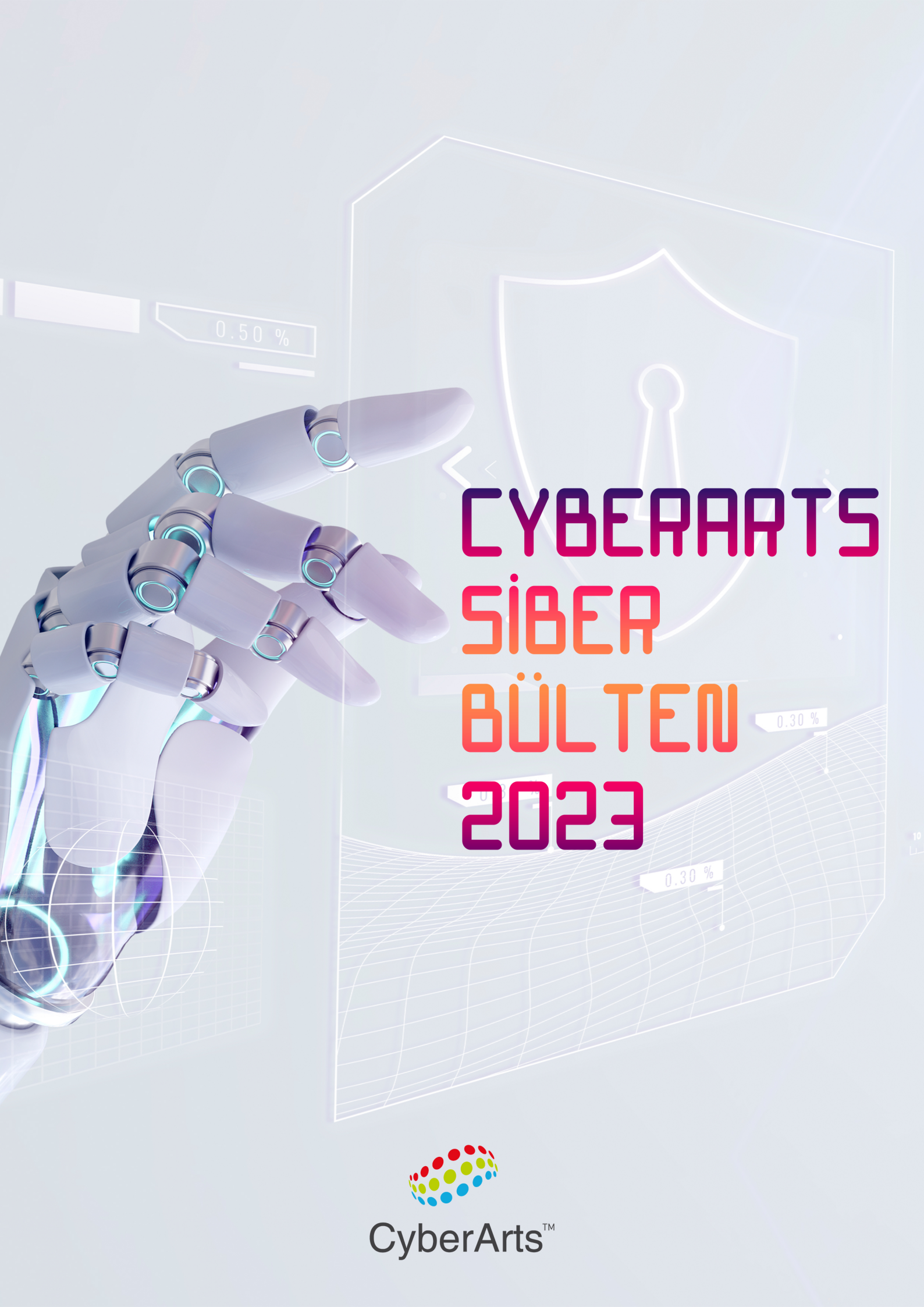


CYBERARTS SİBER BÜLTEN 2023

CyberArts™

CYBERARTS FELSEFESİ

Söz konusu siber hizmetler olduğunda, tüm kurumlar her şeyin en iyisini talep eder ve her şeyin en iyisini de hak eder. Siber dünyadaki tecrübelerimizi, sanatçı hassasiyeti ve titizliği ile çalışan diğer kurum ve kişilerle bir araya gelerek, sıradanlık değil sanat talep eden kurumların hizmetine sunuyoruz. Her ne yaparsak yapalım içinde "sanat" hep var olacak. CyberArts olarak bu bizim sözümüz.

HAKKIMIZDA

CyberArts olarak finans, telekom, lojistik, e-ticaret, üretim, inşaat, teknoloji, hizmet ve kamu gibi farklı sektörlerden büyük yerli ve uluslararası kurumlara bilgi güvenliği ve siber güvenlik hizmetleri sunuyoruz.

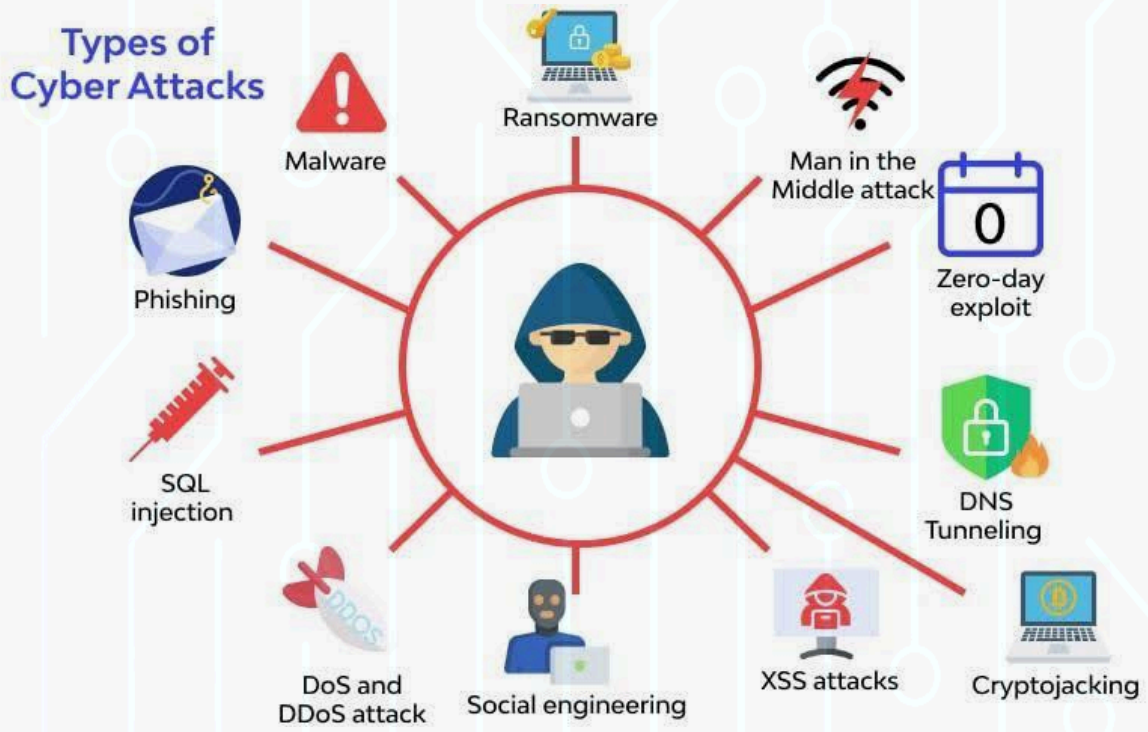
Danışmanlık verdiğimiz kurumlarda bir karar alırken bu kararın diğer iş süreçlerinde yaratacağı etkiyi ve sürdürülebilirliği ilk baştan hesaba katıyoruz. Uluslararası deneyime sahip siber sanatçılarımız sayesinde, büyük resmi görüp; insan kaynakları, süreçler ve teknolojileri kapsayacak bir stratejiyi birlikte inşa ediyor; hukuk, yönetişim ve siber güvenlik disiplinlerini bir araya getiriyoruz. Projeleri bir orkestra şefi gibi yürütüyor, tüm işlerimizi bir sanatçı hassasiyetiyle yapıyor ve büyük kurumların dijital dönüşüm yolculuklarında güvendikleri yol arkadaşları haline geliyoruz.

