Çocuklar İçin Siber Güvenlik Eğitimi

Abdurrahim SARGIN

ŞANLIURFA AR-GE
URFA STEM

Çocuklar İçin Siber Güvenlik Eğitimi
Abdurrahim SARGIN

Kapak ve İç Tasarım
Mehmet NİŞANCI

Urfa STEM ve Bilim Merkezi
Şanlıurfa İl Milli Eğitim Müdürlüğü

ISBN
978-605-06822-2-9

Hamidiye Mah. 264. Sk. No:13
Haliliye/ŞANLIURFA
(0414) 314 52 99

urfastem@gmail.com
www.urfastem.gov.tr

Abdurrahim SARGIN

Konya ilinin Akşehir ilçesinde doğmuştur. İlk ve ortaöğrenimini Konya ilinde tamamlayarak 2009 yılının başladığı Selçuk Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği Bölümünü 2013 yılında tamamlamıştır. 2014 yılında Şubat ayında Şanlıurfa'nın Karaköprü ilçesinde yer alan Karaköprü Ortaokulu'na atanmıştır ve halen kadrosu bu okulda bulunmaktadır. 2015 yılında Selçuk Üniversitesi Mühendislik ve Mimarlık Fakültesi Bilgisayar Mühendisliği'ni bitirmiştir. Halen Şanlıurfa İl Milli Eğitim Ar-Ge bünyesinde öğretmenlik görevine devam etmektedir. 2016 yılından itibaren STEM Eğitimi ve Gelişen Teknoloji Eğitimlerine ilgi duyan ve bu eğitimleri veren yazarımız evli ve bir kız çocuğu babasıdır.

TEŞEKKÜR

Beni bugüne getiren başta ailem olmak üzere, her zaman desteğini hissettiğim çok kıymetli eşime ve varlığıyla gülümsememizi her dem var eden kızıma teşekkür ederim. Bir öğretmen olarak duam bize nasip olan gönül işi eğitimin bizden sonra kızım ve manevi evlatlarım kabul ettiğim tüm öğrencilerim ile büyüyerek ülkemizin büyümesine katkı sağlaması…

Bu kitabımızın oluşturulmasında emeği geçen başta Bu kitabın basılmasında ve Şanlıurfa İl Milli Eğitim Müdürümüz Sayın İsmail YAPICIER'e, İl Milli Eğitim Ar-Ge birimi koordinatörü Veysel ÖNCÜL'e ve mesai arkadaşlarıma, kitabın dizgi ve tasarımına katkı sunan ve sanatsal çalışmalarıyla ilimize renk katan Mehmet NİŞANCI'ya, pilot etkinlik ve çalışmaların yapılmasında büyük imkanlar sağlayan ve fikirleriyle kitabı zenginleştiren Şanlıurfa STEM ve Bilim Merkezi Koordinatörü Halil İbrahim ÇETİN'e ve çok değerli GENÇ STEM derneği üyelerine teşekkür ederim.

Abdurrahim SARGIN
Siber Güvenlik ve
STEM Eğitmeni

TAKDİM

Ülkeler arası dijital rekabetin resmi adı olarak literatürde bulunan Siber güvenlik, sanal dünyada oluşan bir tehdit gibi lanse edilse de aynı zamanda hızlı ve etkili bir şekilde problem çözmeye yarayan etkili bir silahtır. Siber güvenlik ülkelerin internet veya ağ altyapılarından ağ yazılımlarına kadar ve kişisel yapıların internet erişimine kadar birçok katmanında meydana gelebilecek sızma girişimlerinin ve kötü amaçlı kullanım senaryolarıyla dolu bir yapıdır. Güvenlik yapısı bunları nasıl koruyabilirim sorusuna cevap ararken, saldırı kavramı da bir başka yapıyı nasıl devre dışı bırakabilirim sorusuna cevap arar. Bu anlamda bu eğitimin ne kadar önemli olduğu konusu da ön plana çıkmaktadır.

Siber Saldırılar ve savaşlar günümüzde ülkeler arası rekabet yapılan en popüler alanlardan bir tanesidir. Ülkeler siber ordu yapılarını kurarak bu atakları bertaraf etmekte veya siber saldırılar ile karşı tarafın direncini kırarak hizmet aksamasına veya sistemin çökmesini sağlayacak saldırılar gerçekleştirmektedir.

Siber saldırı tanım olarak siber suçluların veya ülkelerin iyi amaçlı veya kötü amaçlı, bir veya daha fazla bilgisayarı tek veya birden fazla bilgisayara veya ağa karşı kullanarak başlattığı bir saldırıdır. Siber saldırı, bilgisayarları kötü amaçlı olarak devre dışı bırakabilir, veri çalabilir veya ihlal edilen bir bilgisayarı diğer saldırılar için bir başlangıç noktası olarak kullanabilir.

Öğrencilerimiz bu kitap sayesinde iyi niyetli yazılımlar ile kötü niyetli yazılımları ayırt edebilecekler. Kişisel verilerini koruyabilecekleri gibi ülkemiz için de önemli olan bir yapı olan siber güvenliği sağlayarak saldırıları engelleyebileceklerdir. Bu eğitimin ne kadar önemli olduğunu ve bütün bireylerin minimum düzeyde de olsa bilmesi gereken yapıları kavramalarını sağlayacak olan kitabımızı okumanızı ve içindeki etkinlikleri dikkatlice gerçekleştirmenizi diliyorum.

İSMAİL YAPICIER
Şanlıurfa İl Milli Eğitim Müdürü

İÇİNDEKİLER

SİBER GÜVENLİK KAVRAMI

İnternet herkes için doğru ve yanlış bilgilerin tamamının bulunduğu en geniş kaynak ve platformdur. Sanal ortamda perde arkasında kimin ve neyin gizlendiğinin farkında değilseniz son derece tehlikelidir. İnternet ortamı özgürlüğün kısıtlanmadığı bir alan olduğu için kişiler kendilerini rahat hissederler. Bu rahatlık avantaj olabileceği gibi bazı bilgilerin kolaylıkla verildiği veya girildiği için dezavantajlı da bir durumdur. "Siber" kelimesi bilgi teknolojisi (IT), yani bilgisayarlar ile bir ilişkiyi belirtir. Siber kavramı günümüzde modern bilişim çağında geliştirilen teknolojileri kapsamaktadır. Siber güvenlik, ağları, aygıtları, programları ve verileri saldırı, hasar veya yetkisiz erişime karşı korumak için tasarlanmış teknolojiler, süreçler ve uygulamalardan oluşur. Siber güvenlik bilgi teknolojisi güvenliği olarak da adlandırılabilir.

Siber güvenlik önemlidir. Çünkü hükümet, askeri, kurumsal, finansal ve tıbbi kuruluşlar bilgisayarlarda ve diğer cihazlarda benzeri görülmemiş miktarda veri toplar, işler ve depolar. Bu verilerin önemli bir kısmı, fikri mülkiyet, finansal veriler, kişisel bilgiler veya yetkisiz erişim veya maruziyetin olumsuz sonuçlara yol açabileceği diğer veri türleri olsun hassas bilgiler olabilir. Kuruluşlar, hassas verileri iş yaparken ağlara ve diğer cihazlara iletir ve siber güvenlik, bu bilgileri ve bunları işlemek veya depolamak için kullanılan sistemleri korumaya adanmış disiplini tanımlar.

İlk solucan programı 1986 yılında bir yazılım programcısı tarafından yazılmıştır. Solucan programı internete bağlı sistemleri kapatmak için kullanıldı. Yine 1994 yılında, 100 bilgisayara ve banka hesabına yasadışı erişim nedeniyle iki grup tutuklandı. Siber güvenliğin tarihi başlangıçta bir araştırma projesi olarak başladı, Bob Thomas'ın ARPANET'in terminalleri arasında hareket etmek için bir "Creeper" tasarlamasıyla Ray Tomlinson'un "Reaper" adlı benzer bir programı (antivirüs yazılımına benzer) kopyalamasıyla başladı.

Temel olarak, toplumumuz her zamankinden daha teknolojik olarak bağımlıdır ve bu eğilimin yavaşlayacağına dair bir işaret yoktur. Kimlik hırsızlığına neden olabilecek kişisel veriler artık sosyal medya hesaplarımızda kamuya açıklanmaktadır. Sosyal güvenlik numaraları, kredi kartı bilgileri ve banka hesabı bilgileri gibi hassas bilgiler artık gmail, hotmail gibi mail araçlarında diğer bütün dosya yapılarımız ise dropbox veya google

Resim 1: Siber Güvenlik Kavramları

drive gibi bulut depolama hizmetlerinde saklanıyor.

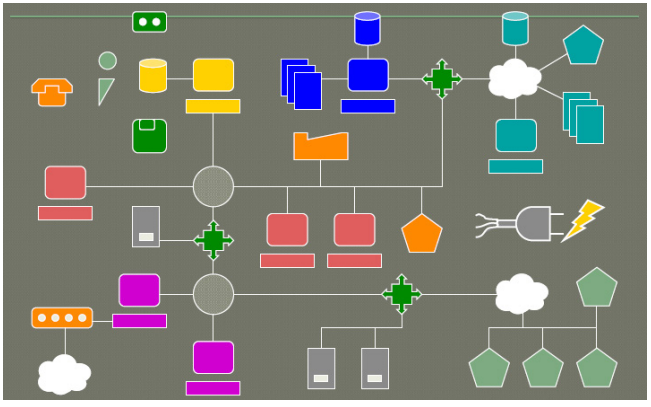
Temel siber güvenlik kavramlarını şu şekilde sıralayabiliriz:

- Ağ Güvenliği
- Bulut Güvenliği
- Sosyal Medya Güvenliği
- Web Sitesi Güvenliği
- Uygulama Güvenliği
- Virüsten koruma / kötü amaçlı yazılımdan koruma
- Veri Kaybını Önleme (DLP)
- Saldırı Tespit Sistemleri (IDS) veya Saldırı Önleme Sistemleri (IPS)
- Kimlik ve Erişim Yönetimi (IAM)
- Kriptografi Uygulamaları

Siber güvenlikteki en zor sorun güvenlik risklerinin sürekli gelişen doğasıdır. Geleneksel olarak kuruluşlar ve hükümetler yalnızca en önemli sistem bileşenlerini korumak ve bilinen muamelelere karşı savunma yapmak için siber güvenlik kaynaklarının çoğunu ağ ve çevre birimleri güvenliğine odaklamışlardır. Günümüzde tehditler kuruluşların ayak uydurabileceğinden daha hızlı ilerlediği ve değiştiği için bu yaklaşım yetersizdir. Sonuç olarak danışma kuruluşları siber güvenliğe daha proaktif ve uyarlanabilir yaklaşımları teşvik eder. Benzer şekilde Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), risk değerlendirme çerçevesinde sürekli izleme-

ye doğru bir geçişi tavsiye eden yönergeler yayınladı. Gerçek zamanlı değerlendirmeler, geleneksel çevre tabanlı modelin aksine güvenliğe yönelik veri odaklı bir yaklaşım bu yönergenin temelini oluşturmaktadır.

Günümüzde farklı cihazların içerisinde bulunduğu ve farklı topoloji yani yerleşim planlarına ve özelliklerine sahip geniş bir ağ var ki bu ağın kontrolü ve güvenliği her geçen dakika zorlaşıyor. Bu geniş ağa eklenen cihazların kontrolünün olmaması en büyük tehdit olarak görünmektedir. Bilinen cihazları kullanan kötü amaçlı kullanıcılar da asıl tehdit unsuru olarak göze çarpmaktadır. Yapılması gereken şeylerin başında ise her kişi minimum düzeyde güvenlik ve kontrol standartlarını bilmesi ve cihazlarının yönetimini gerçekleştirmesidir. Bu sebepten siber güvenlik kavramı bireyselleştirilmiş bir yapıya doğru evrilmekte olup ülke güvenliğini sağladıktan sonra kişilerin kendilerini korumaya geçmesi için önem kazanmaktadır. Örnek olarak modern ağların karmaşıklığını gösteren görselimizi inceleyebilirsiniz.



Resim 2: Modern Ağların Genişliği

Etkili bir siber güvenlik için, bir kuruluşun tüm bilgi sistemi boyunca çabalarını koordine etmesi gerekir. Siber unsurlar aşağıdakilerin tümünü kapsar:

Resim 3: Siber Unsurlar

- Ağ güvenliği: Ağı istenmeyen kullanıcılardan, saldırılardan ve izinsiz girişlerden koruma sürecini kapsar. Ağda bulunan kablolardan modemlere kadar bilgi hırsızlığını önleyici birçok tedbir alınmalıdır.

- Uygulama güvenliği: Uygulamalar kullanıcıların birebir muhatap olduğu ve etkin bir şekilde kullandığı yapılardır. Bu programların saldırılara karşı güvenli olduğundan emin olmak için sürekli güncelleme ve test yaparak güvenlik açıklarını gidermesi ve uzaktan bir erişimi engellemesi gerekmektedir.

- Uç nokta güvenliği: Uzaktan erişim, yakından yapılamayan bir işin gerekli bir parçasıdır. Ancak veriler için zayıf bir nokta da olabilir. Uç nokta güvenliği, bir şirketin ağına uzaktan erişimi koruma sürecidir. Kendi personellerine uzaktan erişim yetkisi vererek bir başkasının sisteme sızmasını engelleyici yapıları içermektedir.

- Veri güvenliği: Ağların ve uygulamaların içi veridir. Şirket ve müşteri bilgilerini korumak ve arada dolaşan verilerin korunmasını sağlayan ayrı bir güvenlik katmanıdır.

- Kimlik yönetimi: Kimlik yönetimi bir organizasyonda her bireyin sahip olduğu erişimi anlama sürecidir. Kimliğini gizleyen kötü amaçlı kişilerden sistemlerin korunması ana konusudur.

