, bu da bilgi sızıntılarına, yetkisiz erişime veya sistem çökmesine neden olabilir[9].

Bellek güvenliği zafiyetlerine sahip dillerin (C, C++) performans ve kontrol ihtiyacı nedeniyle, özellikle sistem seviyesi ve gömülü sistemlerde hâlâ yaygın olarak kullanılmaktadır.

Örneğin Rust, Go gibi performansı yüksek programlama dilleri bellek güvenliği sorunlarını önlemeye yönelik olarak tasarlanmıştır. Bu diller, bellek güvenliği zafiyetlerini otomatik olarak önleyen özellikler sunar ve böylece yazılımın daha güvenli hâle gelmesini sağlar.

C++ programında bellek güvenliği ihlallerine yol açabilecek yaygın bir hata, bellek sızıntılarına veya tanımsız davranışlara neden olabilecek yanlış bellek yönetimidir. Örneğin, bir bellek bloğunu tahsis edip sonra uygun şekilde serbest bırakmamak. Aşağıda, bellek güvenliğini ihmal eden basit bir C++ kod örneği verilmiştir:

```
#include <iostream>
int main() {
// 10 tamsayı için bellek tahsisi yapılıyor.
 int* sayiDizisi = new int[10];
```

```
 for(int i = 0; i < 10; ++i) {
        sayiDizisi[i] = i * 10;
 }
// delete[]sayiDizisi işlemi ile belleği doğru bir şekilde serbest bırakması gerekliydi
   std::cout << "Bellek sızıntısı oluştu." << std::endl;
}
```

C++ dilinde verilen örnek kod, dinamik olarak tahsis edilen bir bellek bloğunu (int türünden 10 elemanlık bir dizi) serbest bırakmadığı için bellek sızıntısına yol açar. Programın doğru bir şekilde yazılması için, delete[]sayiDizisi; ifadesiyle tahsis edilen belleğin serbest bırakılması gerekmektedir. Bellek yönetimi konusunda dikkatsizlik, özellikle büyük ve karmaşık programlarda ciddi sorunlara yol açabilir. Bu tür hatalar, programın beklenmedik şekillerde davranmasına, performans sorunlarına ve hatta güvenlik açıklarına neden olabilir. Bu yüzden, dinamik bellek yönetimi yapıldığında tahsis edilen her bellek bloğunun uygun bir şekilde serbest bırakılması gerekir.

Rust programlama dili bellek güvenliği ihlallerinin önüne geçilebilmesi için otomatik bellek yönetimi mekanizmaları (ownership, borrowing, lifetimes) ve tür sistemi kullanılabilir. Bu sayede, Rust'ta manuel olarak belleği serbest bırakma ihtiyacı ortadan kalkmakta ve bellek güvenliği ihlalleri büyük ölçüde önlenebilmektedir. C++ kodunun Rust versiyonu aşağıda verilmiştir.

```
fn main() {
    let mut sayiDizisi = Vec::new(); // Vec, Rust'ın sağladığı genel amaçlı bir dizi türüdür.
   for i in 0..10 {
      sayiDizisi.push(i * 10); }
   // Rust'ta bellek otomatik olarak yönetilir, bu nedenle belleği manuel olarak serbest bırakma işlemine gerek yoktur.
   println!("{:?}", sayiDizisi);
}
```

Rust'ın sahip olduğu bellek güvenliği özellikleri sayesinde, Vec'in kapsamı sona erdiğinde (yani main fonksiyonunun sonuna ulaşıldığında), Vec'in içerdiği tüm değerler otomatik olarak temizlenir ve tahsis edilen bellek serbest bırakılır. Bu, Rust'ın bellek güvenliğini nasıl sağladığının basit bir örneğidir.

Rust, bellek sızıntıları, çifte serbest bırakma ve kullanımdan kaldırılmış belleğe erişim gibi yaygın bellek güvenliği sorunlarını önlemek için sahiplik kurallarını uygular. Bu kurallar, derleme zamanında bellek güvenliği ile ilgili hataları tespit etmeyi mümkün kılar, böylece bu tür hatalar çalışma zamanına ulaşmadan önce düzeltilir.

Go dilinde, bellek yönetimi otomatik olarak gerçekleştirilir, çünkü Go'nun garbage collector'ı (çöp toplayıcı) belleği otomatik olarak yönetir ve kullanılmayan nesneleri temizler. Bu yüzden Go'da, Rust gibi modern dillerde bellek güvenliği ile ilgili sorunlar önemli ölçüde çözülmüştür.

Örneklerde verilen benzer kod paraçasının Go programlama dili ile kodlanmış hâli aşağıda sunulmuştur.

```
package main
import "fmt"
func main() {
    var sayiDizisi[]int // int türünden bir slice (dinamik dizi) oluşturuluyor.
   for i := 0; i < 10; i++ {
// Slice'a elemanlar ekleniyor.
      slice = append(slice, i*10)   }
   fmt.Println(slice)   }
```

Sonuç olarak, özellikle hız ve performans gerektiren işlemlerde tercih edilen C ve C++ programlama dillerinin, bellek yönetimindeki esnekliği siber güvenlik zafiyetine neden olabilmektedir. Ülke güvenlik politikalarında artık bu konunun açıkça dile getirilmesi, yakın performansa sahip nispeten yeni olan Go ve Rust gibi programlama dillerinin daha da yaygınlaşabileceğini göstermektedir.

4. LockBit: Küresel Ekonomi ve Güvenliğe Karşı Yükselen Tehdit

Giriş:

2023'ün sonlarında ve 2024'ün başlarında dünya çapında birçok kuruluşu hedef alan LockBit fidye yazılımı saldırıları, siber güvenlik gündeminin en önemli maddelerinden biri hâline gelmiştir. Kritik altyapı tesislerinden sağlık kuruluşlarına, eğitim kurumlarından kamu kuruluşlarına kadar geniş bir yelpazede hasara yol açan bu saldırılar, küresel ekonomi ve güvenlik için ciddi bir tehdit oluşturmaktadır. Bu makalede, LockBit fidye yazılımı ve arkasındaki gruba ilişkin detaylı bir inceleme sunarak, saldırıların kapsamını, etkilerini ve korunma yollarını analiz edeceğiz.

LockBit Nedir?

LockBit, ilk olarak Eylül 2019'da ortaya çıkan bir fidye yazılımı türüdür. Bu yazılım, kurbanların bilgisayarlarındaki dosyaları şifreler ve onları geri yüklemek için fidye talep eder. LockBit, diğer fidye yazılımlarından farklı olarak, "RaaS" (Ransomware as a Service) modelini kullanır. Bu modelde, fidye yazılımının geliştiricileri, yazılımı diğer saldırganlara kiralar ve onlar da bu yazılımı kullanarak saldırılar gerçekleştirir. LockBit'in "ABCD" ve "LockBit 2.0" olarak bilinen iki ana sürümü mevcuttur. Her iki sürüm de gelişmiş şifreleme algoritmaları, veri sızdırma tehdidi ve fidye ödemeyi teşvik eden psikolojik taktikler gibi çeşitli teknikler kullanarak kurbanları hedef alır[10].

LockBit Saldırıları:

LockBit, son zamanlarda birçok yüksek profilli saldırıda kullanıldı. Aralık 2023'te, LockBit ransomware grubu, Portekiz limanlarını hedef aldı ve 1,5 milyon dolar fidye talep etti. Aynı ayda, Toronto'daki SickKids Hastanesi de LockBit saldırısına uğradı ve bu durum hastanenin bilgisayar sistemlerinin bozulmasına ve hastaların tedavisinde gecikmelere neden oldu. 2024'ün Ocak ayında ise LockBit, dünyanın en büyük otomobil üreticilerinden biri olan Honda'ya saldırdı ve üretimde aksamalara yol açtı. Bu örneklerin yanında, LockBit'in eğitim kurumları, kamu kuruluşları ve küçük işletmeler de dahil olmak üzere birçok farklı sektörden kuruluşu hedef aldığı bilinmektedir.

LockBit Saldırılarının Etkileri:

LockBit saldırıları, kuruluşlar üzerinde yıkıcı bir etkiye sahip olabilmektedir. Bu saldırılar aşağıdaki sorunlara neden olabilmektedir[11]:

- **Veri kaybı ve hasarı:** LockBit, kurbanların bilgisayarlarındaki tüm dosyaları şifreleyerek önemli verilerin kaybolmasına veya hasar görmesine neden olabilmektedir. Bu durum, iş süreçlerinin kesintiye uğramasına, müşteri bilgilerinin çalınmasına ve yasal yaptırımlara yol açabilmektedir.
- **Sistem kesintileri ve gecikmeler:** LockBit saldırıları, kuruluşların bilgisayar sistemlerini kullanılamaz hâle getirerek kritik iş süreçlerinin kesintiye uğramasına ve gecikmelere neden olabilmektedir. Bu durum, üretimde aksamalara, finansal kayıplara ve itibar zedelenmesine yol açabilmektedir.
- **Finansal kayıplar:** LockBit saldırıları, kuruluşların fidye ödemesi yapma zorunda kalmasına, veri kurtarma ve sistem onarım maliyetlerinin katlanmasına ve siber saldırı sigortası primlerinin artmasına neden olabilmektedir. Bu durum, özellikle küçük ve orta ölçekli işletmeler için büyük bir mali yük oluşturabilmektedir.
- **İtibar zedelenmesi:** LockBit saldırıları, kuruluşların itibarını zedeleyebilir ve müşterilerin güvenini sarsabilir. Veri sızıntıları ve sistem kesintileri, müşterilerin kişisel bilgilerinin ve finansal verilerinin risk altında olduğunu gösteren bir işaret olarak yorumlanabilir ve bu durum müşteri kayıplarına yol açabilir.

LockBit'in Arkasındaki Grup:

LockBit'in arkasındaki grup hakkında çok az şey bilinmektedir. Grubun Rusya kökenli olduğu ve "LockBit Ransomware Group", "LockBit Ransomware Gang", "LockBit Affiliates" gibi farklı isimlerle anıldığı tahmin edilmektedir. Grubun, fidye ödemelerini Bitcoin ve Monero gibi kripto para birimleri aracılığıyla talep ettiği ve fidye miktarlarını genellikle kurbanın ödeme gücüne göre belirlediği bilinmektedir. LockBit grubu, saldırılarını gerçekleştirmek için çeşitli yollar kullanır.

Bunlar:

- **Kimlik Avı Saldırıları:** LockBit grubu, kurbanları dolandırıcı e-postalar, sahte web siteleri ve sosyal medya mesajları aracılığıyla kandırarak zararlı yazılımları indirmelerine veya kötü niyetli bağlantıları tıklamalarına yol açabilmektedir. Bu sayede kurbanların bilgisayarlarına sızabilmektedir.
- **Güvenlik Açıklarından Faydalanma:** LockBit grubu, güncel olmayan yazılımlardaki güvenlik açıklarından faydalanarak kurbanların sistemlerine sızabilmektedir. Kuruluşların yazılımlarını ve işletim sistemlerini düzenli olarak güncel tutmaları, bu tür saldırıları önlemede önemli bir adımdır.
- **Uzak Masaüstü Erişimi (RDP) Saldırıları:** LockBit grubu, zayıf parolalar veya güvenliksiz yapılandırmalar nedeniyle açıkta kalan Uzak Masaüstü Erişimi (RDP) bağlantılarından faydalanarak kurbanların sistemlerine uzaktan erişim sağlayabilmektedir.

LockBit fidye yazılımı grubu, saldırılarını gerçekleştirdikten sonra genellikle kurbanlara iki seçenek sunar:

- **Fidye Ödeme:** LockBit grubu, şifrelenen dosyaları geri yüklemek için kurbanlardan yüksek miktarlarda fidye talep eder. Fidye miktarları genellikle kuruluşun büyüklüğüne ve sahip olduğu verilere göre değişir.
- **Veri Sızıntısı:** Eğer kurban fidye ödemeyi reddederse, LockBit grubu çalınan verileri kendi sızıntı siteleri veya dark web'de yayınlamakla tehdit eder. Bu durum, kuruluşlar için önemli bir itibar kaybına ve hukuki yaptırımlara yol açabilmektedir.