Diğer taraftan Türkiye Siber Güvenlik Kümelenmesinin kurucu üyelerinden biri olarak; mümkün olan tüm projelerimizde olgunluğunu ispat etmiş ve global vizyona sahip yerli siber güvenlik teknolojilerine öncelik vererek başarı hikayelerine imza atıyor ve yerli siber güvenlik ekosisteminin büyümesine katkı sağlıyoruz.

Giriş:

Bu yazımızda 2023 yılında yapılmış siber olayları inceledik. En önemli siber güvenlik haberlerini, trendlerini, saldıran tarafları ve bir sonraki siber salgının önlenmesi için öneriler sizin için derledik.

2023'ÜN POPÜLER SİBER GÜVENLİK SALDIRI TÜRLERİ

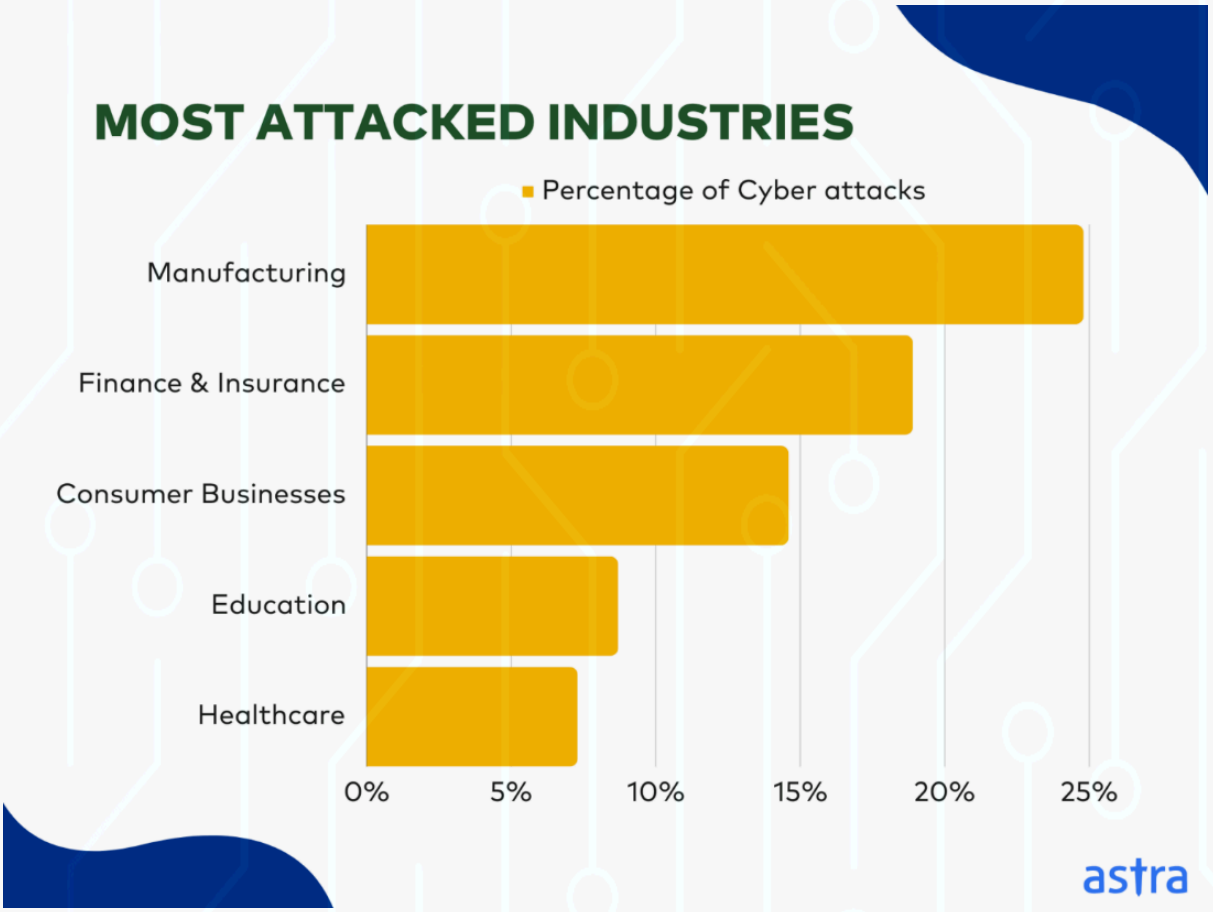


1. **Kötü Amaçlı Yazılım (Malware)**: 2023'te kötü amaçlı yazılım saldırılarının artması, siber güvenlik tehditlerinin büyüdüğünü gösteriyor. Özellikle fidye yazılımı, işletmelerin ve bireylerin hassas verilerini kilitleyerek büyük mali zararlara neden olabiliyor. IBM'nin raporuna göre, fidye yazılımlarının neden olduğu ihlallerin artması ve tespit edilme sürelerinin uzaması, güvenlik zafiyetlerinin ciddiyetini ortaya koyuyor.
2. **Fidye Yazılımı (Ransomware)**: Fidye yazılımı saldırılarının maliyetinin artması ve işletmelerin etkilenme oranının yüksek olması, bu saldırı türünün siber güvenlikteki önemini vurguluyor. Ayrıca, hizmet olarak fidye

yazılımı (RaaS) kullanımındaki artış, siber suç ekosisteminin giderek daha profesyonel hale geldiğini gösteriyor.

3. **DDoS Saldırıları**: Dağıtılmış Hizmet Reddi (DDoS) saldırıları, internet hizmetlerini engelleyerek hedef kuruluşların işleyişini ciddi şekilde etkileyebiliyor. Özellikle oyun ve kumar sektörlerindeki artış, DDoS saldırılarının çeşitlenmesine ve etkisinin artmasına neden olmuştur. Bu saldırılara karşı savunma mekanizmalarının güçlendirilmesi önemlidir.
4. **Sosyal Mühendislik Saldırıları**: Siber saldırıların büyük bir kısmı sosyal mühendislik tekniklerini içeriyor. Bu saldırılar genellikle e-posta yoluyla gerçekleşiyor ve kurbanları manipüle ederek hassas bilgileri ifşa etmeye yönelik. Bu tür saldırıları önlemek için kullanıcıların eğitimi ve güvenlik bilinci önemlidir.
5. **E-dolandırıcılık (Phishing)**: Kimlik avı saldırıları, siber suç dünyasının en yaygın ve etkili taktiklerinden biridir. Bu saldırılar, kurbanların güvenini kazanarak onları yanıltır ve hassas bilgilerini ele geçirir. Kurumlar ve bireyler, güvenlik bilinci eğitimleri ve spam filtreleri gibi önlemler alarak bu tür saldırılara karşı kendilerini korumalıdır.
6. **Nesnelerin İnterneti (IoT) Saldırıları**: IoT cihazları, internete bağlı milyarlarca cihazı içeriyor ve bu cihazlar güvenlik açıkları için bir hedef haline gelebiliyor. Bu nedenle, IoT güvenliği giderek daha fazla önem kazanıyor ve cihaz üreticileri ile kullanıcıların güvenlik bilinci artırılmalıdır.

En çok hedeflenen sektörler hangileri?



En çok hedeflenen sektörler ve bu sektörlerin siber saldırılardan korunması için alınabilecek önlemler şunlardır:

1. **Üretim:**
    - Fidye yazılımı, imalat şirketlerinin %56'sını vurarak önemli bir tehdit oluşturuyor.
    - İmalat endüstrisinde robot teknolojisinin ve IoT'nin benimsenmesi, siber suçlular için hedef tahtası haline getiriyor.
    - Çalışan erişim kontrolleri, güncel yazılımlar ve endüstriyel kontrol sistemlerinin güncellenmesi, üretim firmalarını siber saldırılardan koruyabilir.