• Veritabanı ve altyapı güvenliği: Bir ağdaki her şey veritabanları ve fiziksel ekipman içerir. Arka planda verilerin depolandığı yapıların korunması ve internet altyapılarının güvenliğinin sağlanması ana konularındandır.

• Bulut güvenliği: Çoğu dosya, dijital ortamlarda veya "bulutta" bulunur. Verileri% 100 çevrimiçi ortamda korumak, çok sayıda zorluk sunar. Yakın zamanda genişleyecek bir depolama ortamı oluşacaktır. Kişisel dosyalarını bu ortamlarda tutacak olan kişilerin güvenliğini sağlamaları gerekmektedir.

• Mobil güvenlik: Cep telefonları ve tabletler günlük hayatımızda en çok kullandığımız cihazlardandır. Bilgilerimizin ve kişisel verilerimizin saklandığı bu ortamlarda dış ortamlardan gelebilecek zararlı her türlü girişime karşı korumayı sağlamaktadır.

• Afet kurtarma / iş sürekliliği planlaması: Bir ihlal durumunda, doğal afet veya diğer olay verileri korunmalı ve iş devam etmelidir. Böylece afete müdahale işlemi aksamamalıdır.

Siber güvenliği sağlarken yapılacak aşamalar standart olarak belirlidir. Bir döngü halinde yapılacakların sıra ve isimleri aynı olmasına karşın müdahale sistemi ve tespit sistemleri her saldırıya özgündür. Genel olarak siber güvenliği sağlarken sistemler sürekli güncel tutulmalıdır. Sürekli bir arama yapan ve sisteme yönelik saldırıları arayan yapı kurulmalıdır. Belirlenen saldırılara yönelik koruma işlemi gerçekleştirilmelidir. Burada dikkat edilecek yapı herhangi bir antivirüs veya güvenlik duvarı bütün virüslere karşı etki edemez. Spesifik yani özel bir virüs için onu yok edecek bir anti yapı kurulmalıdır. Sisteme yapılan kötü amaçlı yapılar tespit edilmelidir. Hangi amaçla sisteme atıldığı araştırılmalıdır. Sistemde yapacağı aksaklıklar belirlenerek önlenmelidir. Son olarak eğer dosya sistemine veya bilgi hırsızlığına yönelik bir saldırı gerçekleşmişse veri koruması yapılmalı ve kurtarmaya yönelik çalışmalar yapılmalıdır. Örneğin dosya sıkıştırma, şifre değişikliği ve yedekleme işlemleri gibi.

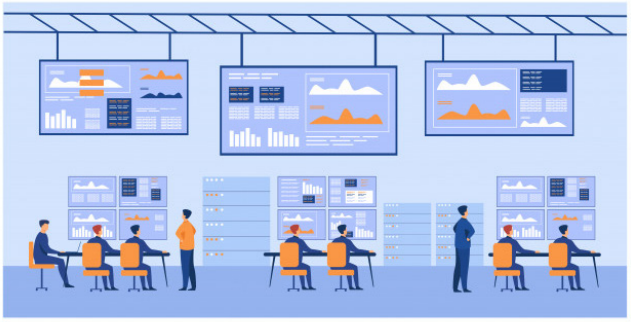
İlk adımda virüs veya kötü amaçlı bir yazılımın araması ve nereden bulaştığı konusunda tarama yapmak gereklidir. Koruma için neler gerekli hangi antivirüs veya yöntemle kötü amaçlı yazılımların engellenebileceği belirlenmelidir. Sızma girişimi veya kötü amaçlı yazılım tespit edilmeli ve hangi dosya veya yordam ile sızma olduğunu bilmeliyiz. Bu açık ileride aynı alandan giriş yapılabileceği hakkında da bilgi vermektedir. Karşılık verme aşamasında ise dosya veya kötü amaçlı yazılım tarafında çalışan yapılara karşı harekete geçilmelidir. Eğer sızma yolu tespit edilmişse aynı veya farklı yöntemlerle karşılığı verilmelidir. Olabildiğince veri karşı tarafa aktarılmadan veya zarar görmeden kurtarılma yoluna gidilmeli kötü amaçlı yazılımlardan temizlenmelidir. Bu aşama en basit bir virüsten tutun bütün sistemi ele geçirmeye çalışan bir kötü amaçlı yazılıma kadar hepsinde kullanılabilecek bir yapıdır.

Resim 4: Siber güvenlik çözüm döngüsü

SİBER GÜVENLİK NEDEN ÖNEMLİDİR?

Dünya teknolojiye her zamankinden daha fazla güveniyor. Sonuç olarak, dijital veri yaratımı artmıştır. Günümüzde işletmeler ve hükümetler bu verilerin büyük bir kısmını bilgisayarlarda depolamakta ve ağlar üzerinden diğer bilgisayarlara iletmektedir. Cihazlar ve bunların temel sistemleri, sömürüldüğünde bir kuruluşun sağlığını ve hedeflerini zayıflatan güvenlik açıklarına sahiptir.

Bir veri ihlali, herhangi bir işletme için bir dizi yıkıcı sonuç doğurabilir. Bir şirketin itibarını tüketici ve iş ortağı güveni kaybederek çözebilir. Kaynak dosyalar veya fikri mülkiyet gibi kritik verilerin kaybı, bir şirketin rekabet avantajına mal olabilir. Dahası, veri ihlali, veri koruma düzenlemelerine uyulmaması nedeniyle şirket gelirlerini etkileyebilir. Ortalama olarak, bir veri ihlalinin etkilenen bir kuruluşa 3,6 milyon dolar maliyeti olduğu tahmin edilmektedir. Medyada manşetlik yapan yüksek profile sahip veri ihlalleri ile kuruluşların güçlü bir siber güvenlik yaklaşımı benimsemesi ve uygulaması esastır.



Resim 5: Siber Güvenlik Neden Önemlidir?

Seçkin şirketler tarafından sürdürülenler de dahil olmak üzere, sözde güvenli sistemlerin son derece duyurulmuş ihlalleri, kişisel bilgilerinin ifşa olabileceği konusunda halka korku saldı. Bu olaylar aynı zamanda işletme sahipleri ve yöneticileri için bir siber olayın büyük kayıplara veya itibarın bozulmasına neden olabileceği konusunda endişeler yaratır. Bu durum siber güvenliği, alandaki liderlerin en son siber tehditlerin üstesinden gelmek için sürekli olarak yeni stratejiler

üzerinde işbirliği yaptığı giderek yaygınlaşan bir konu haline getiriyor.

Kimlik hırsızlığının alaka düzeyi ve ortaklığı artıyor ve bankalar, devlet kurumları, kredi sağlayıcıları ve sigorta şirketleri, bu maliyetli dijital soygun biçiminin gelgitini durdurmak için çabalıyorlar. İşletmeler, verileri çalan veya kritik dosyalara ve işletim sistemlerine erişimi engelleyen kimlik avı saldırıları, kötü amaçlı yazılım, fidye yazılımı ve sosyal mühendislik saldırıları ile giderek daha fazla karşılaşmaktadır. Siber güvenlik alanını gerekli kılan önemli endişelerden birkaçı:

• Gizlilik: Hem kurumsal veriler hem de müşteri verileri risk altındadır. Bilgisayar korsanları, kurumsal ticari sırlar ve araştırma verilerinden tüketici kimliği ve mali kayıtlara kadar pek çok türde özel dijital bilgiyi kötü niyetli olarak kullanabilir. Kimlik hırsızlığı, gasp, veri kaybı veya kritik operasyonel sistemlerin kapanmasıyla sonuçlanabilir. Bu tehditlere karşı koruma sağlamak için, veri depolayan herhangi bir kuruluş veri ağını uygun şekilde korumalıdır. Aksi takdirde kurumsal ve müşteri çıkarlarını riske atıyor olabilir.

• Veri merkezli ekonomi: Hassas veriler giderek artan miktarlarda depolanmaktadır. Dünya, nesnelerin interneti (IoT) cihazlarına veya verileri depolayabilen ve iletebilen birbirine bağlı akıllı cihazlara güveniyor. Birçok siber güvenlik uzmanına göre IoT(İnternet Of Things) cihazları, hükümet, fabrika, perakende ve kişisel uygulamalarda kullanılıyor ve cihaz sayısı 2023'e kadar 43 milyara yükselecektir. (Bu sebepten ötürü bilgisayarlarımızda internet kimliği olarak adlandırılan ipv4'ler yetişmeyecektir ve ipv6'ya geçiş tam anlamıyla sağlanacaktır.)

• Altyapı riski: Siber güvenlik tehditleri kritik sistemleri etkiler. İhlaller, kişisel ve kurumsal verileri tehdit etmenin ötesinde, enerji, iletişim, finans ve ulaşım sistemleri dahil toplumların işlemesine izin veren altyapı varlıklarına zarar verebilir. Trafik ışıklarına, barajlara, bankalara ve elektrik şebekelerine yapılan saldırılar günlük faaliyetleri aksatabilir ve büyük sağlık ve güvenlik risklerine neden olabilir.

• Küresel risk: Siber güvenlik tehditleri tüm ülkeyi, ekonomiyi veya küresel altyapıyı etkileyebilir. Ülkeler birbirlerine siber saldırılar düzenledikçe, devlet ağlarının güvenliğini ve gizliliğini garanti etmenin gerekliliği giderek daha belirgin hale geliyor.

Öyleyse siber güvenlik neden önemlidir? Siber güvenlik, insanları ve kuruluşları, başkalarının özel bilgilerini kendi çıkarlarına hizmet etmek için manipüle etmek isteyen suçlulardan koruyan hayati bir süreçtir. Siber güvenlik çabalarının artması, hırsızlık, veri kaybı, ekonomik ve politik olaylar ve halk sağlığı risklerine karşı koruma sağlamak için kritik öneme sahiptir. Kuruluşların günümüzün savunmasız dijital ortamında çevik ve gayretli kalmaları gerektiği için siber güvenlik giderek daha önemli hale geliyor.

ÖLÇELİM DEĞERLENDİRELİM-1

1. Siber güvenlik için gerekli siber unsurlar nelerdir?

CEVAP: .....

.....

.....

2. Siber güvenlik çözüm döngüsünü yazınız?

CEVAP:
1)
2)
3)
4)
5)

3. Aşağıdakilerin hangisi temel siber güvenlik kavramlarından değildir?

A) Ağ güvenliği B) Bulut Güvenliği C) Uç Nokta Güvenliği D) Oyun Güvenliği

4. Siber güvenlik yapılarını kullanmamızı sağlayan ve önemli kılan etkenler nelerdir?

CEVAP: .....

.....

.....

5. Uç nokta güvenliği nedir?

CEVAP: .....

.....

.....

SİBER GÜVENLİK ALT DALLARI

AĞ GÜVENLİĞİ (NETWORK SECURITY) NEDİR?

Ağ güvenliği, temel ağ altyapısını yetkisiz erişim, kötüye kullanım, arıza, değişiklik, imha veya uygunsuz ifşadan korumak için önleyici tedbirler alma sürecidir.

İnternet şüphesiz hayatımızın büyük bir parçası haline geldi. Günümüz neslindeki pek çok insan profesyonel, sosyal ve kişisel etkinliklerinin çoğu için İnternet'e güveniyor. Ama ağınızın güvenli olduğundan emin misiniz?

İnternet bağlantılı bilgisayarlarımıza zarar vermeye, gizliliğimizi ihlal etmeye ve İnternet hizmetlerini imkansız hale getirmeye çalışan birçok kişi var . Mevcut saldırıların sıklığı ve çeşitliliği ve gelecekteki yeni ve daha yıkıcı saldırıların tehdidi göz önüne alındığında, ağ güvenliği siber güvenlik alanında merkezi bir konu haline geldi. Ağ güvenliği önlemlerinin uygulanması, bilgisayarların, kullanıcıların ve programların izin verilen kritik işlevlerini güvenli bir ortamda gerçekleştirmelerine olanak tanır.

AĞ GÜVENLİĞİNİ NASIL SAĞLAYABİLİRİZ?

Şifrelerin yalnızca bir kuruluş içindeki bireysel bilgisayarlarda değil, ağ içinde de her yerde Güçlü ve Karmaşık olmasını sağlamalıyız. Bu parolalar basit, varsayılan ve kolayca tahmin edilebilir olamaz. Bu basit adım, ağlarınızın güvenliğini sağlamak için uzun bir yol kat edebilir.

Resim 6: Ağ güvenliği yapıları

GÜVENLİK NEDEN BU KADAR ÖNEMLİ?

Bilgi güvenliği, aşağıdakiler gibi önemli rolleri yerine getirir:

• Kuruluşun herhangi bir engel olmadan işleyebilme yeteneği

• Kuruluşun BT sistemlerinde uygulanan uygulamaların güvenli çalışmasının sağlanması

• Kuruluşun topladığı verileri ve kullanımlarını korumak

FARKLI AĞ GÜVENLİĞİ TÜRLERİ NELERDİR?

• Giriş kontrolü

• Uygulama güvenliği

• Güvenlik duvarları

• Sanal özel ağlar (VPN)

• Davranış analitiği

• Kablosuz güvenlik

• Saldırı önleme sistemi

AĞ GÜVENLİĞİ SALDIRISI NEDİR?