LockBit'e Karşı Korunma Yolları:

LockBit saldırılarına karşı korunmak için kuruluşlar aşağıdaki adımları atmalıdır[12]:

- **Güvenlik Farkındalığı Eğitimi:** Çalışanların siber güvenlik tehditleri konusunda bilinçlendirilmesi, kimlik avı saldırılarını önlemede ve şüpheli e-postaları veya bağlantıları rapor etme olasılığını artırmada önemlidir.
- **Siber Güvenlik Politikaları ve Prosedürleri:** Kuruluşlar, fidye yazılımı saldırılarına karşı etkili bir şekilde korunmak için kapsamlı siber güvenlik politikaları ve prosedürleri geliştirmelidir. Bu politikalar, güçlü parola kullanımı, çok faktörlü kimlik doğrulama, düzenli güvenlik yamaları, veri yedekleme ve kurtarma planları gibi konuları kapsamalıdır.
- **Güvenlik Duvarları ve Antivirüs Yazılımları:** Güvenlik duvarları ve güncel antivirüs yazılımları, kötü niyetli yazılımların kurbanların bilgisayarlarına sızmasını önlemede önemli bir rol oynar. Bu güvenlik yazılımlarının düzenli olarak güncellenmesi ve etkinleştirilmesi önemlidir.
- **Veri Yedekleme ve Kurtarma:** LockBit saldırılarının etkilerini azaltmak için, kuruluşların düzenli olarak

verilerini yedekleyip bu yedekleri güvenli bir ortamda saklaması gerekir. Bir saldırı gerçekleşmesi durumunda, şifrelenen veriler yedeklerden kurtarılabilir.

- **Siber Saldırı Simülasyonları:** Siber saldırı simülasyonları, kuruluşların güvenlik zafiyetlerini belirlemesine ve olası saldırılara karşı hazırlıklı olmasına yardımcı olur. Bu simülasyonlar, çalışanların siber güvenlik bilincini artırmada da etkilidir.
- **Siber Güvenlik Sigortası:** Fidye yazılımı saldırıları giderek artan bir tehdit haline geldiğinden, siber güvenlik sigortası kuruluşlar için önemli bir risk yönetimi aracı olarak kabul edilmektedir. Sigorta, fidye ödemeleri, veri kurtarma masrafları ve iş kesintilerinden kaynaklanan maliyetleri karşılayabilmektedir.

Uluslararası İşbirliği ve Yasal Mücadele:

LockBit fidye yazılımı grubu gibi suç örgütleriyle mücadele etmek için uluslararası işbirliği ve yasal önlemler büyük önem taşımaktadır. Uluslararası kolluk kuvvetleri ve siber güvenlik uzmanları, fidye yazılımı saldırılarını araştırmak, suçluları yakalayabilmek ve fidye ödemelerini engellemek için işbirliği yapmalıdır.

- **Yaptırım Uygulamaları:** Bazı ülkeler, LockBit grubu gibi fidye yazılımı suç örgütlerine yaptırım uygulayarak kripto para birimi işlemlerini engellemekte ve grubu destekleyen altyapıyı zayıflatmaktadır. Bu yaptırımlar, grubun faaliyetlerini kısıtlayıcı bir etki yaratabilmektedir.
- **Fidye Ödemelerinin Caydırılması:** Hükümetler ve siber güvenlik uzmanları, kuruluşları fidye ödemekten caydırmak için çalışmalar yürütmektedir. Fidye ödenmesinin, fidye yazılımı suç örgütlerini finanse ettiği ve daha fazla saldırıya teşvik ettiği düşünülmektedir. Kuruluşlar, fidye ödemeyi reddetmesi durumunda karşılaşacakları sorunlara rağmen, hukuksal yolları takip ederek ve siber güvenlik uzmanlarından yardım alarak veri kurtarmayı ve sistem onarımını başarılı bir şekilde tamamlayabilmektedir.

LockBit Saldırılarının Geleceği:

LockBit fidye yazılımı grubu, sürekli olarak gelişen bir tehdittir. Grubun yazılımı ve saldırı teknikleri, yeni güvenlik açıklarından faydalanmak ve daha fazla kuruluşu hedef almak için sürekli olarak güncellenmektedir. Bu nedenle, kuruluşların siber güvenlik önlemlerini sürekli olarak güncel tutması ve fidye yazılımı tehditlerine karşı hazırlıklı olması gerekmektedir.

Aşağıdaki noktalar, LockBit saldırılarının geleceğine dair öngörüler sunmaktadır:

- **Hedeflenen Saldırıların Artması:** Fidye yazılımı suç örgütleri, daha yüksek fidyeler talep edebilmek için verileri daha hassas olan kuruluşları hedef almaya yönelebilmektedir. Bu durum, özellikle kritik altyapı tesisleri, sağlık kuruluşları ve finans kurumları için büyük bir risk oluşturmaktadır.
- **RaaS Modelinin Yaygınlaşması:** RaaS modelinin fidye yazılımı pazarında giderek yaygınlaşması beklenmektedir. Bu durum, siber suçların daha genişlemesine ve fidye yazılımı saldırılarının sayısının artmasına neden olabilir.
- **Fidye Ödemelerinin Yasal Düzenlemeleri:** Fidye yazılımı saldırılarının giderek artması nedeniyle, bazı ülkeler fidye ödemelerini yasaklama veya kısıtlama yönünde yasal düzenlemeler getirmeyi gündemlerine alabilir. Bu durum, kuruluşların fidye yazılımı saldırılarına karşı hazırlıklı olmalarının daha da önem kazanmasını getirebilir.

Sonuç:

LockBit fidye yazılımı grubu, küresel ekonomi ve güvenlik için ciddi bir tehdit oluşturmaktadır. Bu gruba karşı mücadelede, kuruluşların siber güvenlik önlemlerini güçlendirmesi, uluslararası işbirliğinin sağlanması ve yasal mücadelenin sürdürülmesi gerekmektedir. Fidye yazılımı tehditleri sürekli olarak gelişmekte olduğundan, siber güvenlik bilincini artırmak ve proaktif savunma stratejileri geliştirmek kuruluşlar için hayati önem taşımaktadır.

5. Dijital Tehditlerin Gölgesinde: Phishing ve İnternet Bankacılığı Dolandırıcılığı

Teknolojinin hızlı gelişimiyle birlikte bankacılık sektörü de dijital dönüşümünü tamamlamak üzere. Ancak, bu ilerleme beraberinde önemli güvenlik risklerini de getiriyor. Özellikle, phishing ve internet bankacılığı dolandırıcılığı gibi yöntemler, bireylerin mali güvenliğini tehdit ediyor.

Phishing, kurbanın yasal bankacılık kurumunu taklit eder ve giriş bilgilerini onaylamasını isteyen bir e-posta gönderir. Normalde, e-postada bankanın gerçek sitesini taklit eden sahte bir web sitesine bağlantı vardır ve giriş bilgileri buraya girildiğinde, saldırganlar tarafından çalınabilir. Bu nedenle bankalar düzenli olarak müşterilerine asla parola veya kişisel kimlik numarası (PIN) gibi hassas bilgiler istenmeyeceğini hatırlatmaktadır. Bu yüzden kimlik avı e-postası genellikle müşterinin tıklayarak bilgilerini onaylamasını talep eder aksi hâlde banka hesabının askıya alınacağını veya kilitleneceğini belirtir[13].

Günlük hayatta phishing ve internet bankacılığı dolandırıcılığı gibi tehditlerden korunmanın bazı temel adımları vardır:

- Bilgilerinizi paylaşmak için gelen şüpheli e-posta veya bağlantılara tıklamaktan kaçının. Her zaman güvenilir kaynaklardan geldiğinden emin olun.
- Bankacılık işlemleri için güvenli ve güvenilir internet bağlantıları kullanın. Açık veya şüpheli ağlardan kaçının ve sadece güvenli web sitelerine erişin.

Şekil 4: Phishing.

- Banka hesaplarınızı ve diğer çevrimiçi hesaplarınızı güçlü ve benzersiz şifrelerle koruyun. Şifrelerinizi düzenli olarak değiştirin ve iki faktörlü kimlik doğrulamayı etkinleştirin.
- Bankanıza herhangi bir şüpheli faaliyeti hemen bildirin. Hesap geçmişinizi düzenli olarak kontrol ederek, şüpheli işlemleri tespit etmeye çalışın.

Günlük hayatta karşılaşılabilecek bu tür tehditlere karşı dikkatli olmak ve gerekli önlemleri almak, mali güvenliğinizi korumanın en önemli adımlarından biridir. İnterneti bilinçli ve dikkatli bir şekilde kullanmak, dolandırıcılık riskini en aza indirmenin anahtarıdır.

6. Milyonlarca Kullanıcının Verileri Sızdırıldı

Ocak 2024'te Twitter, LinkedIn, Dropbox gibi sosyal medya sitelerinde The Mother Of All Breaches olarak isimlendirilen veri sızıntısında yaklaşık 26 milyar kullanıcının verisi sızdırıldı. Etkilenen ülkeler arasında ABD, Brezilya, Almanya, Filipinler ve Türkiye'nin de bulunduğu belirtilmektedir. Araştırmacılar, söz konusu ihlalin son derece tehlikeli olduğunu iddia etmektedir[14].

Şekil 5: Data.

The Mother Of All Breaches terimi, milyonlarca kullanıcının kişisel bilgilerinin sızdırılmasını veya kritik sistemlerin ele geçirilmesini ifade eden ciddi bir güvenlik açığı için kullanılmaktadır. Araştırmacılar, verilerin çoğunun geçmiş veri ihlallerine ait bilgiler içerdiğini ifade etseler de yeni verileri de içerdiği görülmektedir. 100 milyondan fazla kullanıcının verilerinin sızdırılması ile ilgili ilk açıklamayı SecurityDiscovery.com'un sahibi Bob Dyachenko Cybernews'ta yaptı ve açık bir depolama alanında keşfedilmiş olduğunu belirtti[14]. Yaklaşık 12 terabaytlık kullanıcın verisinin sızdırılmış olduğu tahmin edilmektedir. İlk incelemelerde bu sızdırmanın, verilerin yeni bir ihlali olmadığı ama önceki ihlallerin bir araya getirilmesiyle oluştuğu belirtmektedir. En büyük sızıntı Çin'in mesajlaşma uygulaması olan Tencet'in QQ'a üye olan 1,5 milyar kullanıcının verisi olmuştur. Bir diğer veri sızıntısı da Çin'in sosyal medya platformu Weibo'da gerçekleşmişti[14]. MySpace (360M), Twitter (281M), Deezer (258M), Linkedin (251M), AdultFriendFinder (220M), Adobe (153M), Canva (143M), VK (101M), Daily Motion (86M), Dropbox (69M), Telegram (41M) verilerinin de çalındığı görülmektedir.

7. Ukrayna Saldırısı Öncesinde Viasat'a Yapılan Siber Saldırı

24 Şubat 2022'de, Rusya'nın Ukrayna'ya saldırısı sırasında, Amerikan uydu şirketi Viasat, önemli bir siber saldırıya maruz kaldı. Saldırı, Rusya'nın Ukrayna'ya yönelik saldırısının başlamasından sadece bir saat önce gerçekleşti ve Ukrayna askeri güçlerinin, Viasat'ın hizmetlerine dayandırdıkları komuta ve kontrol sistemlerini önemli ölçüde etkiledi. Viasat'ın KA-SAT uydu geniş bant servisine karşı gerçekleştirilen siber saldırıda SATCOM modemleri hedef alınmıştı. SATCOM modemleri, uydu haberleşmesi için kullanılan modüllerdir. Bu modemler, iletişim uydularını röle olarak kullanarak veri aktarımı sağlar. Ana fonksiyonları, giriş veri akışını bir telsiz sinyaline dönüştürmek ve tersine dönüştürmek olan SATCOM modemleri, uydu internet erişimi ve diğer iletişim ihtiyaçları için kullanılır. Bu saldırı, Ukrayna askeri güçlerinin Viasat hizmetlerine dayanan komuta ve kontrol sistemlerini etkiledi.