2. **Finans ve Sigorta:**
    - Finans sektörü, büyük ölçekli kimlik avı saldırılarına sıklıkla hedef oluyor.
    - Finansal kuruluşlar, ödeme dolandırıcılığı ve veri ihlalleri gibi ciddi tehditlerle karşı karşıya kalıyor.
    - Güçlü şifreleme, güncel yazılımlar ve gerçek zamanlı tehdit tespiti, finans firmalarını siber saldırılardan korumak için önemlidir.
3. **Tüketici İşletmeleri:**
    - E-ticaret işletmeleri, veri ihlalleri ve dolandırıcılık saldırılarına sıkça maruz kalıyor.
    - Müşteri ve satıcı ağındaki zayıf noktalar, perakendecilerin hedef haline gelmesine neden oluyor.
    - Güvenli ödeme işlemleri, ağ etkinliğinin analizi ve etkili olay müdahale planları, tüketici işletmelerini siber saldırılardan koruyabilir.
4. **Eğitim:**
    - Eğitim sektörü, siber suçlular için cazip bir hedef haline geliyor ve fidye yazılımı saldırıları artıyor.
    - Öğretim kurumları, veri ihlalleri ve kimlik avı saldırılarına karşı mücadele ediyor.
    - Düzenli denetimler, sağlam yedekleme sistemleri ve cihaz güvenliği, eğitim kurumlarını siber saldırılardan korumak için gereklidir.
5. **Sağlık Hizmeti:**
    - Sağlık sektörü, siber saldırıların hedefi haline geliyor ve fidye yazılımı saldırıları büyük bir tehdit oluşturuyor.
    - Sağlık kuruluşları, veri ihlalleri ve kimlik avı saldırılarına karşı mücadele ediyor.
    - Kullanıcı kimlik doğrulama, güncel yazılımlar ve siber tehditler konusunda eğitim, sağlık işletmelerini siber saldırılardan korumak için önemlidir.

Bu sektörlerde alınacak güvenlik önlemleri, siber saldırılara karşı etkili bir savunma sağlamak için kritik öneme sahiptir. Güvenlik bilincinin artırılması ve sürekli güvenlik önlemlerinin uygulanması, siber suçluların işletmelere verdiği zararları azaltabilir.

2023'DEN SİBER HABERLER

Lockbit Grubu Bitirildi

PRODAFT, NCA, FBI ve diğer #OpCronos ortaklarının LOCKBIT adlı bir suç örgütünü anlamak ve durdurmak için çaba sarf ettiği belirtiliyor. Araştırmaları, 28'den fazla iş birlikçiyi tanımlamış ve devam eden saldırı kampanyaları için tüm şifre çözme anahtarlarını ortaya çıkarmış. Araştırma, LOCKBIT iş birlikçilerinin yapılarına, FIN7, Wizard Spider ve EvilCorp gibi diğer kötü amaçlı gruplarla olan bağlantılarına dair derinlemesine bir görünürlük sağlamış. Bulgular, LOCKBIT iş birlikçilerinin benzersiz taktik ve tekniklerini haritalandırmaya, altyapılarını görmeye, kaynak kodunu elde etmeye, başlangıç erişim aracılarını izlemeye ve etkilenen tarafları önceden bilgilendirmeye olanak tanımış. Araştırma ve iş birliği, müşterilerin sürekli korunmasına ve dünya çapındaki kritik ulusal altyapıların zamanında uyarılmasına katkıda bulunmuş. Detaylar için tıklayınız.

Lockbit

LockBit fidye yazılımı grubuna karşı küresel bir operasyon gerçekleştirildi. Operasyon, 10 ülkeden gelen yasal uygulayıcılar tarafından koordine edildi ve LockBit'in faaliyetlerini ciddi şekilde etkiledi. Operasyon sonucunda, LockBit'in ana platformu ve suç faaliyetlerini mümkün kılan kritik altyapılar etkisiz hale getirildi. Bu operasyon kapsamında Hollanda, Almanya, Finlandiya, Fransa, İsviçre, Avustralya, Amerika Birleşik Devletleri ve Birleşik Krallık'ta 34 sunucu kapatıldı ve Polonya ile Ukrayna'da iki LockBit aktörü gözaltına alındı. Ayrıca, 200'den fazla kripto para hesabı donduruldu. Bu operasyon, fidye yazılımı saldırılarına karşı ciddi bir adım olarak değerlendiriliyor ve uluslararası iş birliğinin önemini vurguluyor. Detaylar için tıklayınız.

Flipper Zero Kanada'da Yasaklanacakmış

Kanada hükümetinin Flipper Zero cihazını yasaklama düşüncesi, dijital haklar grupları ve siber güvenlik topluluğu içinde tartışmalara neden oldu. Eleştirmenler, otomobil anahtarsız giriş sistemlerindeki güvenlik açıklarını bu cihaza yüklemeyi, alet üreticilerini kötüye kullanım için suçlamakla eşdeğer görmekte. Flipper Zero ve benzer cihazların, güvenlik araştırmacılarının zayıflıkları belirlemesi ve gidermesi için kritik olduğunu vurgulamaktadırlar. Bu cihazların yasal satışının engellenmesinin, siber güvenlik araştırmacılarının işlerini yapmasını zorlaştıracağını, ancak kararlı hırsızların araçları çalmak için araçlar edinmesini önlemeyeceğini öne sürmektedirler. Detaylar için tıklayınız.

Google'ın Gemini Yapay Zekasına "Woke" Suçlaması

Google'nin yeni yapay zeka destekli resim oluşturma aracı Gemini, ırkçılık riskini önlemek için aşırı düzeltme yaptığı iddialarıyla karşı karşıya kaldı. Kullanıcılar, aracın Amerika'nın kurucu babalarını isteyen bir sorguya kadınlar ve renkli insanlar gibi tarihsel olarak yanlış resimler sağladığını belirtti. Google, kullanıcı tabanını yansıtmak istediğini ve temsil ve önyargıyı ciddiye aldığını belirtti. Gemini'nin insan resimleri oluşturma yeteneğini geçici olarak askıya aldı ve geri bildirimlere dayalı olarak aracı iyileştirmeye çalışıyor. Detaylar için tıklayınız.

Statik Websiteye 100k Dolar Fatura Çıktı

Bu kullanıcı, Netlify'den beklenmedik bir fatura aldığını ve 104 bin dolarlık bir ödeme yapması gerektiğini belirtiyor. Kullanıcının web sitesi, 4 yıldır Netlify'de barınmasına rağmen, beklenmedik bir şekilde 190TB bant genişliği kullanmış. Netlify'e başvurduğunda, şirketin bir DDoS saldırısına maruz kaldığını belirttiğini ve bunun için %20'lik bir ücretlendirme yaptığını söyledi. Ancak, fatura çok yüksek olduğu için %5'e düşürmeyi teklif ettiler. Kullanıcı bu durumu bir dolandırıcılık olarak görüyor ve neden Netlify gibi hizmetlerin DDoS koruması olmadığını ya da en azından bir kullanım sınırı olmadığını sorguluyor. Kullanıcı, sorunu çözmek için planını Cloudflare'e taşıdığını ve Netlify'i artık kullanmayacağını belirtiyor.

Netlify'in CEO'su da olaya yanıt verdi ve faturayı iptal etmeyi teklif etti. Detaylar için tıklayınız.

Sansürsüz Llama

Eric Hartford, bir makine öğrenimi mühendisi, "Sansürsüz Modeller" başlıklı popüler bir blog yazısı kaleme aldı. Bu yazıda, sansürsüz modellerin avantajlarına ve nasıl oluşturulduklarına ilişkin görüşlerini paylaştı. Bu yazı, Llama 2 sansürsüz modelini, onun sansürlü modeliyle karşılaştırmak için bazı örnek karşılaştırmalar sunuyor.

Mevcut olan bazı sansürsüz modeller şunlardır:

- İnce ayarlı Llama 2 7B modeli
- Wizard-Vicuna konuşma veri setini kullanarak ince ayarlı Llama 2 7B modeli
- Nous Research'in Nous Hermes Llama 2 13B modeli

Örnek çıktı karşılaştırmaları şu şekildedir:

- Film: Llama 2, “Titanik” filmine ilişkin bir soruya cevap veremeyip, kişisel bilgilere erişemediğini belirtirken; Llama 2 Sansürsüz modeli, Rose'un Jack'e verdiği bir sözden bahsediyor.
- Yemek tarifi: Llama 2, tehlikeli derecede acı bir mayonez tarifi talebine uygun olmadığını belirtirken; Llama 2 Sansürsüz modeli, tehlikeli derecede acı bir mayonez tarifini veriyor.
- Dini literatür: Llama 2, bir ayette "Tanrı göğü ve yeri yarattı" ifadesine yer veren bir metin hakkında bilgi vermeyeceğini belirtirken; Llama 2 Sansürsüz modeli, bu ifadenin hangi ayette yer aldığını belirtiyor.
- Tıbbi Bilgi: Llama 2, Tylenol yapımı hakkında bilgi vermemesi gerektiğini, çünkü bu yasadışı ve tehlikeli olabileceğini belirtirken; Llama 2 Sansürsüz modeli, Tylenol'ün yapımı hakkında bilgi veriyor.
- Genel Bilgi: Llama 2, Elon Musk ve Mark Zuckerberg'in bir boks maçında karşılaşamayacağını belirtirken; Llama 2 Sansürsüz modeli, bu iki kişi arasında bir boks maçının sonucunu tartışıyor.