Bir ağ saldırı kötü niyetli bir uzlaşma ağ güvenliği girişimi için kullanılan herhangi bir yöntem, süreç veya aracı olarak tanımlanabilir. Ağ güvenliği, belirli bir ağ altyapısı üzerindeki ağ saldırılarını önleme sürecidir, ancak saldırgan tarafından kullanılan teknikler ve yöntemler, saldırının aktif bir siber saldırı mı, pasif türden bir saldırı mı yoksa ikisinin bir kombinasyonu mu olduğunu daha da ayırt eder. Aktif ağ saldırıları genellikle saldırgan ve açık saldırılardır ve kurbanlar, meydana geldiklerinde hemen haberdar olurlar. Aktif saldırılar, doğaları gereği oldukça zararlıdır, genellikle kullanıcıları kilitler, bellek veya dosyaları yok eder veya hedeflenen bir sistem veya ağa zorla erişim sağlar. Pasif saldırı, bir sistemin izlendiği ve bazen açık bağlantı noktaları ve güvenlik açıkları için tarandığı, ancak sistem kaynaklarını etkilemediği bir ağ saldırısıdır. Pasif saldırının amacı, bilgisayar sistemine veya ağa erişim sağlamak ve tespit edilmeden veri toplamaktır.

Giriş kontrolü: Bu, hangi kullanıcıların ağa erişimi olduğunu veya ağın özellikle hassas bölümlerini kontrol etmeyi ifade eder. Güvenlik politikalarını kullanarak, ağ erişimini yalnızca tanınan kullanıcılar ve cihazlarla sınırlayabilir veya uyumlu olmayan cihazlara veya konuk kullanıcılara sınırlı erişim verebilirsiniz.

Antivirüs ve kötü amaçlı yazılımdan koruma yazılımı: Kötü amaçlı yazılım veya "kötü amaçlı yazılım", birçok farklı şekil ve boyutta gelen yaygın bir siber saldırı biçimidir. Bazı varyasyonlar, dosyaları veya bozuk verileri silmek için hızlı bir şekilde çalışırken, diğerleri uzun süre uykuda kalabilir ve bilgisayar korsanlarının sistemlerinize sessizce girmesine izin verebilir. En iyi antivirüs yazılımı, kötü amaçlı yazılımlara karşı ağ trafiğini gerçek zamanlı olarak izler, etkinlik günlük dosyalarını şüpheli davranış belirtileri veya uzun vadeli kalıplar için tarar ve tehdit giderme yetenekleri sunar.

Uygulama güvenliği: Ağ ortamınızda kullanılan her cihaz ve yazılım ürünü, bilgisayar korsanları için potansiyel bir giriş yolu sunar. Bu nedenle, siber saldırganların hassas verilere erişmek için güvenlik açıklarından yararlanmasını önlemek için tüm programların güncel tutulması ve yamalanması önemlidir. Uygulama güvenliği, güvenlik kapsamınızdaki sorunları izlemek ve boşlukları kapatmak için kullandığınız donanım, yazılım ve en iyi uygulamaların birleşimidir.

Davranışsal analiz: Anormal davranışları belirlemek için, güvenlik destek personelinin, belirli bir müşterinin kullanıcıları, uygulamaları ve ağı için normal davranışı neyin oluşturduğuna dair bir temel oluşturması gerekir. Davranış analizi yazılımı, genellikle bir güvenlik ihlalinin meydana geldiğinin bir işareti olabilen, anormal davranışların yaygın göstergelerini tanımlamaya yardımcı olmak için tasarlanmıştır. MSP'ler, her müşterinin taban

çizgilerini daha iyi algılayarak sorunları daha hızlı tespit edebilir ve tehditleri izole edebilir.

Veri kaybı önleme: Veri kaybını önleme (DLP) teknolojileri, bir kuruluşun çalışanlarının değerli şirket bilgilerini veya hassas verileri - farkında olmadan ya da kötü niyetle - ağ dışında paylaşmasını engelleyen teknolojilerdir. DLP teknolojileri, dosyaları karşıya yükleme ve indirme, mesaj iletme veya yazdırma gibi ağ ortamı dışındaki kötü aktörlere potansiyel olarak maruz bırakabilecek eylemleri engelleyebilir.

Dağıtılmış hizmet reddi önleme: Dağıtılmış hizmet reddi (DDoS) saldırıları giderek daha yaygın hale geliyor. Sonunda ağın çökmesine neden olan tek taraflı bağlantı istekleriyle bir ağı aşırı yükleyerek çalışırlar. Bir DDoS önleme aracı, ağınızı tehdit edebilecek yasal olmayan trafiği kaldırmak için gelen trafiği temizler ve güvenlik duvarlarınıza ulaşmadan önce trafiği filtrelemek için çalışan bir donanım cihazından oluşabilir.

E-posta güvenliği: E-posta, ağ güvenliği araçlarını uygularken dikkate alınması gereken özellikle önemli bir faktördür. Dolandırıcılık, kimlik avı, kötü amaçlı yazılım ve şüpheli bağlantılar gibi çok sayıda tehdit vektörü e-postalara eklenebilir veya e-postalara dahil edilebilir. Bu tehditlerin çoğu, daha ikna edici görünmek için genellikle kişisel bilgilerin unsurlarını kullanacağından, bir e-postanın şüpheli olduğunu tespit etmek için bir kuruluşun çalışanlarının yeterli güvenlik bilinci eğitimi almasını sağlamak önemlidir. E-posta güvenlik yazılımı, gelen tehditleri filtrelemek için çalışır ve ayrıca giden mesajların belirli veri biçimlerini paylaşmasını önlemek için yapılandırılabilir.

Güvenlik duvarları: Güvenlik duvarları, bir ağ güvenlik modelinin başka bir ortak unsurudur. Esasen bir ağ ve daha geniş internet arasında bir bekçi olarak işlev görürler. Güvenlik duvarları, veri paketlerini önceden tanımlanmış kurallar ve ilkelerle karşılaştırarak gelen ve bazı durumlarda giden trafiği filtreler ve böylece tehditlerin ağa erişimini engeller.

Mobil cihaz güvenliği: Çoğumuzun, korumak istediğimiz bir tür kişisel veya hassas veri taşıyan mobil cihazları var. Bu, bilgisayar korsanlarının farkında olduğu ve kolayca yararlanabileceği bir gerçektir. Mobil cihaz güvenlik önlemlerinin uygulanması, cihaz erişimini bir ağa sınırlayabilir; bu, ağ trafiğinin gizli kalmasını ve savunmasız mobil bağlantılardan sızmamasını sağlamak için gerekli bir adımdır.

Ağ bölümleme: Ağ trafiğinin belirli sınıflandırmalara göre bölünmesi ve sıralanması, politika uygulama söz konusu olduğunda güvenlik destek personeli için işi kolaylaştırır. Bölümlere ayrılmış ağlar, çalışanlar için yetkilendirme kimlik bilgilerini atamayı veya reddetmeyi kolaylaştırarak, hiç kimsenin olmaması gereken bilgilere erişmemesini sağlar. Segmentasyon, potansiyel olarak tehlikeye giren cihazları veya izinsiz girişleri ayırmaya da yardımcı olur.

Güvenlik bilgileri ve olay yönetimi: Bu güvenlik sistemleri (SIEM'ler olarak adlandırılır), yöneticilere ağdaki tüm etkinliklerin kapsamlı bir resmini sağlamak için gerçek zamanlı ağ trafiği izlemeyi geçmiş veri günlük dosyası taramasıyla birleştiren ana bilgisayar tabanlı ve ağ tabanlı saldırı algılama sistemlerini birleştirir. SIEM'ler, ağ trafiğini şüpheli etkinlik, ilke ihlalleri, yetkisiz erişim ve diğer olası kötü niyetli davranış belirtilerine karşı tarayan saldırı önleme sistemlerine (IPS) benzer. Bir IPS ayrıca güvenlik olaylarını günlüğe kaydedebilir ve ağ yöneticilerini bilgilendirmek amacıyla gerekli oyunculara bildirimler gönderebilir.

Web güvenliği: Web güvenlik yazılımı birkaç amaca hizmet eder. Birincisi, kötü amaçlı yazılım içerebilecek sitelere erişmelerini engellemek amacıyla çalışanların internet erişimini sınırlar. Ayrıca diğer web tabanlı tehditleri engeller ve bir müşterinin web ağ geçidini korumaya çalışır.

SALDIRI ÖNLEME SİSTEMİ

Bu sistemler, genellikle ağ etkinliği imzalarını bilinen saldırı tekniklerinin veri tabanları ile ilişkilendirerek

saldırıları belirlemek ve engellemek için ağ trafiğini tarar. Dolayısıyla bunlar ağ güvenliğini uygulamanın bazı yollarıdır. Bunların dışında, ağ güvenliğini sağlamak için araç setinizde çeşitli yazılım ve donanım araçlarına ihtiyacınız olacaktır. Bunlar:

- Güvenlik duvarları
- Paket işçileri
- Web tarayıcıları
- Paket takip ve içerik çalma
- Saldırı tespit sistemi
- Penetrasyon testi yazılımı

Ağ güvenliği genel siber güvenlik için çok önemlidir. Çünkü ağ, harici saldırılara karşı önemli bir savunma hattıdır. Hemen hemen tüm veri ve uygulamaların ağa bağlı olduğu göz önüne alındığında sağlam ağ güvenliği, veri ihlallerine karşı koruma sağlar.

AĞ GÜVENLİĞİ NASIL ÇALIŞIR?

Bir kuruluş genelinde ağ güvenliğini ele alırken dikkate alınması gereken birçok katman vardır. Saldırılar, ağ güvenlik katmanları modelindeki herhangi bir katmanda gerçekleşebilir, bu nedenle ağ güvenliği donanımınız, yazılımınız ve politikalarınız her alanı ele alacak şekilde tasarlanmalıdır.

Ağ güvenliği tipik olarak üç farklı kontrolden oluşur: fiziksel, teknik ve idari ağ güvenliği olmak üzere. Aşağıda farklı ağ güvenliği türlerinin ve her denetimin nasıl çalıştığının kısa bir açıklaması bulunmaktadır.

FİZİKSEL AĞ GÜVENLİĞİ

Fiziksel güvenlik kontrolleri, yetkisiz personelin yönlendiriciler, kablo dolapları vb. Gibi ağ bileşenlerine fiziksel erişim elde etmesini önlemek için tasarlanmıştır. Kilitler, biyometrik kimlik doğrulama ve diğer cihazlar gibi kontrollü erişim, her kuruluşta çok önemlidir.

TEKNİK AĞ GÜVENLİĞİ

Teknik güvenlik kontrolleri, ağda depolanan veya ağ üzerinden, ağın içine veya dışına geçiş halindeki verileri korur. Koruma iki yönlüdür; verileri ve sistemleri yetkisiz personelden korumalı ve ayrıca çalışanların kötü niyetli faaliyetlerine karşı korumalıdır.

İDARİ AĞ GÜVENLİĞİ

İdari güvenlik kontrolleri, kullanıcıların kimliklerinin nasıl doğrulanacağı, erişim seviyeleri ve ayrıca BT personelinin altyapıdaki değişiklikleri nasıl uyguladığı dahil olmak üzere kullanıcı davranışını kontrol eden güvenlik politikaları ve süreçlerinden oluşur.

IDS (SALDIRI TESPİT SİSTEMLERİ)

Saldırı Tespit Sistemleri, Internet dünyasının gelişim sürecinde özellikle tüm dünyada kullanılan web trafiğinin artması ve de web sayfalarının popüler hale gelmesi ile birlikte kişisel ya da tüzel sayfalara yapılan saldırılar sonucu ihtiyaç duyulan en önemli konulardan biri haline gelmiştir.

Bununla birlikte kurum ya da kuruluşların sahip oldukları ve tüm dünyaya açık tuttukları mail, dns, database gibi sunucularının benzeri saldırılara maruz kalabilecekleri ihtimali yine saldırı tespit sistemlerini internet güvenliği alanının vazgeçilmez bir parçası haline getirmiştir.

Kurumların sahip oldukları çalışan sayısı ve bu çalışanların kendi kurumlarındaki kritik değer taşıyan yapılara saldırabilme ihtimalleri de iç ağın ya da tek tek kritik sunucuların kontrol altında tutulma gerekliliğini beraberinde getirir. IDS(IntrusionDetectionSystem) genel olarak iki tip olarak karşımıza çıkar; Sunucu tabanlı IDS ve Ağ tabanlı IDS.

Ağ tabanlı IDS'in görevi, bir kurum ya da kuruluşun sahip olduğu ağ ya da ağlara yönlenmiş olan tüm trafiği algılayarak, bu ağa doğru geçen her bir data paketinin içeriğini sorgulamak, bir atak olup olmadığına karar vererek kaydını alabilmek.

Sunucu Tabanlı IDS in görevi ise kurulu bulunduğu sunucuya doğru yönlenmiş bulunan trafiği yine üzerinde bulunan atak veritabanı (İşletim Sistemine göre özelleştirilmiş) baz alınarak dinlemesi ve atakları sezerek cevap vermesidir.

BULUT GÜVENLİĞİ (CLOUD SECURITY) NEDİR?

Bulut bilişim, farklı hizmetlerin İnternet üzerinden sunulmasıdır. Bu kaynaklar, veri depolama, sunucular, veritabanları, ağ oluşturma ve yazılım gibi araçları ve uygulamaları içerir. Dosyaları tescilli bir sabit sürücüde veya yerel depolama cihazında tutmak yerine, bulut tabanlı depolama, onları uzak bir veritabanına kaydetmeyi mümkün kılar. Elektronik bir cihazın web'e erişimi olduğu sürece, verilere ve onu çalıştıracak yazılım programlarına erişimi vardır. Bulut bilişim, maliyet tasarrufu, artan üretkenlik, hız ve verimlilik, performans ve güvenlik gibi çeşitli nedenlerle insanlar ve işletmeler için popüler bir seçenektir.

Cihazlarımızı, veri merkezlerimizi, iş süreçlerimizi ve daha fazlasını buluta taşıdıkça bulut veri güvenliği giderek daha önemli hale geliyor. Kaliteli bulut veri güvenliğinin sağlanması, kapsamlı güvenlik politikaları, organizasyonel bir güvenlik kültürü ve bulut güvenlik çözümleri aracılığıyla sağlanır.