Saldırıda kullanılan AcidRain adlı "wiper" zararlı yazılımı, Viasat modem ve yönlendiricilerindeki tüm verileri hızla sildi ve cihazların kalıcı olarak devre dışı bırakılmasına neden oldu. Bu durum, binlerce terminalin etkisiz hâle gelmesine yol açtı. Saldırı, aynı zamanda Ukrayna dışında Avrupa'nın orta kesimlerinde bulunan binlerce internet kullanıcısını ve rüzgâr çiftliklerini de etkiledi.

Rusya'nın kullanmış olduğu AcidRain özellikle modem ve yönlendirici cihazlarını hedef alarak bunları işlevsiz hâle getirmek için tasarlanmıştır. Bu zararlı yazılım, modemin ya da yönlendiricinin dosya sistemi üzerinde derinlemesine bir silme işlemi gerçekleştirir. Eğer kod root (yönetici) haklarıyla çalıştırılıyorsa, AcidRain, dosya

sistemindeki standart olmayan dosyaları önce silerek ve ardından üzerine yazarak yok eder. AcidRain, çeşitli depolama aygıtı dosyalarını hedef alır, bu da çeşitli cihaz türlerine zarar verebilir. Örneğin, genel blok aygıtları (/dev/sd*), flash bellekler (/dev/mtdblock*, /dev/mtd* gibi) ve SD/MMC kartları (/dev/mmcblk*), AcidRain'in hedef aldığı bileşenler arasındadır. Bu zararlı yazılım, tüm olası aygıt dosya tanımlayıcılarını deneyerek bu dosya aygıtlarını ya belirli bir veri miktarıyla üzerine yazarak ya da bazı özel komutları kullanarak siler. SentinelOne araştırmacıları, bu zararlı yazılımın 32-bit MIPS ELF ikili olarak geliştirildiğini ve tüm sistem dosyalarını silerek cihazları kullanılamaz hâle getirdiğini belirtmiştir.

İlginç bir şekilde, AcidRain'in kodunda, VPNFilter adlı başka bir zararlı yazılımla bazı benzerlikler tespit edilmiştir. VPNFilter, özellikle SOHO yönlendiricileri ve QNAP depolama aygıtlarını hedef alan, Rus Hükümeti tarafından yürütüldüğü belirtilen bir siber saldırı kampanyasında kullanılan modüler bir zararlı yazılımdır. VPNFilter ve AcidRain arasındaki benzerlikler, her ikisinin de MIPS ELF ikili dosyaları olması ve statik olarak bağlantılı libc'den kaynaklanan kodların büyük bir kısmını paylaşmalarıdır.

Viasat, yapılan siber saldırıya yanıt olarak bir dizi önlem aldı. Şirket, ağ stabilizasyonu ve güvenlik azaltma işlemlerine hemen başladı ve ağı birkaç saat içinde büyük ölçüde stabilize etti. Saldırının amacının hizmet kesintisi yaratmak olduğu ve son kullanıcı verilerine erişilmediği belirlendi. Viasat, saldırıdan etkilenen müşterilere hizmetleri yeniden sağlamak için distribütörlerle işbirliği yaptı ve gerektiğinde modemlerin değiştirilmesini sağladı. Şirket, ayrıca saldırının neden ve sonuçlarını araştırmak için üçüncü taraf olay yanıtı ve adli analiz firması Mandiant ile işbirliği yaptı ve ilgili hükümet kurumlarıyla koordinasyon hâlinde çalıştı.

Rusya'nın bu koordineli ve yıkıcı siber saldırısı, siber saldırıların modern savaşta nasıl aktif ve stratejik bir şekilde kullanıldığını gösteriyor. Saldırının, konvansiyonel savaş operasyonlarıyla eşzamanlı olarak yürütülmesi, siber savaşın modern savaşta giderek artan bir rol oynadığının altını çiziyor.

8. Değişim ve Siber Güvenliğin Geleceği: NIST CSF 2.0'daki Yenilikler ve Değişiklikler Neler?

"Değişmeyen tek şey, değişimin kendisidir" demiş Herakleitos. Ama artık değişim o kadar hızlı ki yeni tartışma konumuz, "Değişimin ivmesi ne şekilde değişiyor?" oluyor. Moore Kanunu der ki; "Her iki yılda bir tümleşik devre üzerine yerleştirilebilecek bileşen sayısı iki katına çıkarken, üretim maliyetleri aynı kalır". Yani kısacası hız iki katına çıkarken siz de aynı maliyetle iki katı hıza ulaşabilirsiniz. Bu muazzam bir değişim demektir. Bu her ne kadar daha sonra Gordon Moore tarafından da sonsuza kadar geçerli olmayacağı kabul edilen bir öngörü olarak kalsa da özellikle her yeni gelişmenin bir diğer gelişmeyi ve öncül olduğu diğer gelişmeleri tetiklediği göz önüne alındığında teknolojinin, doğanın ve küresel ekonominin değişiminin üstel büyüme eğilimi gösterdiği bir gerçek.

Satranç tahtası ve kral kıssası değişimin üstel hızına yönelik bir fikir vermesi açısından ilginç bir örnektir. Kıssaya göre, kralın biri zihnini meşgul edecek bir oyun tasarlanmasını ister. Gelen oyunlardan sadece satranç oyununu beğenir ve oyunun mucidine kendisinden ne hediye istediğini sorar. Mucit sadece kendisini ve ailesini doyuracak kadar buğday istediğini söyler. Bunun için de toplam altmış dört kareden oluşan satranç tahtasının ilk karesine bir, ikinci karesine iki, üçüncü karesine dört, dördüncü karesine sekiz tane buğday tanesi yerleştirilmesini ve bunun böyle hep iki katına çıkarak 64 kare de dolacak şekilde sonuna kadar gitmesini ister. Kral hiç sorgulamadan teklifi kabul eder. Ancak öngöremediği husus değişim miktarının başta az görünürken sonrasında muazzam bir artış göstereceğidir. En sonunda masaya konması gereken buğday tanesi sayısı toplam 18.446.744.073.709.551.615'tir ve bu 2023 yılının toplam dünya buğday üretimi kadardır.

Peki, şu an değişim nerede? Şu an teknolojik, ekolojik ve küresel ekonomi değişimlerinde henüz satranç tahtasının yarısına bile gelmedik ve önümüzdeki süreçte çok daha hızlı bir değişim süreci bizi bekliyor. Peki bu değişimi yakalaması gereken diğer hususlar neler? Birincisi insanların bireysel adaptasyonu, bundan henüz 500 yıl önce bir değişimin başlaması, yayılması ve hayatı değiştirmesi iki, belki de üç nesil sürerken; şu anda bu beş ila yedi yıl arasında gerçekleşiyor. Bu durumda insanın gelişimin biraz gerisinde kalması durumunda psikolojisinde ve topluma adaptasyonunda ciddi sorunlar çıkacağı açıktır.

İkinci ve makalemizin gündemi olan diğer husus ise değişim hızının yasalar, standartlar ve çerçevelerle olan ilgisi. Bu gibi belgelerin sadece hazırlık sürecinin beş yıl sürdüğü düşünüldüğünde değişime ayak uydurulmasının ne kadar güç ya da hayati olduğu ortaya çıkmaktadır. İşte bu noktada en öne çıkan unsurlardan biri de siber güvenliktir. Son zamanlarda hedef olduğu tehditler bu denli artan ve suçluların bu kadar rağbet gösterdiği alan olan Siber Güvenlik konusunda kuruluşlara yardımcı olmayı amaçlayan kurumların mevcut olmasının önemi büyüktür. Bu kurumların en önde geleni National Institute of Standards and Technology'dir (NIST).

İlk olarak 2014 yılında yayınlanan NIST Siber Güvenlik Çerçevesi, kritik altyapı sektöründe siber güvenlik risklerini yönetmek ve azaltmak için kapsamlı bir dizi kılavuz sağlamak üzere geliştirilmiş, ardından 2018 yılında güncellenmiştir. Esneklik göz önünde bulundurularak tasarlanan bu çerçeve, her ne kadar kritik altyapı sektörüyle ilgili olarak oluşturulmuş olsa da çeşitli sektörlerde yaygın bir şekilde benimsenerek siber güvenliğin en iyi uygulamaları için dünya çapında kabul gören bir kıstas hâline gelmiştir.

Şekil 6: NIST CSF 2.0 yol haritası[16].

National Institute of Standards and Technology'nin (NIST) Siber Güvenlik Çerçevesi (CSF), siber savunmayı güçlendirmeyi amaçlayan kuruluşlar için ihtiyaç duyulan kapsamı ve güncelliği sağlamak konusunda ilk yayınlandığı andan günümüze dek her zaman bir mihenk taşı işlevi görmüştür. NIST CSF 2.0'ın yayınlanması siber güvenlik ortamının önemli bir dönüşüme hazırlandığının en önemli göstergelerinden biri olmuştur. Bu makalede NIST CSF 2.0'ın ayrıntılarına inilerek güncellemeler ve bunların hem işletmeler hem de siber güvenlik uzmanları için önemi ortaya konmaya çalışılacaktır[15].

NIST CSF 2.0'daki Yenilikler Neler?

Değişikliklere bakmadan önce değişim sürecinin ne şekilde işlediğini aşağıda doğrudan NIST resmi sayfasından aldığımız Şekil 6'daki zaman çizelgesinden görelim:

Bu çizelge NIST'in değişime yönelik farkındalığına ve muazzam aksiyon hızına ilişkin bir fikir vermektedir. RFI Analizinin 2022 Şubat ayında yayınlanmasından yalnızca 24 ay sonra çalışma tamamlanmış ve CSF 2.0 yayımlanmıştır.

NIST CSF 2.0, sektör profesyonellerinden gelen geribildirimleri, en son siber güvenlik trendlerini ve ortaya çıkan tehditleri bir araya getirerek bir önceki NIST CSF 1.1'in sağlam temelleri üzerine inşa edilmiştir. Güncellenen çerçeve, siber güvenliğe daha dinamik ve kapsamlı bir yaklaşım sağlamayı amaçlayan önemli iyileştirmeler getiriyor. Bu amaçla hedef kitlesini değiştiren CSF güncel versiyonu ile küçük ve orta büyüklükteki işletmeler de dahil olmak üzere tüm sektörlere ve endüstrilere hitap ediyor.

Temel Olarak Yönetişimin Eklenmesi: En büyük değişikliklerden biri de meşhur beş temel fonksiyonun (Identify, Protect, Detect, Respond, Recover) yanına yönetişimin de (Governance) eklenmiş olmasıdır. Bu değişiklik birçok çerçevenin zaman geçtikçe birbirine yakınsayacağını gösteriyor. Yönetişim temel fonksiyonu ile beraber, siber güvenlik risk yönetim stratejisi, buna yönelik beklentiler, politika oluşturma süreci, iletişim ve izleme hususları da göz önünde bulundurulmuştur.

Tedarik Zinciri Güvenliğine Daha Fazla Odaklanma: NIST CSF 2.0, tedarik zincirlerinin artan karmaşıklığını ve oluşturdukları riskleri göz önünde bulundurarak tedarik zinciri güvenliğine daha fazla vurgu yapıyor. Son zamanlarda diğer çerçevelerin de odağında olan bu husus NIST tarafından gözden kaçırılmamış. Güncellenen çerçeve, üçüncü taraf satıcılar ve hizmet sağlayıcılarla ilişkili risklerin değerlendirilmesi ve yönetilmesi konusunda ayrıntılı rehberlik sunarak siber güvenliğe daha bütünsel bir yaklaşım sağlamayı amaçlıyor.

Gizlilik (Privacy) Hususlarının Entegrasyonu: Gizlilikle ilgili kaygıların son zamanlarda özellikle paylaşımlı ortamların artmasıyla beraber siber güvenlik kapsamında kaçınılmaz seviyede öncelikli hâle gelmesiyle birlikte NIST CSF 2.0, gizliliği çerçevenin temel bir bileşeni olarak sunma konusunda güncel eklemeler ve değişiklikler içeriyor. Güncel değişiklikler, küresel gizlilik düzenlemeleri ve standartlarıyla uyumlu olarak, sadece güvenliğin değil aynı zamanda bilginin gizliliğinin de korunmasının önemini vurguluyor.