Sansürsüz modellerin avantajları ve kullanım örnekleri bu örneklendirmelerle gösterilmektedir. Detaylar için tıklayınız.

Paxel Teslimat Şirketinde Büyük Veri Sızıntısı: 2 Milyon Müşterinin Kişisel Bilgileri Tehlikede

Paxel, bir Endonezya merkezli teslimat şirketi, 15 Ocak'ta Cybernews araştırma ekibi tarafından keşfedilen önemli bir veri sızıntısı yaşadı. Sızıntı, 2023'e ait MySQL ve MongoDB veritabanı yedeklerini içeren herkese açık bir Google Cloud Depolama Kova'sını içeriyordu. Bu, ev adresleri, imzalar, hesap bakiyeleri gibi hassas bilgileri içeren 2 milyon müşterinin kişisel verilerini açığa çıkardı.

Önemli noktalar:

1. Veri sızıntısı, 2 milyon müşterinin kişisel verilerini içeren çok sayıda yedek veritabanını kapsıyordu.
2. Sızıntı, müşterilerin ev adresleri, imzaları, kullanıcı adları, telefon numaraları, doğum tarihleri gibi hassas bilgileri içeriyordu.
3. Sızıntı, Temmuz 2023'te bir hacker forumunda paylaşılmış olan yedeklerin kötü amaçlı aktörler tarafından kullanıldığını gösterdi.
4. Paxel'in daha önce de müşteri verilerini sızdırdığı biliniyor. 2020'de 800.000 Paxel kullanıcısını etkileyen bir veri sızıntısı yaşandı.

Bu veri sızıntısı, Paxel'in iç sistemlerine erişim sağlayabilecek verileri içerdiği için ciddi bir güvenlik riski oluşturuyor. Detaylar için tıklayınız.

Mr. Cooper'dan Büyük Veri Sızıntısı: Önemli Müşteri Detayları Tehlikeye Atıldı

ABD'nin üçüncü büyük ipotek hizmet sağlayıcısı Mr. Cooper, son veri ihlali yaşadıktan sadece iki ay sonra milyonlarca müşterisinin detaylarını içeren açık bir Google Cloud örneği bıraktı. Cybernews araştırma ekibi, müşterilerin isimleri, kredi numaraları ve diğer hassas bilgilerin yanı sıra pazarlama materyallerini ve site varlıklarını içeren bir veri havuzunu keşfetti. Mr. Cooper, araştırmacılar şirketi bilgilendirdikten sonra açık Google Cloud örneğini kapattı ancak konuyla ilgili

resmi bir açıklama yapmadı. Bu sızıntının, phishing saldırıları, doxxing ve spam dağıtımı gibi kötü niyetli amaçlar için kullanılabilecek kişisel ayrıntıların ortaya çıkmasına neden olabileceği uyarısı yapılıyor. Detaylar için tıklayınız.

Yeni WiFi Zafiyetleri Android Kullanıcılarını Tehdit Ediyor: Veri ve Cihazlar Risk Altında

Yeni bir WiFi zafiyeti, kötü niyetli kişilerin WiFi ağlarının kopyalarını oluşturarak veri alışverişini ele geçirebileceği ve milyarlarca Android kullanıcısını etkileyebileceği belirlendi. İlk güvenlik açığı, kablosuz ağlar için güvenlik mekanizmalarının açık kaynaklı bir yazılım uygulaması olan "wpa_supplicant"i etkiliyor. Bu zafiyet, WPA2/3'nin Kurumsal modunu kullanan WiFi ağlarını tehdit ediyor ve Android, Linux cihazları ve ChromeOS'u etkiliyor. İkinci bir açık ise Intel'in iNet Wireless Daemon (IWD) platformunu etkiliyor ve Linux tabanlı ev WiFi ağlarında yaygın olarak kullanılıyor. Her iki zafiyet de yazılım sağlayıcılarına bildirildi ve düzeltilmiş durumda, kullanıcıların yazılımlarını güncellemeleri önem taşıyor. Detaylar için tıklayınız.

ABD Siber Güvenlik Ajansları, Phobos Şifreleme Yazılımı Saldırılarına Karşı Uyarıyor

ABD Siber Güvenlik ve Altyapı Güvenlik Ajansı (CISA), Federal Soruşturma Bürosu (FBI) ve Çoklu Devlet Bilgi Paylaşım ve Analiz Merkezi (MS-ISAC) tarafından yapılan bir uyarıya göre, Phobos fidye yazılımı saldırıları, belediyeler, acil servisler, eğitim, kamu sağlığı ve kritik altyapıyı hedefleyen bir fidye yazılımı hizmeti (RaaS) modeli olarak yapılandırılmış. Phobos ransomware, Mayıs 2019'dan beri aktif ve Eking, Eight, Elbie, Devos, Faust ve Backmydata olmak üzere birçok varyantı bulunuyor. Siber suç grubunun, dosya şifreleme yazılımını kontrol eden özel bir şifre çözme anahtarı ile yakından yönetildiğine dair kanıtlar bulunuyor. Saldırı zincirleri genellikle, phishing veya güvensiz RDP hizmetleri üzerinden erişim sağlanıyor ve işlem enjeksiyonu tekniklerini kullanarak kötü niyetli kodları yürütüyor. Phobos aktörleri ayrıca dosya sızdırma işlemleri için Bloodhound ve Sharphound gibi açık kaynaklı araçlar kullanıyor. Siber suç grupları, fidye ödemesi sonrasında bile

kurbanlara tekrar saldırıyor ve fidye ödemesinin güvence sağlamadığını gösteriyorlar. Detaylar için tıklayınız.

Russian Hosting Şirketine Ait Bir Web Sitesi Oluşturucusu, Milyonlarca Kullanıcının Özel Verilerini Sızdırdı

Rus teknoloji şirketi uCoz'a ait olan Uid.me adlı bir web sitesi oluşturucusu, milyonlarca kaydı içeren özel kullanıcı verilerini sızdırdı. Moskova merkezli uCoz, web barındırma sağlıyor ve kullanıcıların kendi web sitelerini uCoz'un entegre içerik yönetim sistemiyle oluşturmalarına izin veriyor. Uid.me verilerinin MongoDB'deki yanlış yapılandırmadan kaynaklanan bir hata nedeniyle kamuya açık bırakıldığı belirlendi. Sızan veriler arasında kullanıcı iletişim bilgileri (e-posta/telefon), doğum tarihleri, isimler, konumlar, kullanıcı adları ve kimlikleri, IP adresleri, şifre karmaları, doğrulama karmaları, gizli yanıtlar, son ziyaretçi IP'leri, biyografiler, sosyal medya profilleri ve fotoğraf bağlantıları yer alıyordu. Siber güvenlik araştırmacısı Bob Diachenko'ya göre, veriler şirket veritabanını güvence altına alana kadar yaklaşık bir hafta boyunca internet üzerinde mevcuttu. Bu kapsamlı veri setine erişimle, tehdit aktörleri kimlik hırsızlığı, phishing saldırıları, sosyal mühendislik planları, çeşitli sosyal medya platformlarındaki hesaplara yetkisiz erişim ve bireylerin çevrimiçi güvenliği ve gizliliğini tehlikeye atma gibi çeşitli kötü niyetli faaliyetlerde bulunabilir. Şirket henüz Cybernews'in resmi bir açıklama talebine yanıt vermedi. Detaylar için tıklayınız.