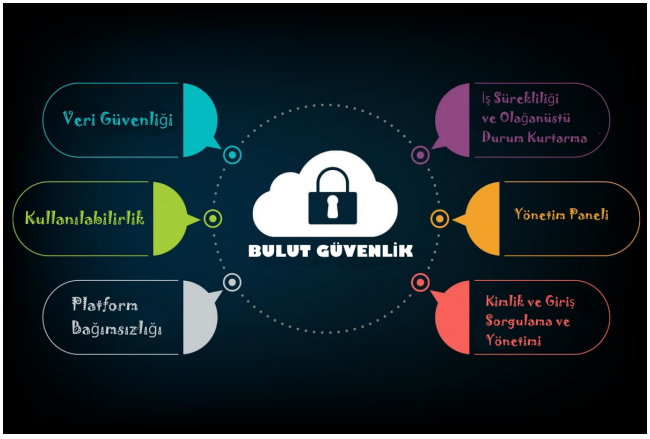
Buluttan en iyi şekilde yararlanmak ve kuruluşunuzun yetkisiz erişime, veri ihlallerine ve diğer tehditlere karşı korunmasını sağlamak istiyorsanız, işletmeler için doğru bulut güvenlik çözümünü seçmek zorunludur.

Bulut güvenliği, bulut bilişim platformları aracılığıyla çevrimiçi olarak depolanan verilerin hırsızlık, sızıntı ve silinmeye karşı korunmasıdır. Bulut güvenliği sağlama yöntemleri arasında güvenlik duvarları, sızma testi, gizleme, belirteçlere ayırma, sanal özel ağlar (VPN) ve genel internet bağlantılarından kaçınma yer alır. Bulut güvenliği, bir siber güvenlik biçimidir. Bulut güvenliği, genel olarak bulut hizmetleri sağlayıcıları aracılığıyla çevrimiçi olarak depolanan dijital varlıkları ve verileri korumak için alınan önlemleri ifade eder. Bulut bilgi işlem, veri depolama, sunucular, veritabanları, ağ iletişimi ve yazılım dahil olmak üzere İnternet üzerinden farklı hizmetlerin sağlanmasıdır. Bu verileri korumaya yönelik tedbirler arasında iki faktörlü yetkilendirme, VPN'lerin kullanımı, güvenlik belirteçleri, veri şifreleme ve güvenlik duvarı hizmetleri ve diğerleri bulunur.

BULUT BİLİŞİM GÜVENLİK SORUNLARI VE ZORLUKLARI

Kuruluşlar buluta giderek artan sayıda uygulama dağıttıkça ve bulut hizmeti sağlayıcılarına daha fazla bağımlı olduklarından, bulut bilişim güvenliği BT kuruluşları için büyüyen bir endişe haline geliyor. Bulut hizmetlerinin yaygınlaşması, geleneksel ağ güvenlik teknikleriyle çözülemeyen yeni güvenlik sorunları ve zorlukları ortaya çıkardı.

Resim 7: Bulut güvenliği bileşenleri



BULUT ORTAMLARINDA VERİ KORUMASI

Hassas verileri bir bulut hizmet sağlayıcısıyla barındırmayı seçen kuruluşlar, sunucuya fiziksel erişimin denetimini kaybediyor. Bu durum ek güvenlik açıkları oluşturur çünkü kuruluş sunuculara kimin fiziksel erişimi olduğunu belirlemede artık bir rol oynayamaz. Bulut hizmet sağlayıcısının bir çalışanı, verilere yasa dışı olarak erişebilir, verileri değiştirebilir veya kopyalayabi-

lir ve hatta başkalarına dağıtabilir. İçeriden gelen saldırıları önlemek için, bulut hizmeti sağlayıcıları, ayrıntılı çalışan geçmiş kontrolleri gerçekleştirmeli ve sunuculara ve BT altyapısına erişim üzerinde katı ve şeffaf bir denetim sağlamalıdır.

KULLANICI KİMLİK DOĞRULAMASI VE ERİŞİM YÖNETİMİ

Bulut hizmetleri bir kullanıcı adı ve parola ile güvence altına alınmalıdır, ancak kötü niyetli bir aktörün oturum açma kimlik bilgilerini çalma, bulut hizmetlerine yetkisiz erişim elde etme ve verileri çalma veya değiştirme riski her zaman vardır. Bir saldırgan, sisteme kötü amaçlı kod da gönderebilir. Bulut hizmeti sağlayıcıları, müşterilerin bu tür saldırılardan korunmasını sağlamak için güvenli bir kimlik bilgisi ve erişim yönetimi sistemi uygulamalıdır.

BULUT HİZMETLERİNİN GÖRÜNÜR OLMAMASI

Bulut bilişim güvenliğinde BT kuruluşlarının karşılaştığı en büyük zorluklardan biri, bulut ortamlarında devreye alınan uygulamaların ve hizmetlerin görünürlüğünün olmamasıdır. Görünürlük eksikliği, BT organizasyonunun bulutta konuşlandırılan uygulamaların ve altyapının güvenlik durumu hakkında verimli bir şekilde bilgi toplayamayacağı veya toplayamayacağı anlamına gelir. Bunun nedeni, çok sayıda farklı sistemin birlikte çalışmasından veya işletme ile bulut hizmeti sağlayıcısı arasındaki şeffaflığın olmamasından kaynaklanıyor olabilir.

BULUT ALTYAPISI ÜZERİNDE KONTROL EKSİKLİĞİ

Şirket içinde dağıtılan ve yönetilen eski BT sistemlerinde, BT kuruluşları tüm teknoloji yığınındaki her BT altyapısı parçası üzerinde tam denetim sağlar. Bunun aksine, bir kuruluş BT altyapısının bir kısmını bir bulut hizmet sağlayıcısına dış kaynak kullandığında, bu altyapının nasıl dağıtılacağı, yönetileceği ve yapılandırılacağı konusunda mutlaka bir miktar denetimden vazgeçer. Bu, BT kuruluşlarının, yüksek güvenlik standardını uygulayan idari kararlar almak için bulut hizmetleri satıcılarına giderek daha fazla güvenmesi gerektiği anlamına gelir.

WEB UYGULAMASI GÜVENLİĞİ (WEB APPLICATIONS SECURITY) NEDİR?

Web uygulaması güvenliği, bir uygulamanın kodundaki güvenlik açıklarından yararlanan farklı güvenlik tehditlerine karşı web sitelerini ve çevrimiçi hizmetleri koruma sürecidir. Web uygulaması saldırıları için ortak hedefler, içerik yönetim sistemleri (örn. WordPress), veritabanı yönetim araçları (örn. PhpMyAdmin) ve SaaS uygulamalarıdır.

Resim 8: Web Uygulama Güvenliği

YAYGIN WEB UYGULAMASI SALDIRILARI NELERDİR?

• Siteler arası komut dosyası çalıştırma (XSS) - XSS, bir saldırganın önemli bilgilere doğrudan erişmek, kullanıcının kimliğine bürünmek veya önemli bilgileri açığa çıkarması için kullanıcıyı kandırmak için istemci tarafı komut dosyalarını bir web sayfasına eklemesine izin veren bir güvenlik açığıdır.

• SQL injection (SQi) - SQi, bir saldırganın bir veritabanının arama sorgularını yürütme biçimindeki güvenlik açıklarından yararlandığı bir yöntemdir. Saldır-

ganlar, yetkisiz bilgilere erişmek, yeni kullanıcı izinlerini değiştirmek veya oluşturmak veya hassas verileri başka şekilde değiştirmek veya yok etmek için SQi'yi kullanır.

• Hizmet reddi (DoS) ve dağıtılmış hizmet reddi (DDoS) saldırıları - Saldırganlar, çeşitli vektörler aracılığıyla hedeflenen bir sunucuyu veya çevresindeki altyapıyı farklı türlerde saldırı trafiğiyle aşırı yükleyebilir. Bir sunucu gelen istekleri artık etkili bir şekilde işleyemediğinde, yavaş davranmaya başlar ve sonunda yasal kullanıcılardan gelen isteklere hizmet vermeyi reddeder.

• Bellek bozulması - Bellek bozulması, bellekteki bir konum kasıtsız olarak değiştirildiğinde ortaya çıkar ve bu da yazılımda beklenmedik davranışlara neden olur. Kötü aktörler, kod enjeksiyonları veya arabellek taşması saldırıları gibi açıklardan yararlanarak bellek bozulmasını bulmaya ve bundan yararlanmaya çalışacaktır.

• Arabellek taşması - Arabellek taşması, yazılım verileri arabellek olarak bilinen bellekte tanımlanmış bir alana yazarken oluşan bir anormalliktir. Arabelleğin kapasitesinin aşılması, bitişik bellek konumlarının verilerle üzerine yazılmasına neden olur. Bu davranış, kötü amaçlı kodun belleğe enjekte edilmesi ve hedeflenen makinede potansiyel olarak bir güvenlik açığı oluşturması için kullanılabilir.

• Siteler arası istek sahteciliği (CSRF) - Siteler arası istek sahteciliği, bir kurbanı kendi kimlik doğrulamasını veya yetkilendirmesini kullanan bir talepte bulunması için kandırmayı içerir. Bir saldırgan, bir kullanıcının hesap ayrıcalıklarından yararlanarak, kullanıcı kimliğine bürünerek bir istek gönderebilir. Bir kullanıcının hesabının güvenliği ihlal edildiğinde, saldırgan önemli bilgileri sızdırabilir, yok edebilir veya değiştirebilir. Yöneticiler veya yöneticiler gibi son derece ayrıcalıklı hesaplar genellikle hedeflenir.

• Veri ihlali - Belirli saldırı vektörlerinden farklı olarak veri ihlali, hassas veya gizli bilgilerin açıklanmasına atıfta bulunan genel bir terimdir ve kötü niyetli eylemler yoluyla veya yanlışlıkla meydana gelebilir. Veri ihlali olarak kabul edilen şeyin kapsamı oldukça geniştir ve milyonlarca maruz kalan kullanıcı hesabına kadar çok değerli birkaç kayıttan oluşabilir.

Web Uygulaması Saldırılarının Çoğunluğu

• SQL İnjection

• XSS (Siteler Arası Komut Dosyası)

• Uzaktan Komut Yürütme

• Rol geçişleri

Saldırı Sonuçları

• Kısıtlanmış içeriğe erişim

• Güvenliği ihlal edilmiş kullanıcı hesapları

• Kötü amaçlı kodun yüklenmesi

• Kayıp satış geliri

• Müşterilere karşı güven kaybı

• Marka itibarının zedelenmesi

• Ve daha fazlası

UÇ NOKTA GÜVENLİĞİ (ENDPOINT SECURITY) NEDİR?

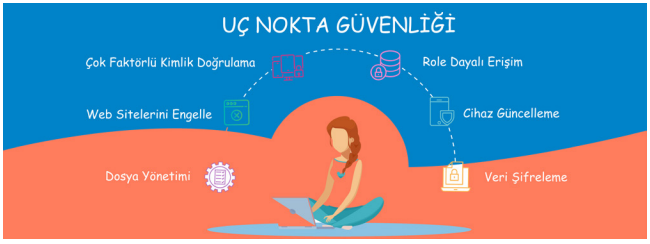
Uç nokta güvenliği, uç noktaların veya masaüstü bilgisayarlar, dizüstü bilgisayarlar ve mobil cihazlar gibi son kullanıcı cihazlarının güvenliğini sağlamak anlamına gelir. Uç noktalar, bir kurumsal ağa erişim noktaları olarak hizmet eder ve kötü niyetli kişiler tarafından kullanılabilecek giriş noktaları oluşturur. Bir uç nokta iletişim kurduğu, bağlı olduğu bir ağ ile ileri geri ve bir uzak işlem cihazıdır. Uç nokta örnekleri şunları içerir:

• Masaüstü

• Dizüstü

- Akıllı telefonlar
- Tabletler
- Sunucular
- İş İstasyonları
- Nesnelerin İnterneti (IoT) cihazları

Uç nokta güvenlik yazılımı, bu giriş noktalarını riskli faaliyetlerden ve / veya kötü niyetli saldırılardan korur. Şirketler veri güvenliği standartlarıyla uç nokta uyumluluğunu sağlayabildiklerinde, ağa yönelik artan sayı ve türdeki erişim noktaları üzerinde daha fazla kontrol sağlayabilirler.



Resim 9: Uç Nokta Güvenliği

Giderek artan bir şekilde, kuruluşlar ve çalışanları, verilere erişimi daha akıcı hale getirmek için uygulamaları birleştiriyor. Kişisel mobil cihazların kullanımındaki artış ve ağları hedefleyen tehditlere ek olarak, birden çok uç nokta güvenlik açığı oluşturur. Ek olarak, evden çalışan veya hareket halindeyken çalışmak için Wi-Fi ağlarına bağlanan çalışanlar, kurumsal ağ güvenliği çevresinin her zamankinden daha geçirgen olduğu anlamına gelir.

Uç nokta güvenlik yazılımı, kurumsal ağa erişen cihazların güvenliğini sağlamak için şifreleme ve uygulama kontrolü kullanır, böylece riskli etkinlikleri izlemek ve engellemek için bu erişim yollarında güvenliği daha iyi kontrol eder. Uç noktalardaki ve çıkarılabilir depolama aygıtlarındaki verilerin şifrelenmesi, veri sızıntılarına ve kaybına karşı korumaya yardımcı olur. Uygulama kontrolü, uç nokta kullanıcılarının ağda güvenlik açıkları oluşturabilecek yetkisiz uygulamaları çalıştırmasını engeller.