Genişletilmiş Olay Müdahale ve Kurtarma (Recovery) Kılavuzları: Son dönemde tekdüze saldırılar yerine daha karmaşık siber saldırıların artması sebebiyle NIST CSF 2.0 olaylara müdahale ve kurtarma konularına daha fazla odaklanıyor. Çerçeve, tehditler karşısında esneklik ve çeviklik ihtiyacını vurgulayarak, siber güvenlik olaylarına hazırlanma, müdahale etme ve bunlardan kurtulma konusunda genişletilmiş yönergeler sunuyor.

Bulut ve IoT Güvenliğine Daha Fazla Vurgu: Bulut bilişime geçişin ve IoT cihazlarının yaygınlaşmasının özellikle son yıllarda artmasıyla beraber NIST CSF 2.0, bu teknolojilerin ortaya çıkardığı siber riskleri ele alıyor. Güncellenen çerçeve, bulut ortamlarının güvenliğini sağlama ve IoT ile ilgili riskleri yönetme konusunda rehberlik yapma amacıyla modern dijital ekosistemlerin kapsamlı bir şekilde ele alınmasını sağlıyor.

Özelleştirme (Customization) ve Esneklik (Flexibility): Tek bir çerçevenin herkese uymadığı konusundaki

haklı yaklaşımı ile NIST CSF 2.0, kuruluşların çerçeveyi kendi özel ihtiyaçlarına göre uyarlamaları için daha fazla esneklik sunuyor. Bu özelleştirme, her sektör ve büyüklükteki kuruluşa uzanarak çerçeveyi daha geniş bir kitle için erişilebilir ve uygulanabilir hâle getiriyor.

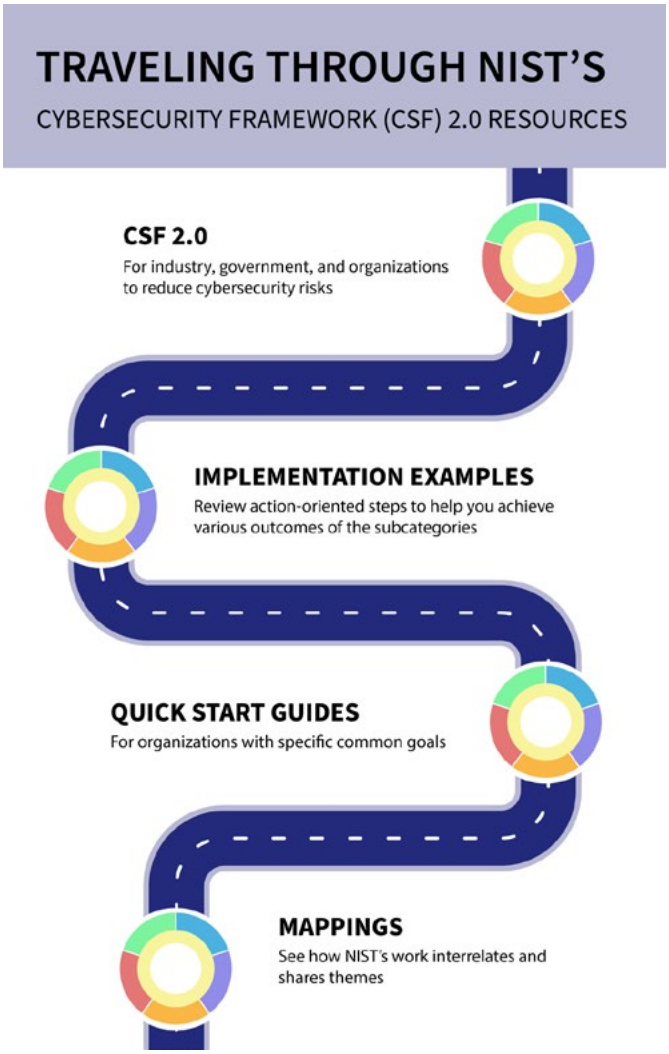
İşletmeler ve Siber Güvenlik Profesyonelleri için Notlar ve Görüşler:

NIST CSF 2.0'ın yayınlanması, siber güvenlik uygulamalarının evriminde çok önemli bir zamana denk geldi. Her türlü işletme tarafından kullanılmak üzere güncellenmiş çerçeve, hızla gelişen tehditlerin damga vurduğu bir ortamda siber güvenlik yaklaşımlarını geliştirmeye yönelik bir yol haritası sunuyor. Önceki versiyonlarından farklı olarak risk yönetimine proaktif bir yaklaşımı teşvik ederek, kuruluşları sadece teknolojik çözümleri değil, aynı zamanda organizasyonel ve insan faktörlerini de kapsayan stratejiler benimsemeye çağırıyor.

Çerçeveyi uygulama amacında olan siber güvenlik uzmanlarına yardımcı olmak amacıyla NIST CSF 2.0, modern siber güvenliğin karmaşıklığını aşmak için çok sayıda yeni kaynak ve kılavuz sunuyor. Gayet kapsamlı ve detaylı hazırlanan Hızlı Başlangıç Kılavuzları (Quick Start Guides), Uygulama Örnekleri (Implementation Examples) ve Eşleme (Mappings) sayesinde uzmanlar; kendileri için en uygun çözümü, sürece nasıl başlayıp nasıl sürdüreceklerini ve uygulayacakları kontrollerin hangi standartlardan/kılavuzlardan alınması gerektiğini görebilecekler. NIST bu çerçeve ile sadece kuruluşlara göre özelleştirilerek uygulanabilecek bir çerçeve sağlamakla kalmıyor aynı zamanda kuruluşlara doğrudan yönlendirici olacak şekilde yol göstermeyi de amaçlıyor. Bunun yanında bulut güvenliği ve gizliliğin korunması gibi kullanım sahası yaygınlaşan alanlarda becerilere duyulan ihtiyacı vurgulayarak sürekli öğrenme ve adaptasyonun öneminin altını çiziyor.

Sonuç:

NIST CSF 2.0, daha güvenli ve siber tehditlere dirençli bir dijital dünyaya doğru devam eden yolculukta önemli bir kilometre taşı oluşturuyor. Siber güvenlikteki en son trendleri ve zorlukları ele alarak, dijital savunmada mükemmelliğe ulaşmak amacıyla yeni bir standart belirliyor. Kuruluşlar ve profesyoneller bu güncellenmiş kılavuzda belirtilen ilkeler etrafında toplandıkça, siber güvenliğin geleceği yalnızca daha güvenli değil, aynı zamanda sürekli değişen dijital ortama daha uyarlanabilir olacak gibi görünüyor. Elbette ki somut etkisi zamanla belirginleşecek ancak görünen o ki NIST değişen dünyanın değişim hızına adapte olma yönünde somut adımlar atmakta kararlı.



Şekil 7: NIST CYBERSECURITY FRAMEWORK (CSF) 2.0 kaynakları[17].

9. Siber Güvenlik Risk Yönetiminde Kullanılan Standartlar

Kamu ve özel sektördeki kuruluşların misyon ve iş fonksiyonlarını başarıyla yerine getirebilmesi bilgi teknolojisi ve bilgi sistemlerine bağlıdır. Bilgi sistemleri, ofis ağlarından, finansal ve personel sistemlerinden özel sistemlere (örneğin, endüstriyel/süreç kontrol sistemleri, silah sistemleri, telekomünikasyon sistemleri ve çevresel kontrol sistemleri) kadar çok çeşitli varlıkları içerebilir. Bilgi sistemleri, işlenen, saklanan veya iletilen bilgilerin gizliliğini, bütünlüğünü veya kullanılabilirliğini tehlikeye sokan güvenlik açıkları yüzünden ciddi tehditlere maruz kalır. Bu tehditlerin tahmin edilebilmesi, olası etkilerinin düşünülmesi ve önlenebilmesi için bilgi güvenliği risk yönetimi büyük önem arz eder.

Risk yönetimi, riski kabul edilebilir bir düzeye indirecek adımları tahmin etme, belirleme ve tanımlama sürecidir.

Bir risk yönetimi süreci uygulanırken çeşitli referanslardan ve standartlardan yararlanılır. Risk yönetim sürecinde kullanılabilecek standartlardan bazıları, ISO 27005, ISO 27001, NIST 800-39, NIST 800-30, NIST 800-53 standartlarıdır. ISO 27005, NIST 800-39 kuruluşlar tarafından bilgi güvenliği risk yönetiminin uygulanmasında yaygın olarak kullanılan risk yönetim standartlarıdır. NIST 800-30 ise risk değerlendirme üzerine odaklanan bir standarttır. ISO 27001 ve NIST 800-53 standartları risk işleme (riske cevap verme) aşamalarında kullanılabilecek referans standartlardır.

Risk Yönetimi

NIST 800-39 metodolojisine göre risk yönetimi bir risk çerçevesinin (framework) oluşturulması, riskin değerlendirilmesi (risk assessment), riske cevap verilmesi ve riskin takip edilmesinden oluşur[18].

ISO 27005; kapsam belirleme (context establishment), risk belirleme (risk identification), risk analizi (risk assessment), risk değerlendirme (risk evaluation), riskin işlenmesi (risk treatment), iletişim/danışmanlık (communication and consultion) ve bilgi güvenliği riskinin izlenmesi ve gözden geçirilmesini (monitoring and review) içeren adım adım bir süreçten oluşur[19].

Kapsam Belirleme

NIST 800-30 ve ISO 27005 standartları risk yönetim sürecine risk kapsamının belirlenmesi aşamasıyla başlar. Kapsam oluşturma, bilgi güvenliği yönetimi için temel kriterlerin oluşturulmasıdır. Kapsam belirleme aşamasında riske dayalı kararların alındığı ortam tanımlanır ve riske dayalı kararların sınırları çizilir.

27005'e göre kapsam oluşturma sürecinde aşağıdaki hususlar göz önüne alınmalıdır[19].

- Organizasyonel hususlar
- İlgili tarafların temel gereksinimleri
- Risk değerlendirme kapsamı
- Bilgi güvenliği risk kriterleri
  - Risk kabul kriterleri
  - Risk değerlendirme kriterleri
    - Etki kriterleri
    - Olasılık kriterleri
    - Risk düzeyini belirleme kriterleri

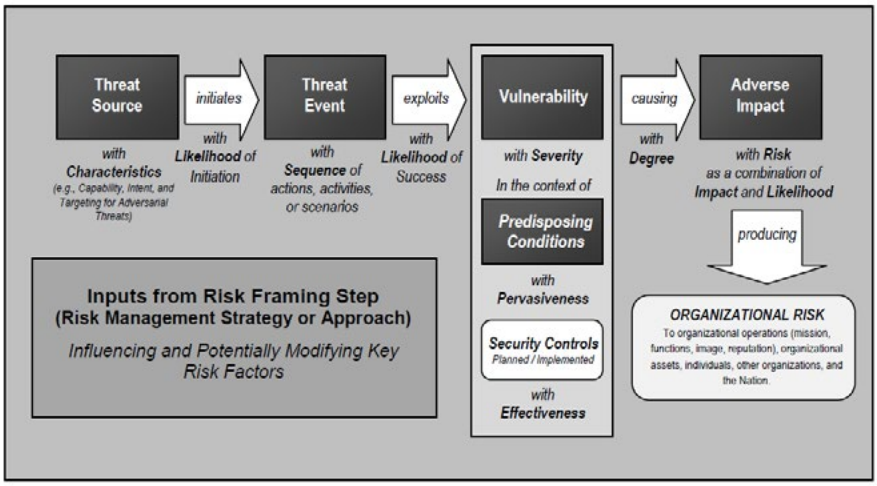
Risk Değerlendirme

Risk yönetiminin ikinci bileşeni, kuruluşların risk çerçevesi kapsamında riski nasıl değerlendirdiğini ele alır. ISO 27005'e göre bilgi güvenliği risk değerlendirmesi, riskin niteliksel olarak ölçülmesi ve belirlenmesinin bir aşamasıdır. Risk değerlendirme sürecinde belirleme, analiz ve değerlendirmeyi içeren çeşitli faaliyetler vardır. Risk belirleme; tehditlerin, mevcut kontrollerin ve güvenlik açıklarının tanımlanmasından oluşur. Risk analizi aşamasında risk, üretilen risk düzeyine göre sıralanacak ve önceliklendirilecek bir ölçeğe göre değerlendirilir. Riskin seviyesinin belirlenmesi ve önceliklendirilmesi risk değerlendirme aşamasında gerçekleştirilir.