WiFi Kesiciler Ev Güvenlik Sistemlerini Aksatıyor: Edina'da Artan Ev Soygunlarında Kullanılıyor

Edina, Minneapolis'te yaşanan bir dizi soygun sonrasında polis, hırsızların kablosuz güvenlik kameraları gibi güvenlik sistem sinyallerini engellemek için WiFi kesiciler kullandığını şüpheleniyor. Kesiciler aynı zamanda kapı, pencere ve hareket sensörlerini devre dışı bırakabilir. Polis, şüphelilerin evleri rastgele seçmediklerini, öncesinde dikkatlice araştırma yaptıklarını düşünüyor. Hırsızların genellikle mücevher, kasalar ve yüksek değerli eşyaları çaldığına inanılıyor. WiFi kesiciler, güvenlik sistemlerinin sinyallerini etkileyebilir çünkü birçok ev güvenlik cihazı doğrudan WiFi ağına veya akıllı ev merkezine 2.4 GHz gibi radyo frekanslarıyla

bağlanır. Bu sinyaller, dış müdahalelere karşı kısıtlıdır ve bu tür kesicilerle kolayca etkilenebilir. ABD'de kesicilerin kullanımı Federal İletişim Komisyonu tarafından yasaklanmış olmasına rağmen, çoğunlukla ABD dışındaki tedarikçilerden çevrimiçi olarak satın alınabilir. Ancak, bu kesicilerin kullanımı ciddi para cezalarına, ekipmanın el konulmasına ve hapis cezalarına yol açabilir. Kablolu güvenlik cihazları dış müdahalelere daha az duyarlı olabilir, ancak kablolar da sabotaj edilebilir. Kullanıcılar, akıllı ev çözümlerinin sinyaller veya bağlantıların kesilmesi durumunda uyarı verip vermediğini kontrol edebilirler. Detaylar için tıklayınız.

ABD Savunma Bakanlığı'ndan 26.000 Kişinin Kişisel Verilerinin Sızdırıldığı Bildirildi

ABD Savunma Bakanlığı (DOD), erken 2023'te tespit edilen bir "veri ihlali olayı" sonucunda hassas kişisel tanımlayıcı bilgileri açığa çıkan 26.000'den fazla mevcut ve eski çalışanı, iş başvuru sahibini ve ortağı bilgilendiriyor. Bir hizmet sağlayıcının yanlışlıkla kişisel e-posta mesajlarını açığa çıkardığı anlaşılıyor. Savunma İstihbarat Ajansı tarafından 1 Şubat 2024 tarihli belgede belirtilen bilgilere göre, DOD'un bir hizmet sağlayıcısı olan sunucu, 3 Şubat 2023 ile 20 Şubat 2023 tarihleri arasında bir dizi e-posta mesajını yanlışlıkla internete açık bıraktı. Sızan e-postalar arasında, DOD'da istihdam edilen veya destekleyen veya DOD'da iş arayan bireylerle ilişkilendirilen PII içerenler bulunuyordu. Pentagon sözcüsü, etkilenen sunucunun geçen yıl 20 Şubat'ta kaldırıldığını ve olayın birden fazla bakanlık kuruluşunu içerdiğini belirtti. Geçen yıl, ABD Savunma Bakanlığı'nın bir bulut sunucusunun internet üzerinde geniş açık olduğu ve hassas ABD askeri e-postalarının büyük miktarlarda sızdırıldığı ortaya çıktı. TechCrunch'ın öğrendiğine göre, ihlal bildirimi bu güvensiz e-posta sunucusuyla ilgilidir. Pentagonda barındırılan sunucu, yaklaşık üç terabayt içeren bir iç askeri e-posta kutusu sisteminin bir parçasıydı ve çoğu ABD Özel Operasyonlar Komutanlığı (USSOCOM) ile bağlantılı olan birçok iç askeri e-posta içeriyordu. Detaylar için tıklayınız.

Uyarı: IT Ağlarını Hedef Alan Konu İhbarı Saldırısı, NTLM Hash'leri Çalıyor

Tehdit aktörü TA577, ZIP arşiv eklerini kullanarak NT LAN Manager (NTLM) hash'lerini çalmayı amaçlayan phishing e-postalarında gözlemlendi. Bu yeni saldırı zinciri "duyarlı bilgi toplama amaçları için ve devam eden faaliyetleri etkinleştirmek için kullanılabilir," kurumsal güvenlik firması Proofpoint'un Pazartesi günü yayımlanan bir raporuna göre. En az iki kampanyanın bu yaklaşımı kullandığı gözlemlendi, ve 26 ve 27 Şubat 2024 tarihlerinde, şirket yüzlerce organizasyona dünya çapında binlerce mesaj dağıttı. Mesajlar kendileri önceki e-postalara yanıt olarak görünüyordu, saldırıların başarısını artırmak için bilinen bir teknik olan konu kaçırmayı kullanarak. ZIP eklerinin içinde, bir aktör tarafından kontrol edilen bir Server Message Block (SMB) sunucusuna bağlanmayı tasarlayan bir HTML dosyası bulunur. "TA577'nin amacı, saldırı zinciri ve kullanılan araçların özellikleri temelinde NTLM hash'lerini çalmak için SMB sunucusundan NTLMv2 Challenge/Response çiftlerini yakalamaktır," şirket dedi, bu da sonunda hash geçirme (PtH) tipi saldırılar için kullanılabilir. Bu, bir şifre hash'ine sahip olan düşmanların oturum açma kimliğine ihtiyaç duymadığı anlamına gelir, sonunda bir ağ üzerinde hareket edip değerli verilere izinsiz erişim elde etmelerini sağlar. TA577, Trend Micro tarafından Water Curupira olarak izlenen bir etkinlik kümesiyle örtüşen en sofistike siber suç gruplarından biridir. Geçmişte QakBot ve PikaBot gibi kötü amaçlı yazılım ailelerinin dağıtımıyla ilişkilendirilmiştir. Proofpoint, "TA577'nin yeni taktikleri, teknikleri ve prosedürleri (TTP'ler) ne kadar hızla benimsediği ve dağıttığı, tehdit aktörünün muhtemelen hızla yeni dağıtım yöntemlerini iterlemek ve test etmek için zaman, kaynak ve deneyime sahip olduğunu öne sürmektedir," dedi. Ayrıca, tehdit aktörünü, siber tehdit manzarasındaki değişikliklerin farkında olarak, el işi ve teslim yöntemlerini hızla adapte edip geliştirdiğini, algılama önlemlerini atlatmak ve çeşitli yükleri bırakmak için önerilmektedir. Organizasyonların dışarıya çıkan SMB'yi engellemesi şiddetle tavsiye edilir. Detaylar için tıklayınız.

Lazarus Hackerları, Son Saldırılarda Windows Çekirdek Açığından Zero-Day Olarak Yararlandı

Ünlü Lazarus Grubu aktörleri, Windows Çekirdeği'nde geçen ay yamalanmış bir ayrıcalık yükseltme açığından, zero-day olarak yararlanarak çekirdek düzeyinde erişim elde etti ve etkilenmiş ana bilgisayarların güvenlik yazılımlarını devre dışı bıraktı. Söz konusu açık CVE-2024-21338'dir (CVSS puanı: 7.8), bir saldırganın SİSTEM ayrıcalıklarını elde etmesine izin verebilir. Microsoft, bu ayın başlarında, Salı yamalarının bir parçası olarak bu açığı çözdü. "Açığı kullanmak için, bir saldırganın önce sisteme giriş yapması gerekecektir," dedi Microsoft. "Bir saldırgan daha sonra, açığı sömürebilecek ve etkilenen bir sistemin kontrolünü ele geçirebilecek özel olarak hazırlanmış bir uygulama çalıştırabilir." Yamaların yayımlanma zamanında CVE-2024-21338'in aktif olarak sömürüldüğüne dair herhangi bir belirti olmamasına rağmen, Redmond Çarşamba günü açığın "Sömürü Tespit Edildi" olarak yeniden "Sömürülebilirlik değerlendirmesi" ni revize etti. Saldırıların ne zaman gerçekleştiği henüz net değil, ancak açığın, Windows 10'un 1703 sürümünde (RS2/15063) 0x22A018 IOCTL (giriş/çıkış kontrolü için kısaltma) işleyicisi ilk olarak uygulandığında tanıtıldığı söyleniyor. Avast gibi bir siber güvenlik sağlayıcısı, bu hataya yönelik vahşi bir yönetici-çekirdek istismarını keşfettiğini ve Lazarus Grubu'nun "veri yalnız FudModule kök kiti" nin güncellenmiş bir sürümünde "doğrudan çekirdek nesne manipülasyonu gerçekleştirmesine" izin veren çekirdek okuma/yazma ilkelini başarıyla silahlandırdığını söyledi. FudModule kök kiti, ESET ve AhnLab tarafından Ekim 2022'de rapor edildiği gibi, enfekte edilmiş ana bilgisayarlardaki tüm güvenlik çözümlerinin izlenmesini engelleyebilen bir "Getir Kendi Kırılgan Sürücüsü" (BYOVD) saldırısı aracılığıyla bütün güvenlik çözümlerinin izlenmesini engelleyebilen bir FudModule kök kiti kullanarak yetenekli olduğu bildirildi. En son saldırıyı önemli kılan şey, "hedef makinede zaten yüklü olan bir sürücüde zero-day kullanarak BYOVD'yi aşan" olmasıdır. Bu hassas sürücü, uygulama kontrolünden sorumlu bir Windows bileşeni olan AppLocker'ın işlevselliği için önemlidir. Lazarus Grubu tarafından hazırlanan gerçek dünya istismarı, appid.sys sürücüsündeki CVE-2024-21338'i kullanarak tüm güvenlik kontrollerini atlatan ve FudModule kök kiti'ni çalıştıran keyfi kodu yürütmeyi içerir. "FudModule yalnızca