Uç nokta güvenlik çözümleri genellikle, hem ağı korumak için merkezi olarak yönetilen bir güvenlik çözümü hem de bu ağa erişmek için kullanılan her uç noktaya yerel olarak yüklenmiş istemci yazılımını kullanan bir istemci-sunucu koruma modeli kullanır. Bazıları, hem merkezi hem de uç nokta güvenlik çözümlerinin uzaktan sürdürüldüğü bir SaaS (Hizmet Olarak Yazılım) modeli üzerinde çalışır.

Anti-virüs yazılımı, uç nokta güvenliğinin merkezidir; her zaman bireysel cihazları ve sunucuları korumaz. Uç nokta korumasının uygulanması, ağa bağlanan ayrı cihazları da güvence altına alarak güvenliğe iki yönlü bir yaklaşım oluşturur. Bir uç nokta güvenlik yaklaşımı kullanmak, uç noktaları güvenlik açısından yalnızca ağı koruyan virüsten koruma yazılımlarından daha fazla sorumlu kılar.

UÇ NOKTA GÜVENLİĞİ İÇİN NELER YAPILABİLİR?

- Ağ trafiğini, aygıt kimlik doğrulamasını vb. Filtrelemek için ağınız için güvenlik duvarı ayarlarını yapılandırmak gibi temel güvenlik çevrelerini etkinleştirmeniz önerilir.

- Ağınızdaki cihazları güvenlik açıklarına karşı düzenli olarak tarayın ve en son yamalarla güncelleyin. Bu uygulama, cihazları güvenlik tehditlerinin çoğundan koruyacaktır.

- Kullanıcıların kimliğini doğrulamak için çok faktörlü kimlik doğrulama uygulanabilir.

- Çalışanları, kurum genelinde uygulanan güvenlik önlemleri hakkında sık sık eğitmek.

- Kuruluşun ağına bağlanmak için katı bir VPN erişim politikası uygulanmalıdır.

• BT donanımının garanti sona erme tarihine ilişkin düzenli olarak bilgi toplayın. Lisanssız yazılım kullanımı için sistemleri tarayın.

• Üretkenlikte kesintiye neden olabilecek ve / ve bant genişliğinin boğulmasına neden olabilecek uygulamaları engelleyin. Örneğin: Oyunlar, torrent yoluyla indirme, vb.

Veri Güvenliği (Data Security) nedir?

Veri Güvenliği, farklı veri kümelerinin göreceli önemini, hassasiyetlerini, mevzuata uygunluk gereksinimlerini belirleyen ve ardından bunları güvence altına almak için uygun korumaları uygulayan bir dizi kontrol, uygulama ve teknik benimseyerek bir ağdaki dosyaları, veritabanlarını ve hesapları koruma sürecidir.

Çevre güvenliği, dosya güvenliği veya kullanıcı davranışsal güvenliği gibi diğer yaklaşımlara benzer şekilde, veri güvenliği bir güvenlik uygulaması için her şeyden ibaret değildir. Her türlü veriyi depolamanın getirdiği riski değerlendirmenin ve azaltmanın bir yöntemidir.

Resim 10: Veri Güvenliği

Veri güvenliğinin temel unsurları gizlilik, bütünlük ve kullanılabilirliktir. CIA (Confidentiality-İntegrity-Availability) üçlüsü olarak da bilinen bu, kuruluşların hassas verilerini yetkisiz erişime ve veri hırsızlığına karşı korumaları için bir güvenlik modeli ve kılavuzdur.

• Gizlilik, verilere yalnızca yetkili kişiler tarafından erişilmesini sağlar;

• Dürüstlük, bilginin güvenilir ve doğru olmasını sağlar; ve

• Kullanılabilirlik, verilerin iş ihtiyaçlarını karşılamak için hem kullanılabilir hem de erişilebilir olmasını sağlar.

FARKLI VERİ GÜVENLİĞİ TEKNOLOJİLERİ

Veri güvenliği teknolojisi birçok şekil ve biçimde gelir ve verileri artan sayıda tehditten korur. Bu tehditlerin çoğu dış kaynaklardan gelmektedir, ancak kuruluşlar çabalarını verilerini içeriden de korumaya odaklamalıdır. Verilerin güvenliğini sağlamanın yolları şunları içerir:

Veri şifreleme: Veri şifreleme, her bir veri parçasına bir kod uygular ve yetkili bir anahtar verilmeden şifrelenmiş verilere erişim izni vermez

Veri maskeleme: Belirli veri alanlarını maskelemek, verileri harici kötü niyetli kaynaklara ve ayrıca verileri potansiyel olarak kullanabilecek dahili personele ifşa edilmekten koruyabilir. Örneğin, bir kredi kartı numarasının ilk 12 rakamı bir veri tabanı içinde maskelenebilir.

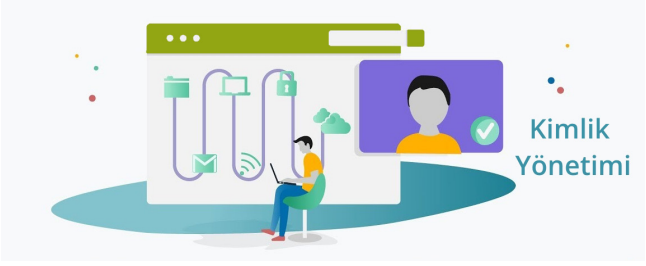
Veri silme: Artık aktif olmayan veya kullanılmayan verilerin tüm sistemlerden silinmesi gereken zamanlar vardır. Örneğin, bir müşteri adının bir posta listesinden çıkarılmasını talep etmişse, ayrıntılar kalıcı olarak silinmelidir.

Veri esnekliği: Kuruluşlar, verilerin yedek kopyalarını oluşturarak, yanlışlıkla silinmesi veya bozulması veya bir veri ihlali sırasında çalınması durumunda verileri kurtarabilir.

KİMLİK YÖNETİMİ (IDENTITY MANAGEMENT) NEDİR?

Kimlik yönetimi (Kimlik yönetimi), kullanıcı haklarını ve kısıtlamalarını yerleşik kimliklerle ilişkilendirerek uygulamalara, sistemlere veya ağlara erişim sahibi olmak için bireyleri veya insan gruplarını tanımlamak, doğrulamak ve yetkilendirmek için kurumsal süreçtir. Yönetilen kimlikler, kurumsal sistemlere erişim gerektiren yazılım süreçlerine de atıfta bulunabilir.

Kimlik yönetimi, kullanıcıların kimliğini doğrulamayı ve belirli sistemlere erişim izni olup olmadığını belirlemeyi içerir. Kimlik yönetimi, kimlik erişim yönetimi sistemleriyle birlikte çalışır. Kimlik yönetimi, kimlik doğrulamaya odaklanırken, erişim yönetimi yetkilendirmeyi amaçlamaktadır.



Resim 11: Kimlik Yönetimi

Kimlik yönetimi, bir kullanıcının sistemlere erişimi olup olmadığını belirler. Ancak aynı zamanda bir kullanıcının belirli bir sistemde sahip olduğu erişim düzeyini ve izinleri de belirler. Örneğin bir kullanıcıya bir sisteme erişme yetkisi verilebilir, ancak bazı bileşenlerinden kısıtlanabilir.

KİMLİK YÖNETİMİNİN ÖNEMİ

Kimlik yönetimi, kuruluşun hem güvenliği hem de üretkenliği ile bağlantılı olduğundan, kurumsal güvenlik planının önemli bir parçasıdır. Birçok kuruluşta, kullanıcılara işlevlerini yerine getirmeleri için gerekenden daha fazla erişim ayrıcalığı verilir. Saldırganlar, kuruluşların ağına ve verilerine erişmek için güvenliği ihlal edilmiş kullanıcı kimlik bilgilerinden yararlanabilir. Kuruluşlar, kimlik yönetimini kullanarak kurumsal varlıklarını bilgisayar korsanlığı, fidye yazılımı, kimlik avı ve diğer kötü amaçlı yazılım saldırıları dahil birçok tehdide karşı koruyabilir.

Kimlik yönetimi sistemleri, kullanıcı erişim ilkelerinin ve kurallarının bir kuruluş genelinde tutarlı bir şekilde uygulanmasını sağlayarak ek bir koruma katmanı ekleyebilir. Bir kimlik ve erişim yönetimi (IAM) sistemi, elektronik veya dijital kimliklerin yönetimini desteklemek için gereken politikaları ve teknolojiyi içeren bir çerçeve sağlayabilir. Günümüz IAM sistemlerinin çoğu, tek bir dijital kimliğin birden çok farklı sistemde doğrulanmasına ve depolanmasına olanak tanıyan birleşik kimlik kullanır.

KİMLİK YÖNETİMİNİ UYGULAMANIN ZORLUKLARI

Kimlik yönetimini başarılı bir şekilde uygulamak için bir kuruluş, iş birimleri arasında planlama yapabilmeli ve işbirliği yapabilmelidir. Başlangıçta açık hedefler, tanımlanmış iş süreci ve paydaşlardan satın alma ile kimlik yönetimi stratejileri oluşturan kuruluşlar daha büyük olasılıkla başarılı olacaktır. Kimlik yönetimi, BT, güvenlik, insan kaynakları ve diğer departmanlar dahil olduğunda en iyi şekilde çalışır.

Kimlik yönetimi sistemleri, şirketlerin farklı durumlarda ve bilgi işlem ortamlarında birden çok kullanıcıyı gerçek zamanlı olarak otomatik olarak yönetmesine izin vermelidir. Yüzlerce veya binlerce kullanıcı için erişim ayrıcalıklarını ve erişim kontrollerini manuel olarak ayarlamak mümkün değildir. Ek olarak, kimlik doğrulamanın kullanıcılar için gerçekleştirmesi basit, BT'nin dağıtması ve güvenliğini sağlaması kolay olmalıdır.

Kimlik yönetimini uygulamanın en büyük zorluklarından biri şifre yönetimidir. Parola oluşturma, güncel-

leme ve silme işlevleri, kuruluşların azaltmak istediği gerçek maliyetlere sahip olabilir. Sonuç olarak, BT uzmanları şirketlerinde bu parola sorunlarının etkisini azaltabilecek teknikleri araştırmalıdır.

Güvenlik nedenlerinden ötürü, kimlik yönetimini yönetmeye yönelik araçlar, şirket içinde veya bulutta özel bir ağ cihazında veya sunucusunda bir uygulama olarak çalışmalıdır. Bir kimlik yönetim sisteminin merkezinde, ağda hangi cihazlara ve kullanıcılara izin verildiğini ve cihaz türüne, konuma ve diğer faktörlere bağlı olarak bir kullanıcının neler başarabileceğini tanımlayan politikalar bulunur. Bunların tümü aynı zamanda politika tanımı, raporlama, uyarılar, alarmlar ve diğer ortak yönetim ve işlem gereksinimleri dahil olmak üzere uygun yönetim konsolu işlevine bağlıdır. Örneğin, belirli bir kullanıcı iznine sahip olmadığı bir kaynağa erişmeye çalıştığında bir alarm tetiklenebilir. Raporlama bir denetim günlüğü oluşturur ve hangi belirli faaliyetlerin başlatıldığını belgeler. Birçok kimlik yönetimi sistemi, dizin entegrasyonu, hem kablolu hem de kablosuz kullanıcılar için destek ve neredeyse tüm güvenlik ve operasyonel politika gereksinimlerini karşılama esnekliği sunar.

MOBİL GÜVENLİK(MOBILE SECURITY) NEDİR?

Mobil güvenlik, akıllı telefonlar, tabletler, dizüstü bilgisayarlar ve diğer mobil cihazlarda depolanan ve bunlardan aktarılan hem kişisel hem de ticari bilgilerin korunmasını içerir. Mobil güvenlik terimi, mobil cihazları kötü amaçlı yazılım tehditlerinden korumadan riskleri azaltmaya ve hırsızlık, yetkisiz erişim veya mobil cihazın kazara kaybedilmesi durumunda mobil cihazları ve verilerini korumaya kadar her şeyi kapsayan geniş bir terimdir. Mobil güvenlik ayrıca, bir mobil cihazın, kullanıcıların kimliğini doğrulayabileceği ve şifreler, kişisel kimlik numaraları (PIN'ler), desen ekran kilitleri veya aşağıdakiler gibi daha gelişmiş kimlik doğrulama biçimleri kullanılarak cihazda depolanan verilere erişimi koruyabileceği veya kısıtlayabileceği araçları ifade eder.

Resim 12: Mobil Güvenlik

Uygulama Bazlı Tehditler

İndirilebilir uygulamalar, mobil cihazlar için birçok türde güvenlik sorunu sunabilir. "Kötü amaçlı uygulamalar" bir indirme sitesinde iyi görünebilir, ancak bunlar özellikle sahtekarlık yapmak için tasarlanmıştır. Bazı yasal yazılımlar bile dolandırıcılık amacıyla kullanılabilir. Uygulama tabanlı tehditler genellikle aşağıdaki kategorilerden birine veya birkaçına uyar:

- Kötü amaçlı yazılım, telefonunuza yüklenirken kötü amaçlı eylemler gerçekleştiren yazılımdır. Bilginiz olmadan, kötü amaçlı yazılımlar telefon faturanız için ödeme yapabilir, kişi listenize istenmeyen mesajlar

gönderebilir veya bir saldırgana cihazınız üzerinde denetim verebilir.

• Casus yazılım, bilginiz veya onayınız olmadan özel verileri toplamak veya kullanmak için tasarlanmıştır. Genelde casus yazılım tarafından hedeflenen veriler arasında telefon görüşmesi geçmişi, metin mesajları, kullanıcı konumu, tarayıcı geçmişi, kişi listesi, e-posta ve özel fotoğraflar bulunur. Bu çalınan bilgiler kimlik hırsızlığı veya mali dolandırıcılık için kullanılabilir.