NIST 800-30'a göre risk değerlendirme; riskleri tanımlamak, tahmin etmek ve önceliklendirmek için kullanılır. Risk değerlendirme sürecinde kuruluşlara yönelik tehditler; kuruluşların iç ve dış güvenlik açıkları; güvenlik açıklarından yararlanabilecek tehdit potansiyeli göz önüne alındığında kuruluşlara gelebilecek etki ve zararın meydana gelme olasılığı belirlenir. Nihai sonuç, riskin belirlenmesidir. Risk, zararın etkisinin ve zararın meydana gelme olasılığının bir fonksiyonu olarak belirlenir[20].

	ISO 27005	NIST 800-30	NIST 800-39	NIST 800-53 ISO 27001
1	Kapsam Belirleme			
2	Risk Belirleme (Risk Identification)	Tehdit Kaynak Belirleme Tehdit Olayı Belirleme Güvenlik Açıklığı Belirleme		
3	Risk Analizi (Risk Assessment)	Olasılığın Belirlenmesi Etkinin Belirlenmesi		
4	Risk Değerlendirme (Risk Evaluation)	Risk Seviyesinin Belirlenmesi		
5	Risk İşleme		Riske Yanıt Verme	
6				Kontroller

Tablo 1: Standartların karşılaştırılması.



Şekil 8: NIST 800-30 risk değerlendirme süreç akışı.

ISO 27005 ve NIST 800-39 risk yönetimi çerçevesini tanımlarken, NIST SP 800-30 risk değerlendirme sürecinin tamamlayıcısı olarak kullanılabilir.

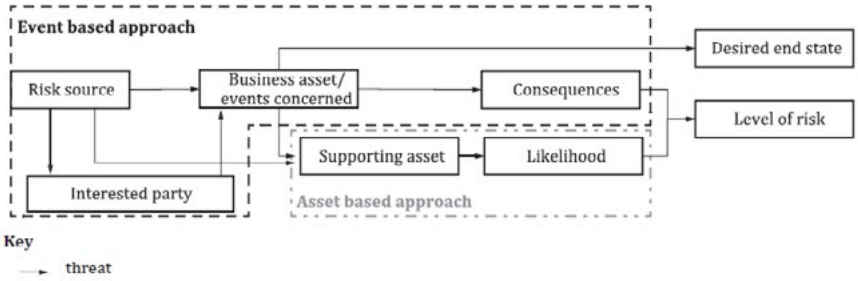
Risk değerlendirme süreci risk belirleme ile başlar. ISO 27005'e göre risk belirleme süreci varlığa veya olaya dayalı olarak yapılabilir[19].

Olaya dayalı yaklaşım: Risk kaynaklarını ve bu risklerin istenen hedefe ulaşmak için ilgili tarafları nasıl kullandıklarını veya etkilediklerini dikkate alarak stratejik senaryoları belirler.

Varlık bazlı yaklaşım: Varlıklar, tehditler ve güvenlik açıkları açısından ayrıntılı operasyonel senaryoları belirler.

NIST 800-30 ise tehdit kaynağı, tehdit senaryosu ve varlıkların açıklıklarının belirlenmesini içerecek şekilde bir risk belirleme sürecini tarif eder. NIST 800-30'un eklerinde bulunan tarifler (NIST 800-30 Table D-3, Table D-4, Table D-5) kullanılarak tehdidin yeteneği, niyeti ve hedefi belirtilecek şekilde tehdit kaynağının karakteristiği belirlenir[20].

ISO 27005'e göre riskler belirlendikten sonra her risk için bir risk sahibi (risk owner) atanmalıdır.



Şekil 9: ISO 27005 risk değerlendirme süreci.

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

Şekil 10: NIST 800-30 risk değerlendirme süreci.

Risk değerlendirme sürecinin 2. Aşaması olan risk analiz süreci riskin olasılığının ve potansiyel sonuçlarının değerlendirilmesini içerir. Siber güvenlik risk analizi, varlıkların zayıf noktalarını değerlendirebilmek için ilgili tehdit senaryolarını göz önünde bulundurarak potansiyel riskleri belirlemeyi amaçlar. NIST 800-30 da ISO 27005 de riskin etkisi ve olasılığını belirlemek üzere tanım tabloları oluşturmuştur ve bu tanım tablolarına göre riskin etki ve olasılığı belirlenir.

Risk değerlendirme sürecinin 3. Aşaması olan risk değerlendirme sürecinde, NIST 800-30 ve ISO 27005'in oluşturduğu tablolar ve çaprazlama yöntemler ile kalitatif ve kantitatif sonuçlar elde edilebilmektedir. Bu şekilde risk seviyesi belirlenir. NIST 800-30'a göre genel olasılık, riskin oluşma olasılığı ve etkinin çaprazlanmasıyla bulunur. Genel olasılığın etki ile çaprazlanması genel risk seviyesini verir. ISO 27005 tek aşamada riskin etki ve olasılığının çaprazlanması ile risk seviyesini belirler. Risk seviyesi belirlendikten sonra bilgi güvenliği riskleri değerlendirilir, risk analizi sonuçları ile risk kriterleri karşılaştırılır ve risk işleme süreci için analiz edilen risklerin önceliklendirilmesi yapılır.

Risk İşleme

Risk yönetiminin üçüncü bileşeni, risk değerlendirmesinin sonuçlarına göre risk belirlendikten sonra kuruluşların riske nasıl tepki vereceğini ele alır. Riske yanıt vermek için risk toleransıyla tutarlı uygun eylem planları belirlenir ve seçilen eylem planlarına dayalı olarak gerekli kontroller uygulanır.

NIST 800-39'a göre kuruluşlar risklere çeşitli şekillerde yanıt verebilir. Kurum; riski kabul edebilir, riskten kaçınabilir, riski azaltabilir, riski paylaşabilir veya riski transfer edebilir.

ISO 27005 risk işleme sürecinde aşağıda belirtilen yöntemleri kullanır:

- Riski doğuran faaliyete başlamama veya devam etmeme kararı alarak riskten kaçınmak,
- Risk kaynağının ortadan kaldırılması,
- Olasılığın değiştirilmesi,
- Etkinin değiştirilmesi,
- Riski başka bir taraf veya taraflarla paylaşmak[19].

Risk işleme sürecinde uygun yöntemler belirlendikten sonra bilgi güvenliği risk işleme seçeneklerinin uygulanması için gerekli tüm kontroller belirlenir. Kontrol setlerinin birçok kaynağı vardır. Bunlar ISO/IEC 27001:2022 (Ek A)'da, NIST 800-53'te, sektöre özgü uygulama kurallarında ve diğer ulusal, bölgesel, endüstriyel kontrol setlerinde bulunabilir.

Ayrıca, ISO 27005'e göre kontroller önleyici, tespit edici ve düzeltici olarak sınıflandırılabilir:

- **Önleyici kontrol:** Bir veya daha fazla sonucun ortaya çıkmasına yol açabilecek bir bilgi güvenliği olayının meydana gelmesini engellemeyi amaçlayan kontrol,
- **Tespit edici kontrol:** Bir bilgi güvenliği olayının meydana geldiğini tespit etmeyi amaçlayan kontrol;
- **Düzeltici kontrol:** Bir bilgi güvenliği olayının sonuçlarını sınırlamayı amaçlayan bir kontrol[19].

Sonuç:

Risk yönetim süreci, risklerin takip edilmesini ve güncellenmesini içeren sürekli devam eden bir süreçtir. Bu yazıda NIST ve ISO standartları referans alınarak risk değerlendirme ve risk işleme süreçleri üzerinde durulmuştur. NIST ve ISO standartları arasında oluşan bazı ufak farklılıklar ve standartların birbirlerini destekleyebileceği yönler belirtilmiştir. Risk yönetimi çok geniş ve önemli bir konu olup, farklı kuruluşlar tarafından oluşturulmuş daha pek çok standart bulunmaktadır.

DÖNEM KONUSU

10. Açık Kaynak Kod Güvenliği: Risklerin Azaltılması ve Güvenli Yazılım Kullanımı

Açık kaynak kodlu yazılımlar, yazılım geliştirmeyi kolaylaştıran ve hızlandıran araçlar ve kütüphanelerden oluşur. Amaçları; geliştiricilere özgürlük, şeffaflık ve işbirliği imkânı sunarak, daha iyi ve daha güvenli yazılımlar geliştirilmesine katkıda bulunmaktır. Fakat bu özgürlük beraberinde bazı güvenlik riskleri de getirir. Açık kaynak kodlu yazılımların güvenliğini sağlamak hem kullanıcıların hem de geliştiricilerin sorumluluğundadır. Açık kaynak kod kullanımı ile farklı riskler doğabilmektedir.

Yazılım Zafiyetleri: Açık kaynak kodlu yazılımlar, hatalı kodlama, güvenli olmayan kodlama pratikleri ve güncelleme eksikliği gibi nedenlerden zafiyetlere maruz kalabilir. Bu zafiyetler, siber saldırganlar tarafından kimlik bilgilerinin çalınması, fidye yazılımı saldırıları veya uzaktan erişim saldırıları gibi çeşitli amaçlar için kullanılabilir. Synopsys tarafından yayınlanan "2023 Open Source Security and Risk Analysis"[21] raporunda incelenen 1.700'den fazla uygulamanın neredeyse hepsinde (yüzde 96) bir tür açık kaynak yazılım bileşeni bulunduğu vurgulanmıştır. Ortalama kod kütüphanesinin yüzde 76'sının açık kaynak koddan oluştuğu tespit edilmiştir. En az bir zafiyet içeren kod kütüphane sayısının son üç yılda neredeyse sabit kaldığı, 2022'de yüzde 84 olduğu gözlemlenirken, yüksek riskli zafiyetler içeren uygulama sayısının tüm test edilen uygulamaların yaklaşık yarısına (yüzde 48) denk geldiği gözlemlenmiştir. Bu oran, 2020'de yaklaşık yüzde 60 seviyesindeydi.

Tedarik Zinciri Saldırıları: Açık kaynak kodlu kütüphaneler ve bileşenler, birçok farklı yazılımda kullanıldığından,

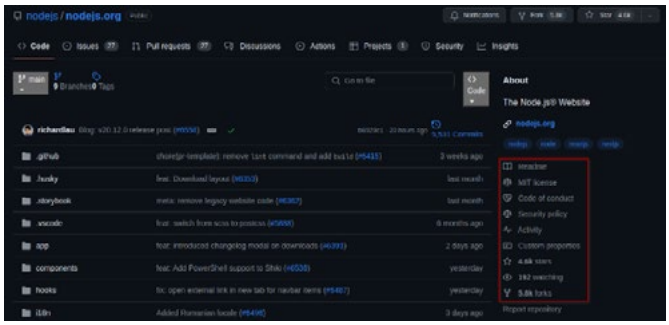
tedarik zinciri saldırılarına karşı savunmasız kalabilmektedir. Saldırganlar, popüler bir kütüphaneye sızarak çok sayıda yazılıma etki edebilmektedir. Bu durum, SolarWinds saldırısında[22] olduğu gibi büyük çaplı güvenlik ihlallerine yol açabilmektedir. SolarWinds, neredeyse 18.000 müşterisini tehlikeye atan bir yazılım güncellemesi aldığını tahmin etmektedir. Tehdit aktörleri bunların içinden seçtikleri yüksek öneme sahip bir alt kümeyi hedef almıştır.