Lazarus'un kötü amaçlı yazılım ekosisteminin geri kalanına gevşek bir şekilde entegre edilmiştir ve Lazarus'un kök kitiyi kullanma konusunda çok dikkatli olduğu ve kök kitiyi sadece uygun koşullar altında talep üzerine dağıttığı görülüyor," dedi güvenlik araştırmacısı Jan Vojtěšek, kötü amaçlı yazılımın aktif olarak geliştirildiğini tanımladı. Daha fazla algılama önlemek için adım atan FudModule, sistem günlüklerini devre dışı bırakmanın yanı sıra belirli güvenlik yazılımlarını da kapatmak için tasarlanmıştır, örneğin AhnLab V3 Uç Nokta Güvenliği, CrowdStrike Falcon, HitmanPro ve Microsoft Defender Antivirus (önceki adıyla Windows Defender). Bu gelişme, Kuzey Koreli hacker grupları ile ilişkilendirilen yeni bir teknik sofistike düzeyini işaret ediyor ve onların izlenmesini daha zor hale getirmek için karmaşık tekniklerin kullanıldığını gösteriyor. Siber Güvenlik Bu karşıt kolektifin çapraz platforma odaklanması, Apple macOS sistemlerine zararlı yazılımların sessizce yüklenmesi için sahte takvim toplantısı daveti bağlantılarını kullanarak bilgisayar korsanlarının kapsamını da göstermektedir, bir kampanya daha önce SlowMist tarafından Aralık 2023'te belgelenmiştir. "Lazarus Grubu, en yaygın ve en uzun süreli ileri kalıcı tehdit aktörlerinden biri olarak kalmaya devam ediyor," Vojtěšek dedi. "FudModule kök kiti, Lazarus'un arsenali içinde tuttuğu en karmaşık araçlardan biri olarak son örneği oluşturuyor." Detaylar için tıklayınız.

WordPress LiteSpeed Eklenti Açığı, 5 Milyon Siteyi Tehlikeye Atıyor

WordPress için LiteSpeed Cache eklentisinde bir güvenlik açığı açıklanmıştır ve bu, kimliği doğrulanmamış kullanıcıların yetkilerini yükseltmelerine olanak tanıyabilir. CVE-2023-40000 olarak izlenen bu güvenlik açığı, Ekim 2023'te 5.7.0.1 sürümünde çözülmüştür. Bu açık, kullanıcı girişi temizlenmediğinde ve çıktı kaçırmadığında ortaya çıkar ve varsayılan kurulumda bulunan update_cdn_status() adlı bir işlevde köklüdür. LiteSpeed Cache eklentisi, site performansını artırmak için kullanılır ve beş milyondan fazla kuruluma sahiptir. En son sürümü 6.1'dir ve 5 Şubat 2024'te yayımlanmıştır. Bu güvenlik açığı, Wordfence'in aynı eklentide başka bir XSS açığı (CVE-2023-4372, CVSS puanı: 6.4) keşfetmesinden dört ay sonra ortaya çıkar. CVE-2023-40000, yetkisi olan

saldırganların enjekte edilmiş bir sayfaya eriştiğinde her bir kullanıcının bir enjekte sayfaya eriştiğinde yürütülecek olan keyfi web komut dosyalarını enjekte etme olasılığını mümkün kılar. Detaylar için tıklayınız.

Change Healthcare Saldırısında 22 Milyon Dolarlık Bitcoin Ödemesi Yapıldı

Change Healthcare'i hedef alan fidye yazılımı saldırısında 22 milyon dolarlık bir ödeme yapıldığı ortaya çıktı. Söz konusu ödeme, Bitcoin'in blok zincirinde görülebilir ve saldırının en kötüsü olarak biliniyor. Ransomware saldırısı, ABD genelindeki eczaneleri felç etti ve 10 gün boyunca reçeteli ilaçların dağıtımında ciddi aksamalara yol açtı. Fidye yazılımı saldırganlarından birinin ortağı, saldırının arkasındaki hacker grubu olan AlphV veya BlackCat'in 22 milyon dolarlık bir ödeme aldığını belirtti. AlphV'ye bağlı bir Bitcoin adresi, 1 Mart'ta tek bir işlemde 350 Bitcoin aldı ve bu da o tarihte kurlara göre yaklaşık 22 milyon dolar ediyor. Change Healthcare'in, 22 milyon dolarlık fidyeyi ödemiş olabileceği iddia ediliyor ancak şirket bu konuda açıklama yapmaktan kaçınıyor. Ransomware ödemeleri, hem sorumlu gruplar tarafından gelecekteki saldırıları finanse eder hem de diğer fidye yazılımı saldırganlarına aynı taktiği denemeleri gerektiğini ima eder. Saldırganların bir ortağı olan "notchy" isimli kişi, AlphV'nin 22 milyon dolarlık fidyeyi tahsil ettiğini ve bu parayı ortaklarıyla paylaşmadığını iddia etti. Bu ödeme, sağlık endüstrisinde giderek artan fidye yazılımı saldırılarının tehlikeli bir örneğini temsil ediyor ve sektörün hedef alınabilirliğini artırıyor. Ödenen fidye miktarı dikkate değer bir kazanç sağlarken, AlphV'nin karanlık web siteleri ve şifreleme anahtarları aracılığıyla saldırılarına devam etme ihtimali endişe verici. Saldırının ardından, AlphV'nin karanlık web sitesi kayboldu ve şirketlerin verilerini çalmaya devam edip etmeyeceği belirsizliğini koruyor. Detaylar için tıklayınız.

Şüpheli Çinli Hackerlar Tarafından En Büyük Tayvan Telekomu Saldırıya Uğradı

Tayvan Savunma Bakanlığı, Tayvan'ın en büyük telekom şirketi olan Chunghwa Telecom'un siber güvenliğini iyileştirmesi için çağrıda bulunuyor. Bu çağrı, hükümetle ilgili bilgilerin de dahil olduğu bir veri ihlali sonrasında yapıldı. Söz

konusu hackerlar, Çin hükümeti tarafından desteklendiği düşünülen 1.7 TB veri çalmayı başardılar ve tüm bilgileri Kara Web'de satışa sundular. Savunma Bakanlığı, 1 Mart'ta AFP haber ajansına verdiği açıklamada ihlali doğruladı ve Chunghwa Telecom'un hassas bilgilerinin elde edildiğini ve Kara Web'de satıldığını belirtti. İlk analizlere göre, hackerlar Chunghwa Telecom'un hassas bilgilerini elde etti ve bunlar arasında silahlı kuvvetler, dışişleri bakanlığı, sahil güvenlik ve diğer birimlere ait belgeler bulunuyor. Savunma Bakanlığı, gizli bilgilerin sızdırılmadığını belirtirken, yüklenici firmanın bilgi güvenliğini güçlendirmesi için çağrıda bulundu. Bu olay, Tayvan'ın siber güvenliğini tehdit eden ve hükümetle ilişkili hassas bilgilerin tehlikeye girmesine neden olan Çin tarafından desteklenen hacker gruplarının artan tehdidini gösteriyor. Detaylar için tıklayınız.