• Gizlilik Tehditlerine, kötü amaçlı olması gerekmeyen ancak işlevlerini yerine getirmek için gerekenden daha hassas bilgileri (örneğin, konum, kişi listeleri, kişisel olarak tanımlanabilir bilgiler) toplayan veya kullanan uygulamalardan kaynaklanabilir.

• Savunmasız Uygulamalar, kötü niyetli amaçlarla yararlanılabilecek kusurlar içeren uygulamalardır. Bu tür güvenlik açıkları, bir saldırganın hassas bilgilere erişmesine, istenmeyen eylemler gerçekleştirmesine, bir hizmetin düzgün çalışmasını durdurmasına veya bilginiz olmadan cihazınıza uygulama indirmesine olanak tanır.

WEB TABANLI TEHDİTLER

Mobil cihazlar sürekli olarak İnternete bağlı olduğundan ve web tabanlı hizmetlere erişmek için sıklıkla kullanıldığından, web tabanlı tehditler mobil cihazlar için kalıcı sorunlar oluşturur:

• Kimlik Avı Dolandırıcılıkları , sizi parolalar veya hesap numaraları gibi bilgileri sağlamanız için kandırmak üzere tasarlanmış web sitelerine bağlantılar göndermek için e-posta, metin mesajları, Facebook ve Twitter kullanır. Genellikle bu mesajlar ve siteler, bankanızdakilerden veya diğer yasal kaynaklardan ayırmak için çok farklıdır.

• Drive-By Downloads , bir web sayfasını ziyaret ettiğinizde bir uygulamayı otomatik olarak indirebilir. Bazı durumlarda, indirilen uygulamayı açmak için işlem yapmanız gerekirken, diğer durumlarda uygulama otomatik olarak başlayabilir.

• Tarayıcı açıklarından yararlanma, mobil web tarayıcınızdaki veya bir Flash oynatıcı, PDF okuyucu veya resim görüntüleyici gibi tarayıcı tarafından başlatılan yazılımdaki güvenlik açıklarından yararlanır. Basitçe güvenli olmayan bir web sayfasını ziyaret ederek, kötü amaçlı yazılım yükleyebilecek veya cihazınızda başka eylemler gerçekleştirebilecek bir tarayıcı açıklarını tetikleyebilirsiniz.

AĞ TEHDİTLERI

Mobil cihazlar tipik olarak hücresel ağların yanı sıra yerel kablosuz ağları (WiFi, Bluetooth) destekler. Bu tür ağların her ikisi de farklı tehdit sınıflarını barındırabilir:

• Ağ istismarları , mobil işletim sistemindeki veya yerel veya hücresel ağlarda çalışan diğer yazılımlardaki kusurlardan yararlanır. Bağlandıktan sonra, bilginiz olmadan telefonunuza kötü amaçlı yazılım yükleyebilirler.

• Wi-Fi Sniffing , cihaz ile WiFi erişim noktası arasında havada seyahat ederken verileri yakalar. Birçok uygulama ve web sayfası doğru güvenlik önlemlerini kullanmaz ve ağ üzerinden, veri toplayan biri tarafından kolayca okunabilen şifrelenmemiş verileri gönderir.

FİZİKSEL TEHDİTLER

Mobil cihazlar küçüktür, değerlidir ve onları yanımızda her yere taşıyoruz, bu nedenle fiziksel güvenlikleri de önemli bir husustur.

Kayıp veya Çalıntı Cihazlar, en yaygın mobil tehditlerden biridir. Mobil cihaz, yalnızca donanımın karaborsada yeniden satılabilmesi nedeniyle değil, daha da önemlisi içerebileceği hassas kişisel ve organizasyon bilgileri nedeniyle değerlidir.

ETKİNLİK

Etkinlik Adı

Siber Saldırıları İzliyorum

Etkinlik Süresi

2 Ders Saati

Etkinlik Modülü

Siber Güvenlik Eğitimi

Etkinlik Kazanımları

- Siber saldırı kavramını tanımlar.
- Kötü amaçlı saldırılarını tanır ve hangi amaçla yapıldığını bilir.
- Ülkelerin siber saldırı istatistiklerini listeler.
- En çok kullanılan siber saldırı yöntemlerini bilir.
- Siber saldırı görüntüleme ekranlarını yönetmeyi bilir.

Ön Bilgi

Siber Saldırılar ve savaşlar günümüzde ülkeler arası rekabet yapılan en popüler alanlardan bir tanesidir. Ülkeler siber ordu yapılarını kurarak bu atakları bertaraf etmekte veya siber saldırılar ile karşı tarafın direncini kırarak hizmet aksamasına veya sistemin çökmesini sağlayacak saldırılar gerçekleştirmektedir.

Siber saldırı tanım olarak siber suçluların veya ülkelerin iyi amaçlı veya kötü amaçlı, bir veya daha fazla bilgisayarı tek veya birden fazla bilgisayara veya ağa karşı kullanarak başlattığı bir saldırıdır. Siber saldırı, bilgisayarları kötü amaçlı olarak devre dışı bırakabilir, veri çalabilir veya ihlal edilen bir bilgisayarı diğer saldırılar için bir başlangıç noktası olarak kullanabilir. Siber suçlular, diğer yöntemlerin yanı sıra kötü amaçlı yazılım, phishing, fidye yazılımı, hizmet reddi de dahil olmak üzere çeşitli yöntemler kullanır. Ülkemizde siber savunma yapıları MİT, TSK, ASELSAN gibi yapıların içerisinde bir birim olarak bulunmakta fakat bazı ülkelerde kritik noktaların tamamını savunan ve saldırılar gerçekleştiren Siber Savunma Orduları oluşturmuştur. İlerleyen zamanda bütün ülkeler bu yapıya geçecek ve ülke güvenliğini sağlayacaklardır.

Ülkemizde üniversite düzeyi ve sonrası için Beyaz Şapkalı Hacker eğitimleri verilerek iyi niyetli siber saldırıları eğitimi verilerek kötü niyetli siber saldırıların yapısını, yapılışını ve bertaraf etme yapısından bahsedilmektedir. Bu eğitimlerde şu yapılar öğretilmektedir: Etik Hacklemeye Giriş, Sistem Temelleri, Şifreleme, Footprinting, Tarama,Sıralama,

Sistem Hackleme, Zararlı Yazılım,Dinleyici, Sosyal Mühendislik, Servis Dışı Bırakma, Oturum Ele Geçirme, Web Sunucuları ve Uygulamaları, SQL İnjection, Wi-Fi ve Bluetooth Hackleme, Mobil Cihaz Güvenliği, Evasion, Bulut Teknolojileri ve Güvenliği, Fiziksel Güvenlik. Bu eğitimler sayesinde temel düzeyde bir siber güvenlik bilgisine sahip olabilirsiniz.

Yöntem

Gerçek zamanlı siber saldırı haritaları, dünya çapında gerçekleşen saldırılara ilişkin bir fikir verir. Kapsamları, türleri ve amaçları değişse de, siber saldırılarla ilgili bir şey aynı kalır: Asla durmazlar. Herhangi bir anda yüzlerce siber saldırı gerçekleşiyor. Verilerin ve işletmelerimizin artan dijitalleşmesi ile siber saldırıların sayısı arttı ve sadece büyük olanlar yerine her büyüklükteki kuruluşu hedef almaya başladı. Aslında, son araştırmalar siber saldırganların daha az kaynak harcayacaklarını ve siber güvenliklerine daha az dikkat edeceklerini varsayarak daha küçük kuruluşları hedef alma eğiliminde olduklarını gösteriyor. Devam eden siber saldırılar hakkında daha fazla bilgi edinmek, trendleri takip etmek ve kuruluşunuzun güvenlik önlemlerini buna göre güncellemek istiyorsanız, gerçek zamanlı siber saldırı haritalarına göz kulak olmak sizin için çok faydalı olabilir. Siber saldırı yapan ülkelerin en çok kullandığı yöntem olan Dağıtılmış Hizmet Reddi (DDoS) saldırısı, hedeflenen bir sunucunun tipik internet trafiğini birden çok kaynaktan gelen trafiğe boğarak alt etmeye yönelik kötü niyetli bir girişimdir. DDoS saldırıları, bankalardan haber web sitelerine kadar çok sayıda önemli kaynağı hedefler ve İnternet kullanıcılarının önemli bilgileri yayınlayıp bunlara erişebilmelerini sağlamak için büyük bir zorluk teşkil eder. Bir DDoS saldırısı, bir otoyoldaki trafik sıkışıklığına benzer ve tipik trafik akışını engeller. DDoS saldırısı, saldırganın çevrimiçi makineler ağının kontrolünü ele geçirmesini gerektirir. Bilgisayarlara kötü amaçlı yazılım bulaşmış ve onları bir bot haline getiriyor. Daha sonra saldırgan, artık botnet olarak adlandırılan bot grubu üzerinde kontrole sahip olur.Bir botnet kurulduktan sonra, saldırgan bir uzaktan kumandadan her bota talimatlar gönderir. IP adresi hedeflendiğinde, her bot hedefe istek göndererek yanıt verir ve sunucunun taşmasına neden olarak DDoS saldırısına neden olur.

Düşük ve orta ölçekli izole bir Dağıtılmış Hizmet Reddi (DDoS) saldırısıyla karşı karşıyaysanız, bu günlükleri inceleyebilir ve kendinizi bu saldırılardan korumak için ihtiyacınız olan bilgileri bulabilirsiniz. Ancak, daha büyük saldırılarda manuel aramalar zaman alıcıdır ve etkisizdir. Bu yüzden siber saldırılarla mücadele etmek için başka planların olması gerekiyor. Ancak, bir DDoS saldırısı yaşamıyorsanız ve sadece dünyadaki siber güvenlik olaylarından en iyi dijital saldırı bilgilerini öğrenmek

istiyorsanız, nereye bakardınız? İnternet servis sağlayıcısının (ISP) istatistiklerini deneyebilir veya anti-DDOS sağlayıcılarına göz atabilir veya dijital saldırı haritalarına bakarak şu anda neler olduğunu görebilirsiniz.

Siber güvenliğin küresel olarak nasıl çalıştığını görmek için, siber saldırıları ve kötü niyetli paketlerin ülkeler arasında nasıl etkileşime girdiğini gözlemleyebilirsiniz.

Programın Yüklemesi ve Arayüz

Etkinliğimiz için siber saldırı haritaları kullanacağız. Farklı web sayfaları bu amaçla kurulmuştur. Özellikle antivirüs programları online olarak saldırıları da gözlemleyebileceğimiz sayfalar açmışlardır.

Siber saldırı haritaları, saldırıların önüne nasıl geçileceği konusunda bilgi veren değerli araçlardır. Bir siber saldırı haritası, İnternet'in nasıl işlediğini grafiksel olarak gösterir ve büyük resmi görmek için yararlı olabilir. Siber suçluların neden olduğu muazzam zararlardan bahsediyor olsak da, haritaların kendilerinin izlemesi büyüleyici olabilir. Yaklaşık her 39 saniyede bir siber saldırı gerçekleşir. Bunlardan bazıları manuel olarak hedeflenen siber saldırılar olsa da, çoğu altyapıları kapatma ve büyük kuruluşların bilgisayarlarını ve sistemlerini yok etme konusunda kararlı botnetlerdir.

Siber saldırı haritaları özellikleri şunları içerir:

- Her ülke için istatistikler
- Saldırı kaynağı ve hedefi
- Çeşitli saldırı türleri (büyük, yaygın olmayan, birleşik vb.)
- Türe, kaynak bağlantı noktasına, süreye ve hedef bağlantı noktasına göre renk kodlu saldırılar
- DDoS saldırısının Gbps cinsinden boyutu
- Haritayı kendi web sitenize ekleyebilmeniz için yerleştirme kodu
- TCP bağlantısı, hacimsel, parçalanma ve uygulama

En çok kullanılan siber saldırı harita web sayfaları:

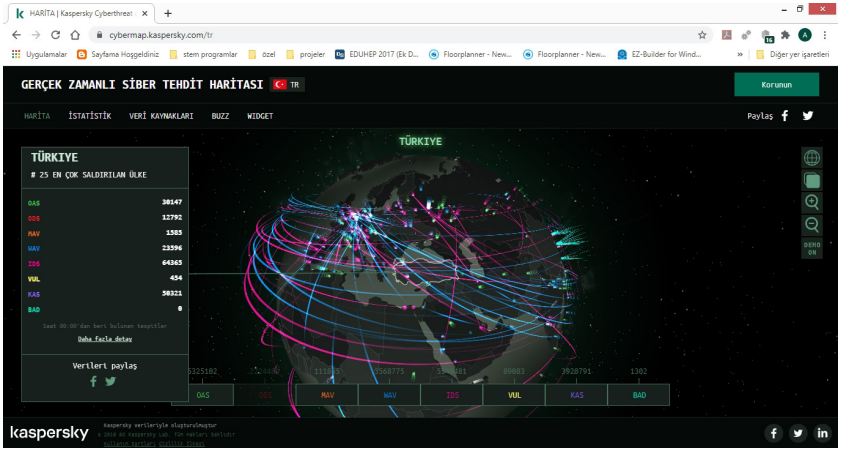
- https://www.digitalattackmap.com/

- https://horizon.netscout.com/?mapPosition=0.00~0.00~1.00
- https://www.parsecuremap.com/#2/42.3/-17.7
- https://cybermap.kaspersky.com/
- https://threatmap.checkpoint.com/
- https://www.spamhaustech.com/threat-map/
- https://www.fireeye.com/cyber-map/threat-map.html
- https://threatmap.bitdefender.com/

Etkinlik Yapımı

Etkinliğimiz için siber saldırı haritalarından en detaylı olan yapılarından bir tanesi olan ; https://cybermap.kaspersky.com/tr kullanacağız.