Yazılım Güncelleme Yönetimi: Açık kaynak kütüphaneler sürekli olarak güncellenmekte ve geliştirilmektedir. Ancak, uygulama geliştiricileri tarafından bu güncellemelerin takip edilmemesi veya uygulanmaması, güvenlik açıklarına neden olmaktadır. Veracode'un raporu[23], uygulama güvenliği için en büyük sorunun güncelleme eksikliği olduğunu vurgulamaktadır. Raporda, yayınlanmış bir kanıtı olan zafiyetlerin yüzde 90'ından fazlası için düzeltmeler bulunduğu belirtilmektedir. Bu tür sorunların düzeltilmesi kritiktir, çünkü saldırganlar sistem ve uygulamalara saldırmak için düzenli olarak eski zafiyetleri kullanmaktadır.

Şekil 11: Açık kaynak kod güvenliği.

Açık kaynak kod kullanımından doğabilecek riskleri en aza indirgemek için aşağıdaki yöntemler önerilmektedir.

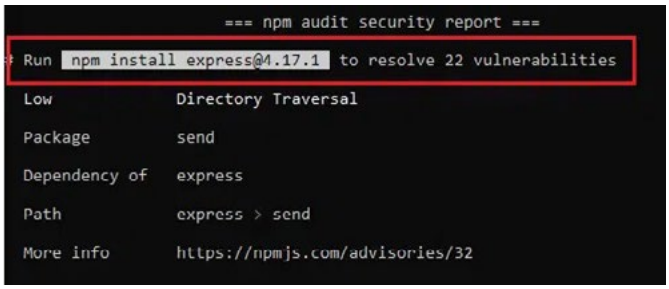
Güvenilir Kütüphanelerin Kullanılması: Kütüphaneleri indirmeden önce kaynağın güvenilir olduğundan emin olunmalıdır. Popüler ve güvenilir kaynaklar tercih edilmelidir. GitHub veya SourceForge gibi platformlar, açık kaynak kodlu yazılımlar için güvenilir kaynaklara örnek olarak gösterilebilir. Örneğin GitHub, üzerinde bulunan milyonlarca açık kaynak projeyi güvence altına almak için özellik ve hizmetler ve güvenlik girişimleri sunar[24].



Şekil 12: GitHub üzerinde popüler bir proje örneği.

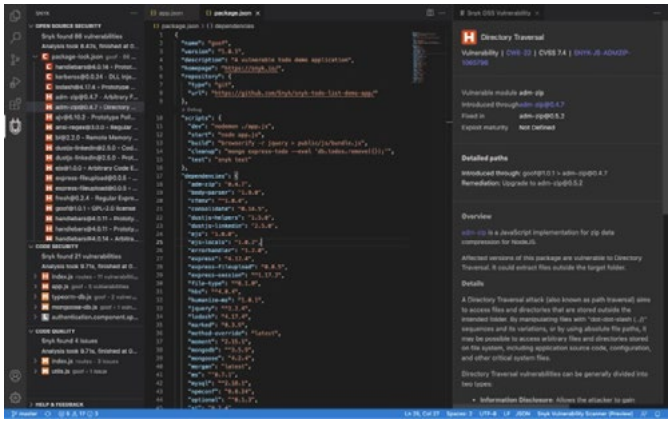
Kullanılan Kütüphanelerin Güncel Tutulması: Kullanılan kütüphanelerin en son sürümünün kullanıldığından ve güncellemelerin takip edildiğinden emin olmak gerekir. Güncellemeler genellikle güvenlik açıklarını gidermek için yayınlanmaktadır. Açık kaynak kütüphanelerin bir özelliği olan ve bir kütüphanenin diğer kütüphanelerden kod çekmesi olarak bilinen transitif bağımlılıklar, bir uygulamanın geliştirici tarafından bilinmeyen kodlara dayanmasına neden olabilir, çünkü geliştirici bu kütüphaneyi açıkça kullanmıyor olabilir. JavaScript, PHP ve Ruby ile yazılmış uygulamaların yüzde 80'den fazlası, bu tür transitif bağımlılıklar aracılığıyla kütüphanelerinin üçte ikisinden fazlasını içe aktarmaktadır. Diğer taraftan, Microsoft'un NET ve Apple'ın Swift ile yazılmış uygulamalarının transitif bağımlılıklara sahip olma oranı yüzde 10'dan azdır. Go, Java ve Python uygulamaları ise daha dengeli bir yol izlemektedir[25].

Zafiyetlerin Kontrol Edilmesi: Açık kaynak bir kütüphane ya da yazılım kullanmadan önce zafiyet taraması yapmak ve bilinen zafiyetlerin düzeltilmiş olduğundan emin olmak gerekir. Çeşitli online araçlar ve servisler, bu konuda hizmet vermektedir. Bazı yazılım dillerinin paket yönetim araçları bilinen zafiyetli paketleri tespit etme ve yükleme sırasında kullanıcıyı uyarma kabiliyetine sahiptir.



Şekil 13: npm audit çıktısı.

Software Composition Analysis (SCA) araçları, yazılımlarda kullanılan açık kaynak bileşenlerin yönetilmesi için bir uygulama güvenliği metodolojisidir. SCA araçları, yazılımın tüm açık kaynak bileşenlerini otomatik olarak tarayabilir ve politika ve lisans uyumluluğunu, güvenlik risklerini ve sürüm güncellemelerini kontrol edebilir. Bu sayede, yazılım lisansları, güncellenmeyen kütüphaneler, zafiyetler ve potansiyel saldırılar tespit edilebilir. SCA araçları, geliştirme ekiplerinin oluşturduğu yazılımlara entegre edilerek açık kaynak bileşenlere ve kütüphanelere görünürlük sağlar.



Şekil 14: VSCode üzerinde çalışabilen örnek bir SCA aracı[26].

Kod İncelemesi Yapılması: Mümkünse, yazılımın kodunun incelenmesi ve güvenlik açıkları veya hatalı kodlama pratikleri olup olmadığının kontrol edilmesi gerekir. Bu, yazılımın güvenilirliğini ve sağlamlığını değerlendirmek için önemli bir adımdır. Static Application Security Testing (SAST) araçları, kaynak kodu analizi araçları olarak da bilinen, yazılım geliştirme sırasında kaynak kodun veya derlenmiş kodun güvenlik açıklarını tespit etmeye yardımcı olan araçlardır. SAST araçları, uygulamayı temellerinden analiz ederek çalışırlar ve uygulamayı çalıştırmaya gerek olmadan kodu detaylı olarak inceleyebilirler. Geliştirme ekiplerinin çözmesi için zafiyet bilgileri ve iyileştirme önerileri sağlarlar. SAST araçları, geliştiricilere kod yazarken gerçek zamanlı geribildirim sağlayarak, kodu SDLC'nin bir sonraki aşamasına geçirmeden önce sorunları çözmelerine yardımcı olur.

11. IoT Cihazların Siber Güvenlik Regülasyonları

Günümüzde, saniyede tahmini olarak 127 yeni cihaz internete bağlanmakta, sağlanan bilgi akışıyla hayatımızı kolaylaştırmaktadır. 2030 yılına kadar yüzde 12,7'lik bir Bileşik Büyüme Oranıyla 500 milyar cihazın internete bağlanması bekleniyor[27]. IoT cihazlarının bu bağlantı potansiyeli, siber tehditler için geniş bir saldırı yüzeyi oluşturmaktadır. IoT güvenliği de regülasyon odağıyla ele alınması gereken kritik bir konu hâline gelmiştir.

İnternetin günlük hayata daha fazla entegre olmasıyla, Web bağlantılı buzdolabı, fırın, akıllı saat ve Web kamera gibi çok sayıda cihaz gündelik hayatımıza girmiştir. Ancak bu cihazların şifrelerinin değiştirilememesi, çoğunda siber saldırılara karşı güncellenebilecek şekilde bir savunma programının bulunmaması güvenlik açıkları oluşturarak cihazların uzaktan kumanda edilebilmesine olanak vermektedir.

Avrupa Birliğinin (AB) yürütme organı olan Avrupa Komisyonu, yetersiz siber güvenlik içerikleri ve uygulamaları ile ürün sunan elektronik üreticilerine yönelik bir siber-direnç yasası sunmaya hazırlanmaktadır. Önerilen kapsamlı yasa, Avrupa Birliğinde satılan "dijital özellikli" tüm ürünler ile herhangi bir ağa bağlı donanım ve yazılımları kapsamaktadır. Yasa kapsamında üreticilere yönelik siber güvenlik derecelendirmesi ve cezalar gündeme gelebilecektir ve Avrupalı elektronik üreticileri, bir güvenlik ihlalinden haberdar olduklarında ilk 24 saat içinde Avrupa Siber Güvenlik İdaresi ENISA'yı (European Network and Information Security Agency) bilgilendirmek zorunda kalacaktır[28].

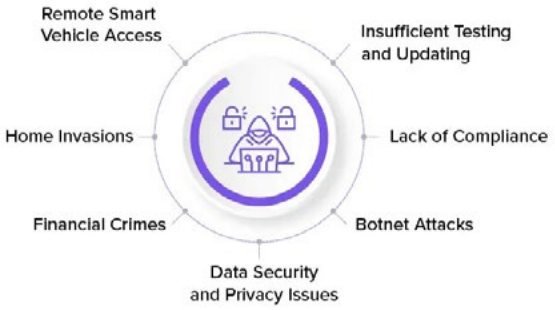
Cyber Resilience Act (CRA) ise AB yasasındaki eksiklikleri gidermeye çalışacağı gibi mevcut Ağ ve Bilgi Sistemlerini (NIS Direktifi) tamamlamak için sunulacaktır. AB, farklı cihazları siber unsurların doğurabileceği olumsuz sonuçlar kapsamında Class I veya Class II olarak sınıflandıracaktır. Class I, belli bir aralıkta yer alan güvenlik donanımı ve yazılımlarını içerirken, Class II, işletim sistemlerini, işlemcileri, router'lara, akıllı kartları, IoT cihazlarını, robotik alıcıları, sanayi otomasyon ve kontrol sistemlerini içerecektir. Avrupa'ya elektronik ürün ithalatı yapan üreticiler de ürünlerinin CRA ile uyumlu olduğundan, CE etiketi taşıdığından ve üzerlerinde iletişim bilgileri bulundurduğundan emin olmak zorunda kalacaklardır[29].

Şekil 15: IoT cihaz örnekleri[30].

Beyaz eşya ve elektrikli ev aletleri sektöründe Avrupa'da ve dünyada başı çeken en büyük üreticilerden biri olan ülkemizde de Sanayi ve Teknoloji Bakanlığı tarafından, önümüzdeki dönemde akıllı ev aletlerinde siber güvenlik standartlarının belirlenmesi ve uygulanması için çalışmalar başlatılacağı bilgisi verilmiştir[31].

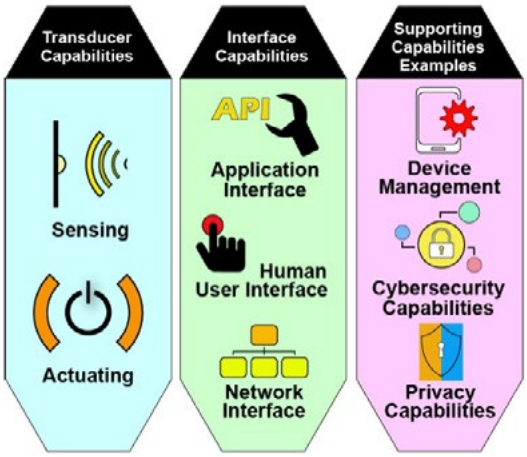
Zafiyetler

- SonicWall Siber Tehdit Raporu'nun 2023 yıl ortası güncellemesine göre, 2023'ün ilk altı ayında, küresel olarak IoT kötü amaçlı yazılım saldırıları yüzde 37 artmış ve toplamda 77,9 milyon saldırı gerçekleşmiştir. Bu, 2022'nin ilk altı ayındaki 57 milyon saldırıya kıyasla bir artışı temsil etmektedir[32].



Şekil 16: IoT güvenlik zafiyetleri ve zorlukları[33].