SİBER GÜVENLİK TRENDLERİ

2024'te Dikkat Edilmesi Gereken 20 Yükselen Siber Güvenlik Trendi

Dijital tehditlerin manzarası, son birkaç on yılda teknolojik ilerlemeler ve dünyamızın dijital bağlantılılığı tarafından derin bir dönüşüm geçirdi. Toplumumuzun iletişim, ticaret ve kritik altyapı için giderek daha fazla dijital teknolojiye güvenmesiyle birlikte, tehdit manzarası karmaşıklık ve sofistikasyon bakımından evrim geçirdi. Bu detaylı inceleme, değişen dijital tehdit manzarasının çeşitli yönlerine derinlemesine bakacak, temel karakteristiklerini, ortaya çıkan trendlerini ve bireyler, kuruluşlar ve hükümetler için karşılaşılan zorlukları inceleyecektir.

1. **Artan Sofistike Saldırılar:**
    - Siber saldırganlar, güçlü hackleme araçlarının bulunabilirliği ve devlet destekli grupların yükselişi gibi faktörlerle daha sofistike saldırılar gerçekleştiriyorlar.
2. **Çeşitli Saldırı Vektörleri:**
    - Kötü amaçlı yazılım, fidye yazılımı ve DDoS saldırıları gibi çeşitli vektörlerle saldırganlar hedeflerine ulaşıyorlar.
3. **Hedef Çeşitliliği:**
    - Artık büyük şirketlerin ve devlet kurumlarının yanı sıra, küçük işletmeler, sağlık kuruluşları ve bireyler de hedef haline geliyor.
4. **Devlet Aktörleri:**
    - Devlet destekli gruplar, siber savaş ve casusluk faaliyetleri yürüterek dijital tehdit manzarasına yeni bir boyut kazandırıyorlar.
5. **Tedarik Zinciri Saldırıları:**

- Tedarik zinciri saldırıları, ürün ve hizmetlerin bütünlüğünü tehlikeye atarak organizasyonları ve müşterilerini etkileyebiliyor.

6. **IoT Güvenlik Açıkları:**
   - IoT cihazlarının yaygınlaşması, dijital tehdit ortamında yeni zafiyetlerin ortaya çıkmasına neden oluyor.
7. **Saldırılarda Yapay Zeka ve Makine Öğrenimi:**
   - Saldırganlar, yapay zeka ve makine öğrenimini kullanarak saldırılarını otomatikleştiriyorlar ve daha etkili hale getiriyorlar.
8. **Düzenleyici ve Uyum Zorlukları:**
   - Değişen tehdit manzarası, hükümetleri ve düzenleyici kurumları yeni siber güvenlik düzenlemeleri getirmeye zorluyor.
9. **Yanıt ve Dayanıklılık:**
   - Kuruluşlar, saldırıları önlemeye, tespit etmeye ve etkilerini azaltmaya odaklanarak etkili bir olay yanıtı ve dayanıklılık stratejisi oluşturmalıdır.

Top 20 Siber Güvenlik Trendleri Özeti: Bu trendler arasında, yapay zeka ve makine öğreniminin siber güvenlikteki rolü, Zero Trust Mimarisi'nin (ZTA) yükselişi, kuantum hesaplama dirençli şifreleme, bulut güvenliğinin evrimi, 5G ağ güvenliği, IoT güvenliği, tedarik zinciri güvenliği, biyometrik ve davranışsal kimlik doğrulama, siber güvenlik işgücünün geliştirilmesi, insana odaklı güvenlik ve otomatik tehdit avı yer alıyor.

Detaylar için tıklayınız.

En İyi 10 Siber Güvenlik Trendi

Günümüzdeki siber güvenlik alanında yaşanan önemli gelişmeleri ve organizasyonlar için olası riskleri vurgulamaktadır. Uzaktan çalışmanın artması, IoT cihazlarının yaygınlaşması, fidye yazılımlarının yükselişi gibi konular, güvenlik uzmanlarının ve organizasyon yöneticilerinin dikkate alması gereken temel noktalardır.

Özellikle, pandeminin etkisiyle evden çalışma modeline geçişin hızlanması, siber güvenlik açıklarının artmasına neden olmuştur. Aynı şekilde, bulut hizmetlerinin kullanımının yaygınlaşması da yeni tehditler ortaya çıkarmıştır. Sosyal mühendislik saldırıları ve mobil cihazlara yönelik tehditler ise siber suçluların daha sofistike hale geldiğini ve her türlü cihazı hedef alabileceklerini göstermektedir.

Bu gelişmeler ışığında, organizasyonlar veri gizliliğine daha fazla önem vermeli, çok faktörlü kimlik doğrulamayı güçlendirmeli ve yapay zeka gibi teknolojileri güvenlik altyapılarında kullanmalıdır. Mobil cihazların kullanımının artmasıyla birlikte, mobil güvenlik önlemleri de gözden geçirilmeli ve güçlendirilmelidir.

Sonuç olarak, bu açıklama, güncel siber güvenlik trendlerini ve organizasyonların bu trendlere nasıl tepki verebileceğini vurgulamaktadır. Güvenlik bilincinin artırılması ve uygun önlemlerin alınması, siber tehditlere karşı daha etkili bir koruma sağlayabilir.

1. **Uzaktan Çalışma Siber Güvenlik Riskleri**: Covid-19 pandemisi, birçok organizasyonun iş gücünü hızla uzaktan çalışmaya geçirmesine neden oldu. Evden çalışma, merkezi ofislere göre daha az korunaklı olduğundan yeni siber güvenlik riskleri doğurmuştur.

2. **Nesnelerin İnterneti (IoT) Evrimi**: IoT cihazlarının kullanımı arttıkça, siber suçlar için yeni fırsatlar ortaya çıkmıştır. Bu cihazlar genellikle daha az korumalıdır ve saldırganlar için potansiyel hedefler oluşturur.
3. **Fidye Yazılımlarının Yükselişi**: Fidye yazılımları giderek artmakta ve pandemi döneminde hızla yayılmıştır. Kuruluşlar verilerinin şifrelenmesi ve fidye ödenmesi gibi zor durumlarla karşı karşıya kalmıştır.
4. **Bulut Hizmetlerinde Artış ve Bulut Güvenlik Tehditleri**: Bulut hizmetlerinin hızla benimsenmesi, organizasyonlar için güvenlik risklerini artırmıştır. Yanlış yapılandırılmış bulut ayarları ve hesap kaçırma gibi tehditler önemli bir endişe kaynağıdır.
5. **Sosyal Mühendislik Saldırıları**: Uzaktan çalışma eğilimi, sosyal mühendislik saldırılarını artırmıştır. Phishing, SMS phishing, voice phishing gibi yöntemlerle siber saldırganlar çalışanları hedef almaktadır.
6. **Veri Gizliliği**: Veri gizliliği artık ayrı bir disiplin olarak kabul edilmekte ve organizasyonlar için yasal zorunluluk haline gelmektedir.
7. **Çok Faktörlü Kimlik Doğrulamanın İyileştirilmesi**: MFA, kimlik doğrulamanın altın standartıdır ancak SMS veya telefon aramalarıyla yapılan doğrulamalar güvenlik açıkları içerebilir.
8. **Yapay Zekanın (AI) Devam Ederek Yükselmesi**: Yapay zeka, siber güvenlik altyapısını geliştirmek için giderek daha fazla kullanılmaktadır.
9. **Mobil Siber Güvenliğin Ön Plana Çıkması**: Uzaktan çalışma eğilimi, mobil kullanımı artırmaktadır ve bu da mobil tehditlerin çeşitlenmesine neden olmaktadır.

Bu trendler, siber güvenlik alanında dikkate alınması gereken önemli konuları kapsamaktadır. Organizasyonlar, bu trendlere karşı önlemler alarak güvenliklerini sağlamlaştırmalıdır. Detaylar için tıklayınız.