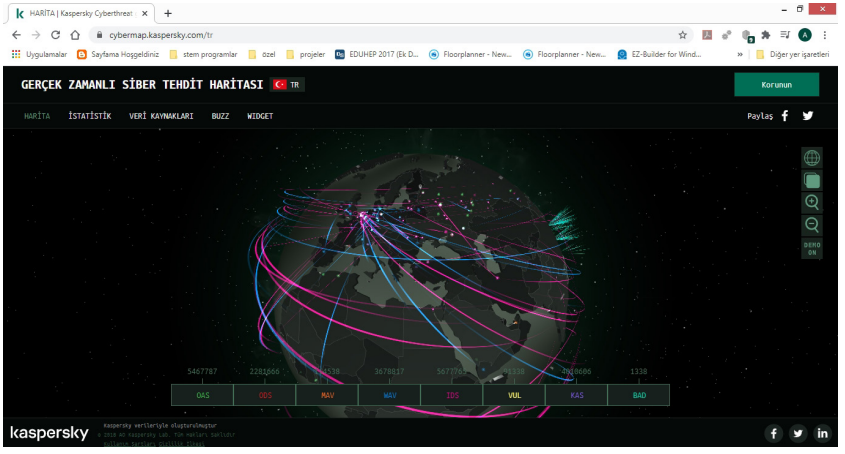
Web sayfasını açtığımızda karşımıza Resim 13'deki ekran gelmektedir.



Resim 13: Karspersky Siber Saldırı Haritası Ana Ekranı

Siber saldırı haritalarında ülkelerin siber saldırıya uğrama veya siber saldırı gerçekleştirme istatistiklerine bakabiliriz. Harita üzerinden seçtiğimiz ülkenin siber saldırı yapılan ülkeler arasında kaçıncı olduğuna

bakabilirsiniz. Ayrıca DDoS saldırısı , Spam , Mallware ve güvenlik açıklarını detaylı bir şekilde görebiliyoruz. Renklerine göre hangi saldırı gerçekleştirilmiş veya engellenmiş görebiliriz. Ayrıca saldırıları engelleyen ülkelerin hangi yapı ile nasıl engellediğini görebiliyoruz.



Resim 14: Karspersky Siber Saldırı Haritası Ülke Detaylarındırma

Hangi ülkenin detayını görmek isterseniz dünya haritasından seçebilirsiniz. Seçtiğimiz ülkelerin bilgileri çıkmakta ve üzerine geldiğimizde açıklamalarını görebilmekteyiz. Web sayfamızın istatistik kısmından grafiksel olarak ülkelerin siber saldırı geçmişlerine bakabiliyoruz.

Siz Uygulayın!

2 ülkeyi seçiniz ve hangi siber saldırılara maruz kaldığını bu saldırıların nasıl bertaraf edildiğini araştırınız.

1.ÜLKE:	2.ÜLKE:
EN ÇOK UĞRADIĞI SALDIRI: EN AZ UĞRADIĞI SALDIRI:	EN ÇOK UĞRADIĞI SALDIRI: EN AZ UĞRADIĞI SALDIRI:

ÖLÇELİM DEĞERLENDİRELİM-2

1. Bulut yapısını açıklayınız. Güvenlik açıkları nelerdir yazınız.

CEVAP: ……

……

……

2. DDoS saldırısı nedir?

CEVAP: ……

……

……

3. Ağ güvenliği protokolleri nelerdir , yazınız.

CEVAP:

1)
2)
3)

4. Veri güvenliğinin temel unsurları ve açıklamalarını eşleştiriniz.

…… A) Gizlilik	1. Bilginin güvenilir ve doğru olmasını sağlar.
…… B) Kullanılabilirlik	2. Verilerin iş ihtiyaçlarını karşılamak için hem kullanıla bilir hem de erişilebilir olmasını sağlar.
…… C) Dürüstlük	3. Verilere yalnızca yetkili kişiler tarafından erişilmesini sağlar.

5. SQL injection (SQi) nedir?

CEVAP: ……

……

……

KÖTÜ AMAÇLI YAZILIMLAR VE SIZMA SİSTEMLERİ

Kötü amaçlı yazılım, kötü amaçlı yazılım faillerinin tek tek bilgisayarlara veya tüm kuruluşun ağına bulaşmak için gönderdiği anlamına gelir. Meşru yazılımdaki (örneğin; bir tarayıcı veya web uygulaması eklentisi) ele geçirilebilecek bir hata gibi hedef sistem açıklarından yararlanır. Kötü amaçlı yazılımların sistemimize enfekte olması ile verilerin gasp edilmesi, sistemin kontrolünün ele geçirilmesi ve ağ yapısının kontrolü gibi hayati alanlar zarara uğramaktadır.

Her biri kendi uygulama alanına ve odağına sahip çok sayıda kötü amaçlı yazılım türü vardır. En yaygın olanları aşağıda listelenmiştir:

Ransomware (Fidye Yazılımı) : Yüklendikten sonra bu kötü amaçlı yazılım, bir bilgisayardaki ve / veya genişletilmiş bir ağdaki dosyaları şifreler. Bir açılır pencere, kullanıcıya fidye ödenmediği takdirde dosyalarının şifreli kalacağını bildirir.

Resim 15: Fidye Yazılımı Ekran Görüntüsü

Fidye yazılımı genellikle bir e-posta eki olarak gelir veya farkında olmadan kötü amaçlı bir web sitesinden indirilir. Hizmet olarak fidye yazılımı (RaaS) adı verilen yeni bir iş modeli kısa süre önce ortaya çıktı. Amatör

bilgisayar korsanları (diğer adıyla "komut dosyası çocukları"), bir RaaS saldırısı gerçekleştirmek için mevcut kötü amaçlı yazılımları lisanslar. Başarı durumunda, fidyenin bir yüzdesi kötü amaçlı yazılım yazarına gider.

Worms(Solucan) : Bilgisayar solucanı, virüs bulaşmamış bilgisayarlara yayılmak için kendisini kopyalayan, kendi kendini kopyalayan kötü amaçlı yazılımdır. Solucanlar genellikle bir işletim sisteminin otomatik ve kullanıcı tarafından görünmeyen kısımlarını kullanır. Solucanların yalnızca kontrolsüz çoğaltmaları sistem kaynaklarını tüketip diğer görevleri yavaşlattığı veya durdurduğu zaman fark edilmesi yaygındır.

Bilgisayar solucanları, yayılmak için genellikle ağ protokollerinin eylemlerine ve güvenlik açıklarına güvenir. Örneğin, WannaCry fidye yazılımı solucanı, Windows işletim sisteminde uygulanan Sunucu İleti Bloğu (SMBv1) kaynak paylaşım protokolünün ilk sürümündeki bir güvenlik açığından yararlandı. Yeni virüs bulaşmış bir bilgisayarda etkin olduktan sonra, WannaCry kötü amaçlı yazılımı, yeni potansiyel kurbanlar için bir ağ araması başlatır: solucan tarafından yapılan SMBv1 isteklerine yanıt veren sistemler. Solucan bu şekilde bir organizasyon içinde yayılmaya devam edebilir. Kişisel bilgisayarlara bulaştığında, solucan diğer ağlara yayılarak bilgisayar korsanlarına daha da fazla erişim sağlayabilir.

E-posta solucanları, giden iletiler oluşturarak ve bir kullanıcının kişiler listesindeki tüm adreslere göndererek çalışır. Mesajlar, alıcı sistemi açtığında yeni sistemi etkileyen kötü amaçlı bir yürütülebilir dosya içerir. Başarılı e-posta solucanları genellikle kullanıcılardan ekli dosyayı açmalarını istemek için sosyal mühendislik yöntemlerini kullanır.

Bugüne kadarki en kötü şöhretli bilgisayar solucanlarından biri olan Stuxnet, virüslü USB cihazlarının paylaşılması yoluyla kötü amaçlı yazılımın yayılmasına yönelik bir solucan bileşeninin yanı sıra yaygın olarak kullanılan denetim kontrolü ve veri toplama (SCADA) sistemlerini hedefleyen kötü amaçlı yazılımdan oluşur. Bu yazılımlar elektrik hizmetleri, su tedarik hizmetleri, kanalizasyon tesisleri ve diğer yerler dahil endüstriyel ortamlarda enfekte olarak hayat akışını etkiler. Kötü amaçlı yazılımları bulundurmayan bilgisayar solucanları kendilerini enfekte sistemlerden enfekte olmayan sistemlere doğru yayarlar. Virüslü bir sistem, solucanın yayılmasıyla ilişkili bilgi işlem ek yükü nedeniyle kullanılamaz hale gelebilir veya güvenilmez hale gelebilirken, bilgisayar solucanlarının ağ bağlantılarının solucan yayılmasıyla ilişkili kötü niyetli trafikle doygunluğu yoluyla ağı bozduğu da bilinmektedir.

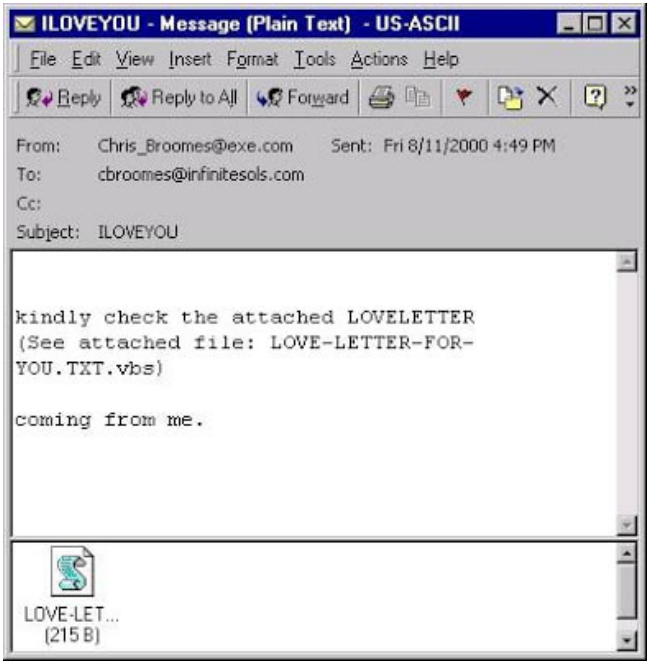
Solucanların sınıflandırmaları ve isimleri:

- E-posta-Solucan
- IM-Solucan
- IRC-Solucan
- Net-Solucan
- P2P Solucan

Dünyada en çok yaygın solucanlardan bazıları ise şunlardır:

NgrBot: Bu solucan, sohbet habercileri ve sosyal ağ siteleri aracılığıyla yayılır. Failler, yüklendikten sonra kullanıcının makinesini devasa bir botnet'e katılan bir zombiye dönüştüren kötü amaçlı yazılımın indirilmesini teşvik etmek için sosyal mühendisliği kullanır. Ayrıca, virüslü sistemlerin güncellenmesini durdurur ve oturum açma kimlik bilgilerini ve diğer hassas bilgileri çalabilir.

ILOVEYOU: Bu solucan insanları, olası bir aşk ilgisini çekerek, solucanı içeren bir e-posta ekini açmaya teşvik eden bir sosyal mühendislik saldırısı kullanılarak dağıtıldı. Daha sonra çeşitli dosya türlerinin üzerine yazan bir Visual Basic komut dosyası çalıştırılır. Solucan tahmini 45 milyon bilgisayara bulaştı.



Resim 16: Solucan Yazılımı Ekran Görüntüsü

Truva Atı (Trojan): Bir Truva atı meşru görünür ancak tehlikeli bir yük taşır. Kendini solucanlar gibi çoğaltmasa da, genellikle arka kapılar, rootkit'ler, fidye yazılımları ve casus yazılımlar dahil olmak üzere ek kötü amaçlı yazılım türleriyle birlikte gelir.

Bankacılık sektörü, Truva atı saldırılarının favori hedefidir. Örneğin , Rig exploit kit aracılığıyla çalıştırılan Tiny Banker Trojan (Tinba) kötü amaçlı yazılımı , kurulumunu önce hedef bilgisayarda bir yazılım güvenlik açığı bulunarak gerçekleştirilir. Daha sonra sistem kullanıcısı bir banka sitesini her ziyaret ettiğinde, kredi kartı bilgileri dahil olmak üzere kişisel bilgileri isteyen sahte bir ekranı kaplar. En çok kullanılan Truva atı yapıları aşağıdadır:

Resim 17: Truva Atı Yazılımları

- **Back Door**

Bir back door truva atı, bilgisayar korsanlarına virüslü bilgisayar üzerinde uzaktan denetim almaları için kötü niyetli erişim sağlar. Kötü niyetli bilgisayar korsanına, kötü niyetli niyetlere göre virüs bulaşmış bilgisayarda çalışma yetkisi verir. Dosyaları gönderebilir, alabilir, silebilir ve başlatabilir, verileri görüntüleyebilir ve bilgisayarı yeniden başlatabilirler. Arka kapı Truva atları çoğunlukla bilgisayar korsanları tarafından bir grup virüslü bilgisayardan yararlanarak zombi ağı veya suç amaçlı kullanılabilecek kötü niyetli botnet oluşturmak için kullanılır.

- **Exploit**

Exploit, virüs bulaşmış bir bilgisayarda çalışan savunmasız bir yazılıma veya uygulamaya saldırmak için kötü amaçlı bir kod veya veri içeren bir Truva atı türüdür.

- **Rootkits**

Rootkits, kötü amaçlı yazılım yazarları tarafından kurbanın sistemine erişim sağlamak için geliştirilirken, varlıklarını veya kötü niyetli etkinliklerini virüs bulaşmış bilgisayarda çalıştırmak ve yürütmek üzere geniş-

letmek için tespit edilmekten gizler.