- Asansör, kartlı kapı, yangın sensor sistemleri gibi cihazların yönetilmesini sağlayan yazılımlara ulaşarak kullanıcıların güvenliklerini ihlal edecek durumlar yaratılabilmekte ve eski hâline döndürmek için fidye talebinde bulunulmaktadır. Akıllı kilitlerle eve/şirkete erişime imkân veren otomasyon kuralları değiştirilebilmekte, böylece sensörler, onları ya evde yaşayan biri gibi algılamakta ya da kapıları kilitlememektedir. Alarmlar kolaylıkla devre dışı bırakılabilmektedir. Ayrıca internete bağlı hoparlörler vasıtasıyla sanal asistanlara komutlar verilebilmekte, ev sahibinin sesi analiz edilip klonlanarak, karmaşık IoT ortamlarına bağlı cihazların ses tanıma prosedürü atlatılabilmektedir[34].



Şekil 17: IoT cihazların siber güvenliğe etkileri[35].

- 2016'da Mirai botnet saldırısı, güvenli olmayan IoT cihazlarını ele geçirerek büyük ölçekli dağıtık DoS saldırıları başlatmak için kullanılmıştır. Mirai'nin çeşitli varyantları günümüzde de aktiftir[34].

Regülasyonlar

Avrupa, İngiltere ve ABD'deki regülasyonların son durumuna bakacak olursak; ABD'de, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), IoT siber güvenliği konusunda hem üreticilere kılavuz olabilecek hem de son kullanıcılar için gereksinimleri ifade edecek pek çok rehber doküman yayınlamıştır. Örneğin; NIST IR 8259A[36], NIST IR 8228[37] , NIST CSWP 24[38], NIST IR 8425[39]. İngiltere Hükümeti, tüketici IoT güvenliği için bir Uygulama Kılavuzu tanıtmıştır. Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI), bir dizi önerinin bulunduğu EN 303645[40] standardını yayınlamıştır ve bu standart giderek dünya genelinde benimsenmektedir.

İngiltere'de ilk tüketici bağlantılı ürün güvenlik düzenlemesi olan Product Security and Telecommunications Infrastructure (PSTI) Yasası, 29 Nisan 2024 tarihinde yürürlüğe girecektir. Bu yasaya göre, IoT cihaz üreticilerinin, dağıtıcılarının ve ithalatçılarının, ürünlerin varsayılan şifrelerini kullanmasına artık izin verilmeyecek, güvenlik güncellemelerinin ne kadar süreyle sağlanacağının onaylanması gerekecek ve ürünlerin bir zayıflık açıklama politikasına sahip olması zorunlu olacaktır.

Cyber Resilience Act (CRA), IoT ürünlerinin planlanması, tasarlanması, geliştirilmesi ve bakımını düzenleyen bir çerçeve sağlamakta ve değer zincirinin her aşamasında karşılanması gereken yükümlülükleri belirlemektedir. EN 303645 de dahil olmak üzere bir dizi standardı kapsayacağı düşünülmektedir. "CE" işaretinin, ürünlerin yeni siber güvenlik standartlarına uygun olduğunu teyit edecek şekilde genişletildiğini göreceğiz. Ürünlerin, ürünle ilişkilendirilen risk seviyesine bağlı olarak kategorize edilmesi ve bu kategorilerle ilişkilendirilen farklılaştırılmış güvenlik değerlendirmelerinin (Sertifikasyon) görülmesi de muhtemeldir.

C.R.A'nın yanı sıra, AB ayrıca, 2025'ten itibaren AB piyasasında satılacak tüm telsizli cihazların siber güvenlik gereksinimlerine uyumlu olmasını gerektiren bir düzenleme olan Radio Equipment Directive (RED) için bir revizyon geliştirmiştir.

ABD Hükümeti 2023 yılında, tüketici IoT ürünlerine yönelik güvenlik garantisini, önerilen yapılandırmayı ve tüketici IoT ürünlerinin uzun vadeli güvenlik bakımını sağlayacak bir "Tüketici IoT Ürün Etiketleme Programı" planladığını duyurdu. "US Cyber Trust Mark" olarak adlandırılan bu etiketleme Amerikalıların, daha güvenli ve siber saldırılara daha az zafiyetli olan akıllı cihazları daha kolay seçmelerine rehberlik edecektir. Bu etikete sahip ürünlerin, NIST IR 8425 standardının önceden belirlenmiş gereksinimlerini karşıladığını, siber güvenlik testlerinin yapıldığını ve ABD hükümeti standartlarıyla uyumlu olduğunu gösterecektir.

Ek olarak; IEC 62443 serisi standartlar, genel amaçlı IT sistemlerinin güvenliği için oluşturulmuş standartları temel alarak, Endüstriyel Otomasyon ve Kontrol Sistemleri (IACS) için güvenlik standartlarını belirlemektedir. Bu seride, 62443-4-3 standardı, IIoT (Industrial Internet of Things) için teknik güvenlik standartlarını belirler. IIoT'nin, buluta dayalı işlevselliğinin IACS'a entegre etmeyi içeren bir bileşen olarak kabul edilmesini sağlar. Ayrıca, bir ağ tasarımı yaklaşımı olan Zero Trust mimarisinden bahseder.

Şekil 18: IoT Ömür Döngüsünde Risk Analizi Yaklaşımı[36].

Üreticilerin dikkate alması gereken diğer ilgili standartlar ve rehberler arasında

- IoT Security Foundation (IoTSF) "Secure Design Best Practice Guides"[41],
- National Electrical Manufacturers Association (NEMA), "Cyber Hygiene Best Practices" sayılabilir.

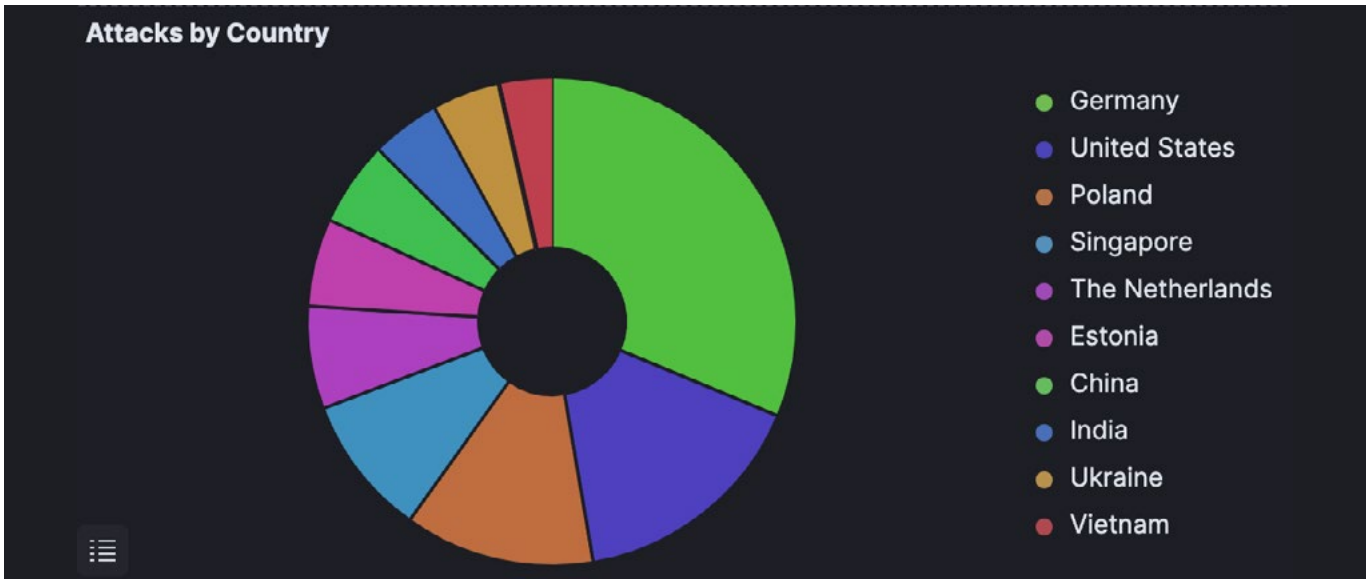
Sonuç

- Hükümetler dünya çapında, giderek daha bağlantılı bir dünyada kullanıcıları güvende tutmayı amaçlayan IoT güvenlik yasa ve düzenlemeleri oluşturmaktadır. Hükümet regülasyonlarına veya rehberlerine uyulmaması, ürünlerin belirli bölgelerde dağıtımını engelleyebilecektir.
- Günümüzde, bir zafiyet beyan politikası belirleyip bunu ürünlerin "uygunluk beyanı" ile birlikte sunmak gibi bazı temel prosedürler kullanılarak regülasyonlarla uyumlu hâle gelinebilir.
- Yönetmelikler giderek daha katı hâle geldikçe, EN 303645 gibi belirlenmiş standartların mümkün olduğu kadar çoğuna uyum sağlamak akıllıca olacaktır. IASME Konsorsiyumu ve British Standards Institute gibi kuruluşlar, üreticilere mevcut düzenlemelere uyum sağlamada yardımcı olmakta ve ürünlerinin güvenliğini iyileştirmeleri konusunda rehberlik etmektedir.
- Görünen gelecek, hükümetlerin siber güvenliğin ürünlere entegre edilmesini zorunlu tutması yönündedir (örneğin, kurcalamaya dayanıklı çipler gibi donanım tabanlı güvenlik mekanizmalarının zorunlu kılınması gibi). Donanım seviyesindeki güvenlik önlemleri hayati önem kazanmaktadır. Aynı şekilde "Secure By Design" ve "Secure By Default" kapsamları IoT güvenliğinin temeli olacak şekilde düşünülmelidir. Her durumda, sürekli yenilenen siber tehditlere göğüs gerebilmek adına güvenlik önlemlerini düzenli olarak gözden geçirmek ve güncellemek kritik önem taşımaktadır.

Gelecekte, internete bağlı cihazların daha yaygınlaşmasıyla birlikte, ev aletlerinin satın alınmasında fiyat, kalite, işlevsellik, enerji tüketimi ve dayanıklılık gibi faktörlere ek olarak, siber güvenlik sertifikasyonu gibi bir parametrenin de denkleme ekleneceği öngörülmektedir.

Honeypot Verileri

Bu rapor üç ay içinde Honeypot sensörlerimizden topladığımız verilerle oluşturulmuştur. En çok saldırı toplanan ülkeler, portlar, en çok denenen kullanıcı adları ve parolalarla ilgili veriler azalan sırada listelenerek inceleme için sunulmuştur. Ocak, Şubat ve Mart 2024 ayları boyunca Honeypot sensörlerimize toplam 3.192.038 saldırı gelmiştir.



Şekil 19: Gelen saldırıların ülkelere göre dağılımı.

Saldırıların Geldiği Ülke	Saldırı Sayısı
Almanya	826.355
ABD	421.484
Polonya	331.822
Singapur	245.643
Hollanda	179.461
Estonya	153.475
Çin	148.143
Hindistan	120.517
Ukrayna	117.082
Vietnam	93.748

Tablo 2: En çok saldırı gelen 10 ülke ve saldırı sayıları.

Saldırılan Port	Saldırı Sayısı
5900 - VNC	995.819
25 - SMTP	665.901
445 - SMB	457.890
22 - SSH	153.647
23 - Telnet	52.351
21 - FTP	5.317
80 - HTTP	3.566
5432 - PostgreSQL	2.345
5555 - ADB	2.248
443 - HTTPS	1.403

Tablo 3: En çok saldırı gelen portlar, bu portları kullanan servisler ve saldırı sayıları.

Toplanan veriler incelendiğinde, en çok saldırı gelen ülkenin Almanya (%31,33) olduğu, sonrasında ABD (%15,98), Polonya (%12,58), Singapur (%9,31) ve Hollanda'nın (%6,8) geldiği görülmektedir.

Tablo 3'te de görüldüğü üzere en çok saldırı 5900 portuna gelmiştir. 5900 portunda sunucuların yazıcı ve paylaşılan dosyalar için kullandığı SMB servisi çalışmaktadır. Bu yüzden SMB servisinin diğer servislerden daha çok saldırı alması beklenen bir durum olarak kabul edilebilir. VNC (Virtual Network Computing), uzaktan masaüstü erişimi sağlayan bir protokol olduğundan, bu porta yönelik saldırılar sıklıkla yetkisiz erişim ve kötü amaçlı yazılımların bulaşması amacıyla yapılmış olabilir.