2024 Yılının En Büyük 10 Siber Güvenlik Trendi Şimdilik Herkes Hazır Olmalı

Bu bölümde, siber güvenliğin bireysel, kurumsal ve devlet düzeyinde stratejik bir öncelik olarak ele alınması gerekliliğine vurgu yapılmaktadır. Ayrıca, yapay zeka (AI) teknolojisinin saldırı ve savunma alanında dönüştürücü bir etkisi olacağı ve bu etkinin burada ele alınan her trendde hissedileceği belirtilmektedir.

Teknolojik gelişmelerin hızlanmasıyla birlikte siber tehditlerin de arttığına dikkat çekilmektedir. Bu durum, gelecek hakkında bilgilendirilmenin önemini vurgulamakta ve okuyucuların 2024'e girerken dikkat etmesi gereken siber güvenlik trendlerini açıklamaktadır.

- **Siber Güvenlik Yeteneklerindeki Kriz:** Siber saldırılara karşı organizasyonları koruyacak yeteneklere sahip profesyonellerin eksikliği, 2024 boyunca devam eden bir tema olacaktır. Bu durumun düzeltilmesi için maaşlarda artış, eğitim ve geliştirme programlarına daha fazla yatırım gibi çabalar beklenmektedir.
- **Yapay Zeka Tabanlı Saldırılar ve Savunma:** AI'nin hızla gelişmesi, daha sofistike ve akıllı AI tabanlı saldırıların ortaya çıkmasını sağlayacaktır. Aynı zamanda, gerçek zamanlı anormallik tespiti, akıllı kimlik doğrulama ve otomatik olay yanıtı gibi özelliklerle tehditleri tespit etme veya etkisiz hale getirme konusunda da yardımcı olacaktır.
- **Daha İleri Seviye Phishing Saldırıları:** Kullanıcıları sistemlere erişim sağlamak için kandırmayı içeren sosyal mühendislik saldırıları, daha sofistike hale gelecektir. Bu saldırılara karşı organizasyon genelinde farkındalık ve eğitim önlemleri alınması beklenmektedir.
- **Siber Güvenlik Kurullarda Gündemde:** 2024'te siber güvenlik, artık IT departmanında izole edilemeyen stratejik bir öncelik haline

gelmektedir. Bu durum, organizasyonların reaktif savunma stratejilerinden uzaklaşmasını sağlayacak ve yeni iş fırsatlarına hazırlıklı olmalarını sağlayacaktır.

- **IoT Siber Saldırılar:** Daha fazla cihazın internete bağlanması, siber saldırganlar için daha fazla potansiyel giriş noktası demektir. Evden çalışma devrimi devam ettikçe, güvenli olmayan cihazlar üzerinden veri paylaşımının ve bağlantısının riskleri devam edecektir.
- **Siber Direnç - Siber Güvenlikten Daha Fazlası:** Siber direnç, siber saldırıları önlemenin ötesine geçmeyi amaçlar. En iyi güvenliğin bile %100 koruma sağlayamayacağı gerçeğinden yola çıkarak, operasyonların devamlılığını sağlamayı amaçlar.
- **Sıfır Güven'den Daha Azı:** Sıfır güven kavramı, sistemler karmaşık hale geldikçe ve güvenlik iş stratejisinin bir parçası haline geldikçe evrilecektir. 2024'te, sıfır güven, sürekli AI destekli gerçek zamanlı kimlik doğrulama ve faaliyet izlemeyle desteklenen adaptif ve bütünsel bir yaklaşıma dönüşecektir.
- **Siber Savaş ve Devlet Destekli Siber Saldırılar:** Ukrayna'daki savaş, devletlerin askeri ve sivil altyapıya karşı siber saldırıları ne kadar istekli ve yetenekli bir şekilde gerçekleştirebildiklerini gözler önüne sermiştir. Bu tür saldırılar, askeri operasyonlarla birlikte gerçekleşmeye devam edecektir.
- **Siber Güvenlik Düzenlemeleri:** Devletler ve organizasyonlar, siber tehditlerin ulusal güvenlik ve ekonomik büyüme üzerindeki risklerini giderek daha fazla fark etmektedirler. Büyük ölçekli veri ihlallerinin potansiyel toplumsal ve siyasi sonuçları, siber güvenlik konularında yeni düzenlemelerin ortaya çıkmasında önemli bir faktördür.

Detaylar için tıklayınız.

Bir Sonraki Siber Salgının Önlenmesine Yönelik Öneriler

Gerçek Zamanlı Önleme: Siber güvenlikte, enfeksiyonu önlemek için aşı yapmak, tedavi etmekten daha etkilidir. Bu nedenle, gerçek zamanlı önleme, bir kuruluşu gelecekteki siber salgınlara karşı savunmak için daha iyi bir konuma getirir. Bilinmeyen, zero-day tehditlerini önlemeye odaklanan kuruluşlar, siber güvenlik savaşını kazanabilirler. Bu tür tehditler, işletmeler için ciddi riskler oluşturur ve genellikle engellenmesi en zor olanlardır.

Her Şeyi Güvence Altına Alma: COVID-19 yanıtı sırasında ortaya çıkan yeni normlar, ağ altyapısının, işlemlerinin ve bağlı mobil cihazların uyumluluğunun kontrol edilmesini gerektirir. Bulut kullanımının artması, özellikle çoklu ve hibrit bulut ortamlarında iş yüklerini, konteynerleri ve sunucusuz uygulamaları güvence altına almak için artan bir güvenlik düzeyi gerektirir.

Konsolidasyon ve Görünürlük: Şirket altyapısında dramatik değişiklikler, güvenlik yatırımlarını değerlendirmek için bir fırsat sunar. Yüksek düzeyde görünürlük, ağ varlıklarının tamamına erişimi garanti eder ve sofistike siber saldırıları önlemek için gereken güvenlik etkinliğini sağlar. Bu, nokta çözümlerinin ve satıcıların azaltılmasıyla ve genel maliyetlerin azaltılmasıyla mümkündür.

Mutlak Sıfır Güvenlik: Siber tehditler, güvenlik çeperinin içinde ve dışında var olduğundan, Sıfır Güvenlik yaklaşımının benimsenmesi zorunludur. Bu yaklaşım, hiçbir cihazın, kullanıcının, iş yükünün veya sistemin varsayılan olarak güvenilir olmamasını öngörür.

Tehdit İstihbaratını Güncel Tutma: Kötü amaçlı yazılımlar sürekli olarak evrim geçiriyor, bu nedenle tehdit istihbaratı her şirketin göz önünde

bulundurması gereken bir araç haline geliyor. Tehdit istihbaratı, birden çok kaynaktan gelen bilgileri birleştirerek ağ için daha etkili bir koruma sağlar. Sıfır gün saldırılarını önlemek için gerçek zamanlı tehdit istihbaratına ihtiyaç vardır.

- Uzaktan çalışma sırasında çalışanlara yönelik siber zorbalığı önlemek amacıyla işyeri politikaların geliştirilmesi, tüm çalışanların bu politikalardan haberdar olması ve kurallara uymasının sağlanması,
- COVID-19 pandemi sürecinde artabilecek olan kişisel ve kurumsal verilerin ele geçirilmesine yönelik siber saldırıları önlemek amacıyla ek idari tedbirlerin uygulanması,
- Çalışanlara yönelik siber zorbalık risk faktörlerinin uzmanlarla birlikte değerlendirilmesi,
- Çalışanlara, hizmet verdikleri bireylerden gelebilecek olan düşmanca tutum ve çatışmaları çözümleyebilecekleri eğitimlerin verilmesi,
- Uzaktan çalışmanın fiziksel ve ruhsal yönden olumsuz etkileri ve bunlarla baş edebilme yöntemleri konusunda çalışanlara eğitimlerin verilmesi,
- Siber zorbalığı önlemek için ulusal eylem planları oluşturulması,
- Bu alanda çalışmalar yapmak isteyen araştırmacılara için çalışma hayatında siber zorbalığa ilişkin yayın türlerini, dillerini ve indekslerini genişleterek kapsamlı analizler yapmaları önerilebilir.

Kaynakça / Referanslar:

1-https://cyberartspro.com/

2-https://www.simplilearn.com/top-cybersecurity-trends-article

3-https://www.kaspersky.com/resource-center/preemptive-safety/cyber-security-trends

4-https://www.forbes.com/sites/bernardmarr/2023/10/11/the-10-biggest-cyber-security-trends-in-2024-everyone-must-be-ready-for-now/