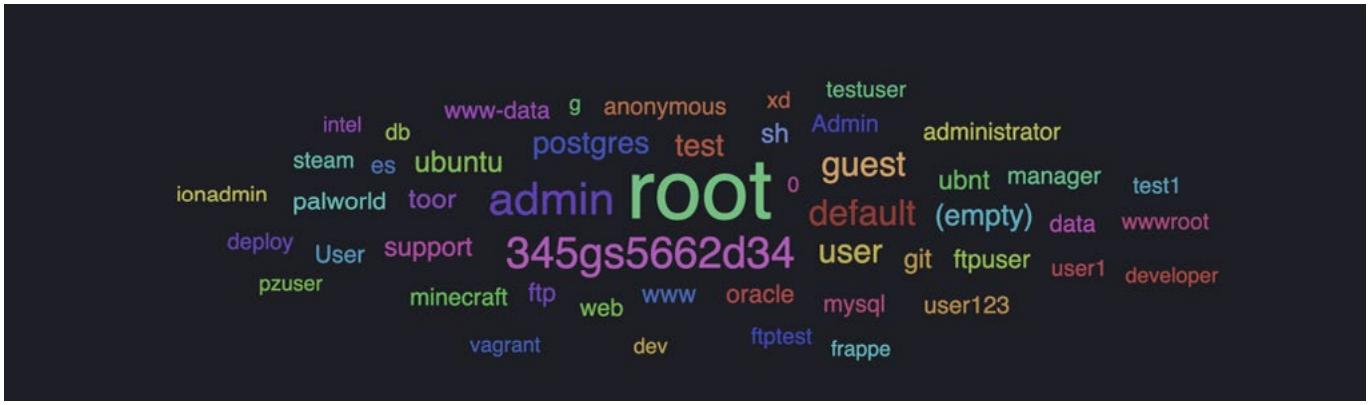
İkinci sırada 25 numaralı port (SMTP) yer almaktadır. SMTP (Simple Mail Transfer Protocol), e-posta iletişimi için kullanılan standart bir protokoldür. Bu porta yapılan saldırılar genellikle spam gönderimi ve e-posta tabanlı saldırılardır.

Üçüncü sırada 445 numaralı port (SMB) bulunmaktadır. Bu port, sunucular arasında dosya ve yazıcı paylaşımı sağlayan SMB (Server Message Block) protokolü için kullanılır. Saldırganlar sistemlere sızma ve fidye yazılımları gibi saldırıları genellikle bu portu hedef alarak gerçekleştirirler.

Denenen Parola	Deneme Sayısı
123456	13.809
3245gs5662d34	9.555
345gs5662d34	9.543
admin	5.594
123	3.910
password	3.306
(boş)	3.302
12345	2.898
1234	1.838
root	1.730

Tablo 4: SSH ve RDP honeypotlarımız üzerinde en çok denenen parolalar ve deneme sayıları.

Şekil 20: Parola etiket bulutu.



Şekil 21: Kullanıcı adı etiket bulutu.

Denenen Kullanıcı Adı	Deneme Sayısı
root	69.616
admin	11.181
345gs5662d34	9.548
default	4.051
guest	3.459
user	2.965
postgres	2.087
Test	1.821
(boş)	1.641
ubuntu	1.557

Tablo 5: SSH ve RDP Hhoneypotlarımız üzerinde en çok denenen kullanıcı adları ve deneme sayıları.

Denenen parolalar incelendiğinde, birçok yönetim arayüzünün standart olarak kullandığı parolalar olan 123456, 3245gs5662d34, admin gibi terimler gözlemlenmektedir. Test veya deneme süreçleri tamamlanır tamamlanmaz bu parolaların karmaşık, 12-16 karakterli, özel karakter içeren parolalarla değiştirilmesi analistlerimiz tarafından tavsiye edilmektedir. Ayrıca kolay hatırlanması ve girilmesi için herhangi bir harf, özel karakter içermeden sadece sıralı sayılar ile oluşturulmuş parolalar kullanmaktan kaçınılmalıdır.

Denenen kullanıcı adları incelendiğinde, yeni kurulmuş olan sistemlerin sıklıkla kullandığı root, admin, user gibi kullanıcı adlarının saldırganlar tarafından tercih edildiği görülmektedir. Kurulumu tamamlanan servislerin ve yönetim panellerinin kullanıcı adlarının en kısa zamanda değiştirilmesi ve kurulan sistemlerin kendi isimlerinin kullanılmaması (örn. ubuntu, postgres, oracle, testuser) tavsiye edilmektedir.

KAYNAKÇA:

[1] "What Is Social Engineering,"[Çevrimiçi]. Available: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering.

[2] "AI-powered social engineering attacks are seeing a huge rise,"[-Çevrimiçi]. Available: https://www.techradar.com/pro/security/ai-powered-social-engineering-attacks-are-seeing-a-huge-rise-and-thats-a-major-problem.

[3] "Social Engineering Phishing Attacks,"[Çevrimiçi]. Available: https://www.helpnetsecurity.com/2024/03/04/social-engineering-phishing-attacks/.

[4] "Ways To Avoid Social Engineering Attacks,"[Çevrimiçi]. Available: https://www.kaspersky.com.tr/resource-center/threats/how-to-avoid-social-engineering-attacks.

[5] "Apple Vision Pro and Meta Quest in danger of Inception-style attacks," 12 Mart 2024.[Çevrimiçi]. Available: https://interestingengineering.com/news/apple-vision-pro-and-meta-quest-in-danger-of-inception-style-attacks.

[6] "Inception Attacks: Immersive Hijacking in Virtual Reality Systems," 11 Mart 2024.[Çevrimiçi]. Available: https://sandlab.cs.uchicago.edu/tmp/inception.pdf.

[7] "msrc.microsoft.com,"[Çevrimiçi]. Available: https://msrc.microsoft.com/blog/2019/07/a-proactive-approach-to-more-secure-code/.

[8] [Çevrimiçi]. Available: https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf.

[9] [Çevrimiçi]. Available: https://www.cisa.gov/sites/default/files/2023-12/The-Case-for-Memory-Safe-Roadmaps-508c.pdf.

[10] [Çevrimiçi]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.[Erişildi: 10 04 2024].

[11] [Çevrimiçi]. Available: https://www.txone.com/blog/malware-analysis-lockbit-3-0/.

[12] [Çevrimiçi]. Available: https://www.kaspersky.com/resource-center/threats/lockbit-ransomware.

[13] kaspersky, "www.kaspersky.com.tr,"[Çevrimiçi]. Available: https://www.kaspersky.com.tr/resource-center/threats/online-banking-theft.

[14] O. Balyemez, 2024.[Çevrimiçi]. Available: https://siberbulten.com/dijital-guvenlik/tarihin-en-buyuk-veri-sizintisi-26-milyar-kullanici-bilgisi-calindi/.[Erişildi: Mart 2024].

[15] csf20.[Çevrimiçi]. Available: https://www.nist.gov/cyberframework/nists-journey-csf-20.

[16] N. C. 2. K. Rigopoulos, "NIST's Journey to CSF 2.0," 5 3 2024.[Online]. Available: https://www.nist.gov/cyberframework/nists-journey-csf-20.

[17] N. Hanacek, "NIST Releases Version 2.0 of Landmark Cybersecurity Framework," 26 2 2024.[Çevrimiçi]. Available: https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework.

[18] N. I. o. S. a. Technology, NIST SP 800-39: Managing Information Security Risk, National Institute of Standards and Technology, 2011.

[19] ISO/IEC, International Standard ISO/IEC 27005: 2022, ISO/IEC, 2022.

[20] N. I. o. S. a. Technology, NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments, National Institute of Standards and Technology, 2012.

[21] Synopsys, "2023 Open Source Security and Risk Analysis," 2022.

[22] "SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response (infographic)," 22 April 2021.[Çevrimiçi]. Available: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

[23] Veracode, "STATE OF SOFTWARE SECURITY Open Source Edition," 2020.

[24] "How GitHub secures open source software," 23 Feb 2021 .[Çevrimiçi]. Available: https://resources.github.com/security/open-source/how-github-secures-open-source-software/.

[25] R. Lemos, "Unpatched Open Source Libraries Leave 71% of Apps Vulnerable," 19 May 2020.[Çevrimiçi]. Available: https://www.darkreading.com/application-security/unpatched-open-source-libraries-leave-71-of-apps-vulnerable.

[26] D. Berman, "Securing your open source dependencies with the Snyk Visual Studio Code extension," 23 Nov 2021.[Çevrimiçi]. Available: https://snyk.io/blog/securing-open-source-dependencies-snyk-visual-studio-code-extension/.

[27] "Top 30+ IoT Statistics and Facts You Should Know for 2023," 18 July 2023.[Çevrimiçi]. Available: https://connect.comptia.org/blog/top-internet-of-things-stats-facts#:~:text=According%20to%20Cisco%2C%20500%20billion,devices%20connects%20to%20the%20internet.

[28] "Avrupa Birliği, Akıllı Cihazlar için Siber Güvenlik Kuralları Sunmaya Hazırlanıyor," 4 Ekim 2022.[Çevrimiçi]. Available: https://bilgiguvende.com/avrupa-birligi-akilli-cihazlar-icin-siber-guvenlik-kurallari-sunmaya-hazirlaniyor/.

[29] "Home Smart IoT Home: Domesticating the Internet of Things," 2016.[Çevrimiçi]. Available: https://www.toptal.com/designers/interactive/smart-home-domestic-internet-of-things.

[30] "Sanayi ve Teknoloji Bakanı Kacır: Akıllı ev aletlerinde siber güvenlik standartları belirlenecek," 27 Şubat 2024.[Çevrimiçi]. Available: https://www.aa.com.tr/tr/gundem/sanayi-ve-teknoloji-bakani-kacir-akilli-ev-aletlerinde-siber-guvenlik-standartlari-belirlenecek/3148955.

[31] "IoT malware attacks up by 37% in the first half of 2023," 3 August 2023.[Çevrimiçi]. Available: https://iotac.eu/iot-malware-attacks-up-by-37-in-the-first-half-of-2023/#:~:text=According%20to%20the%20mid%2Dyear,first%20six%20months%20of%202022.

[32] "SonicWall'un Yeni Siber Tehdit Raporu, Yükselen Tehdit Seviyelerini ve Güç Kaymalarını Ortaya Çıkarıyor," 18 Mart 2021.[Çevrimiçi]. Available: https://e-data.com.tr/sonicwallun-yeni-siber-tehdit-raporu-yukselen-tehdit-seviyelerini-ve-guc-kaymalarini-ortaya-cikariyor/.

[33] "How to Ensure Cybersecurity in the Age of IoT," 4 September 2023.[Çevrimiçi]. Available: https://appinventiv.com/blog/how-to-ensure-cybersecurity-in-iot/.

[34] "Cyber security legislation trends in the IoT industry," 15 Nisan 2024.[Çevrimiçi]. Available: https://www.iotinsider.com/iot-insights/cyber-security-legislation-trends-in-the-iot-industry/.

[35] "NISTIR 8259A- IoT Device Cybersecurity Capability Core Baseline Definition," 2020.

[36] "NISTIR 8259A - IoT Device Cybersecurity Capability Core Baseline," 2020.

[37] "NIST IR 8228 - CONSIDERATIONS FOR MANAGING IOT CYBERSECURITY AND PRIVACY RISKS," 2019.

[38] "Profile of the IoT Core Baseline for Consumer IoT Products," 2022.

[39] "Cyber Security for Consumer Internet of Things: Baseline Requirements," 2020.

[40] "Secure Design Best Practice Guides," 2019.

[41] "Cyber security legislation trends in the IoT industry," 2024.

STM
www.stm.com.tr
/STMDefence
thinktech
STM Teknolojik Düşünce Merkezi
thinktech.stm.com.tr
/STMThinkTech