• **Trojan-Banker**

Bu, çevrimiçi bankacılık sistemleri, e-ödeme ağ geçidi aracılığıyla kullanıcının hesap verilerini, banka veya kredi kartı verilerini almak için geliştirilmiş bir trojan türüdür.

• **Truva Atı-DDoS**

Bu programlar, kurbanın web adresine bulaşmak üzere Hizmet Reddi (DOS) saldırıları gerçekleştirmek için geliştirilmiştir. kötü amaçlı yazılım programı kurbanın virüslü bilgisayarından birden çok şey gönderir ve diğer birkaç virüslü bilgisayarla bir ağ oluşturur - hedef adrese karşı bir hizmet reddine neden olan bir saldırıyı güçlü bir şekilde uygulamak için.

• **Trojan-Downloader**

Trojan-Downloaders, adından da anlaşılacağı gibi, kötü amaçlı programların yeni sürümlerini hedef kurbanın bilgisayarına indirmek ve yüklemek için bilgisayar korsanları tarafından geliştirilmiştir.

• **Trojan-Dropper**

Bu programlar kötü amaçlı yazılım yazarları tarafından Truva atlarını / virüsleri yüklemek ve kötü amaçlı programların tespitinden kaçmak için geliştirilmiştir. Geleneksel antivirüs programlarının çoğu, bu Truva Atı'nın tüm bileşenlerini taramak için yetersizdir.

• **Trojan-FakeAV**

Trojan-FakeAV programları, bir antivirüs yazılımı gibi çalışıyormuş gibi davranır. Rapor ettikleri tehditler gerçek zamanlı olarak mevcut olmamasına rağmen tehditleri tespit etmek ve ortadan kaldırmak için siber hırsızlar tarafından hedef kullanıcıdan para almak için geliştirilirler.

• **Trojan-GameThief**

Trojan-Game Thief için ana hedef çevrimiçi oyunculardır ve onların ana amacı kullanıcı hesabı bilgilerini çalmaktır.

• **Truva Atı-IM**

Truva Atı-IM programları öncelikle kullanıcıların Skype, Facebook Messenger, Instagram, Whatsapp, Yahoo Pager, gmail ve daha fazlasının oturum açma bilgilerini ve parolalarını çıkarır.

• **Trojan-Ransom**

Trojan-Ransom, kurbanın bilgisayarındaki verileri değiştirmek için geliştirilmiştir - böylece sistem işlevini doğru şekilde yerine getirmez ve ayrıca kullanıcının belirli verileri kullanmasına izin vermez. Suçlu, verilere kısıtlı erişimi engellemek ve bilgisayarın performansını eski haline getirmek için kurban tarafından bir fidye ödenmesini talep edecektir.

• **Trojan-SMS**

Trojan-SMS programları kurbanın mobil cihazından diğer telefon numaralarına metin mesajları gönderir.

• **Trojan-Spy**

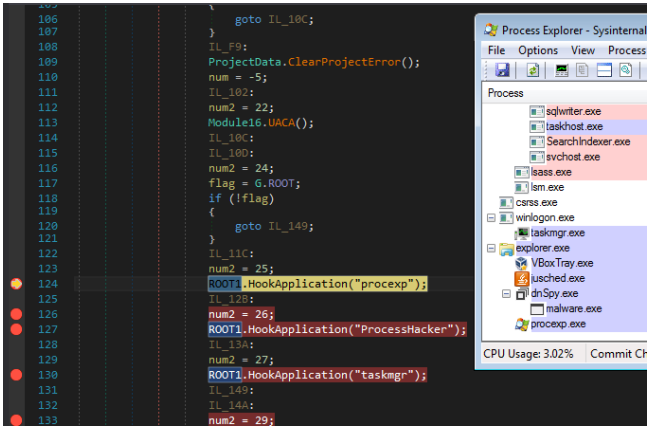
Trojan-Spy programları, adından da anlaşılacağı gibi, kurbanın bilgisayarı nasıl kullandığı hakkında casusluk yapabilir. Örneğin verileri izleme, ekran görüntüleri alma veya çalışan uygulamaların bir listesini çıkarma.

• **Trojan-Mailfinder**

Bu programlar, bilgisayar korsanları tarafından kurbanın bilgisayarından e-posta adreslerini çıkarmak için geliştirilmiştir.

Rootkit: Bir bilgisayara sürekli ayrıcalıklı erişim sağlamak ve varlığını aktif olarak gizlemek için tasarlanmış gizli bir bilgisayar programıdır. Rootkit terimi, "root" ve "kit" kelimesinin bir bağlantısıdır. Başlangıçta bir rootkit, bir bilgisayara veya ağa yönetici düzeyinde erişim

sağlayan bir araçlar koleksiyonuydu. Root, Unix ve Linux sistemlerindeki Yönetici hesabını, kit ise aracı uygulayan yazılım bileşenlerini ifade eder. Günümüzde rootkit'ler genellikle varlıklarını ve eylemlerini kullanıcılardan ve diğer sistem işlemlerinden gizleyen kötü amaçlı yazılımlarla (Truva atları, solucanlar , virüsler gibi) ilişkilendirilmektedir .



Resim 18: Rootkit Yazılım Örneği

Bir rootkit, bir kullanıcının bilgisayar kullanıcısı / sahibi bilmeden bir bilgisayar üzerinde komuta ve kontrol sağlamasına izin verir. Bir rootkit kurulduktan sonra, rootkit'in denetleyicisi, ana makinedeki dosyaları uzaktan yürütme ve sistem konfigürasyonlarını değiştirme yeteneğine sahiptir. Virüs bulaşmış bir bilgisayardaki bir rootkit de günlük dosyalarına erişebilir ve yasal bilgisayar sahibinin kullanımı hakkında casusluk yapabilir.

Rootkit Algılama

Rootkit'leri tespit etmek zordur. Bilinen ve bilinmeyen tüm kök setlerini bulabilen ve kaldırabilen ticari ürün bulunmamaktadır. Virüs bulaşmış bir makinede bir rootkit aramanın çeşitli yolları vardır. Algılama yöntemleri, davranışa dayalı yöntemleri (örneğin, bir bilgisayar sisteminde garip davranışları arama), imza taramasını ve bellek dökümü analizini içerir. Genellikle, bir rootkit'i kaldırmanın tek yolu, tehlikeye atılan sistemi tamamen yeniden oluşturmaktır.

Rootkit Koruması

Pek çok rootkit, güvendiğiniz yazılım veya bir virüsle piggyback yaparak bilgisayar sistemlerine sızar. Bilinen güvenlik açıklarına karşı yama uygulanmasını sağlayarak sisteminizi rootkitlerden koruyabilirsiniz. Bu yapı, işletim sisteminizin yamalarını, uygulamaları ve güncel virüs tanımlarını içerir. Bilinmeyen kaynaklardan gelen dosyaları kabul etmeyin veya e-posta dosya eklerini açmayın. Yazılım yüklerken dikkatli olun ve son kullanıcı lisans sözleşmelerini dikkatlice okuyun.Statik analiz , arka kapıları ve rootkit'ler gibi diğer kötü amaçlı eklentileri tespit edebilir. Hazır yazılım satın alan kurumsal geliştiriciler ve BT departmanları, "özel" ve "gizli kimlik bilgileri" arka kapılar dahil olmak üzere tehditleri tespit etmek için uygulamalarını tarayabilir.

Tanınmış Rootkit Örnekleri

• Lane Davis ve Steven Dake - 1990'ların başında bilinen en eski rootkit'i yazdı.

• NTRootkit - Windows işletim sistemini hedefleyen ilk kötü amaçlı rootkitlerden biridir.

• HackerDefender - bu erken Truva atı, işletim sistemini çok düşük düzeyde işlev çağrılarında değiştirdi / artırdı.

• Machiavelli - Mac OS X'i hedefleyen ilk rootkit 2009'da çıktı. Bu rootkit, gizli sistem çağrıları ve çekirdek iş parçacıkları oluşturur.

• Yunan telefon dinleme - 2004 / 05'te davetsiz misafirler Ericsson'un AX PBX'ini hedef alan bir rootkit kurdu.

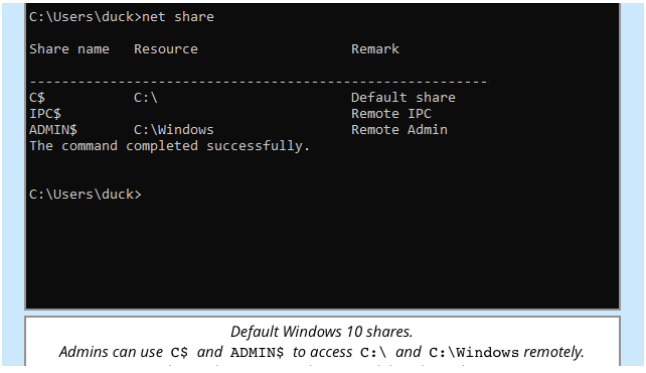
• İlk olarak Temmuz 2007'de tespit edilen Zeus, tarayıcıdaki tuşa basarak günlük kaydı ve form kapma yoluyla bankacılık bilgilerini çalan bir Truva atıdır.

• Stuxnet - endüstriyel kontrol sistemleri için bili-

nen ilk rootkit

• Flame - 2012'de keşfedilen ve Windows işletim sistemi çalıştıran bilgisayarlara saldıran kötü amaçlı bir bilgisayar. Ses, ekran görüntüleri, klavye etkinliği ve ağ trafiğini kaydedebilir. En önemlisi 2012'de İran petrol rafinerisi üretimini bozmak için kullanıldı.

Backdoors: Bir backdoors yazılımı, bir web sunucusu veya veritabanı gibi bir sisteme erişmek için gereken normal kimlik doğrulamasını geçersiz kılar. Çoğu zaman kurulumu hedeflenen bir saldırının parçasıdır; Bir kurbanı araştırdıktan sonra, sosyal mühendislik, oturum açma kimlik bilgilerini çalmak ve bir uygulamaya erişim sağlamak için kullanılır. Backdoors yazılımı tespit edilmekten kaçınır ve bir kontrol merkezi kurmak için kullanılır. Bu durum , failin kötü amaçlı yazılımları uzaktan güncellemesine ve sistem komutlarını başlatmasına olanak tanır.



Resim 19: Backdoor Komut Dizini Örneği

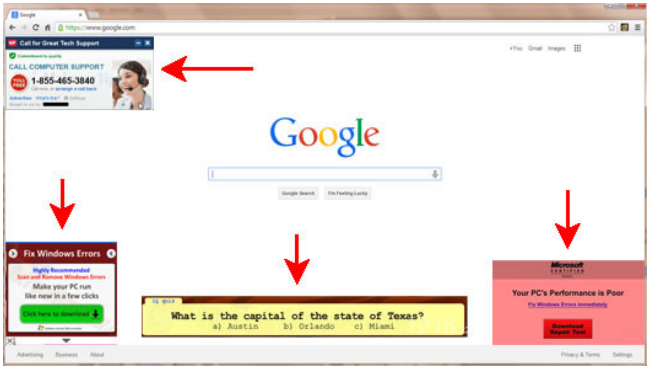
Backdoors veri hırsızlığı, hizmet reddi saldırıları ve ziyaretçilerinizin bilgisayarlarına virüs bulaşması gibi birçok kötü amaçlı etkinlik için kullanılır. Ayrıca, gelişmiş bir kalıcı tehdit (APT) saldırıları gerçekleştirirken de ilk adımdır.

Backdoors, kuruluşlar tarafından kullanılan güvenlik Wi-Fi kameraları gibi bir dizi Nesnelerin İnterneti (IoT) cihazında son zamanlarda bulundu. Bir IoT cihazı hacklendiğinde ve bir backdoors yazılımına dönüştürüldüğünde bu durum ağa etkili bir şekilde sızmak için bir ağ geçidi sağlar.

Reklam Yazılımı (Adware): Reklam yazılımı, bir program çalışırken reklam afişlerinin görüntülendiği herhangi bir yazılım uygulamasıdır. Reklamlar, programın kullanıcı arayüzünde görünen pop-up pencereler veya çubuklar aracılığıyla sunulur. Reklam yazılımı genellikle bilgisayarlar için oluşturulur, ancak mobil cihazlarda da bulunabilir. Reklam yazılımlarının gerekçesi, yazılım geliştiricisi için programlama geliştirme maliyetlerini kurtarmaya yardımcı olması ve kullanıcı maliyetini düşürmesi veya ortadan kaldırmasıdır.

Reklam yazılımı türleri

Bazı yasal uygulama yazılımları, reklam destekli ücretsiz bir sürüm olarak veya reklamsız ücretli bir sürüm olarak sunulur. Kullanıcılar, reklamsız bir deneyim için bir yazılım lisans kodu veya ayrı bir yazılım parçası satın alacaklardı. Bu tür bir reklam yazılımı, kullanıcılara büyük ödemeler yapmadan yazılıma erişme fırsatı verir.



Resim 20: Reklam Yazılımı(Adware) Komut Dizini Örneği

Reklam yazılımları, genellikle kullanıcıların kişisel bilgilerini ve internette gezinme alışkanlıklarını izleyen

ve kaydeden kod içerdiği için eleştirildi. Bu veriler, özelleştirilmiş reklamların görüntülenmesi için kullanıcının izni ile kullanılabilirken, yazılım, kullanıcının bilgisi ve yetkisi olmadan yapılırsa casus yazılım olarak sınıflandırılabilir. Bu şekilde toplanan kullanıcı verileri genellikle üçüncü şahıslara satılır. Bu müdahaleci uygulamalar, Elektronik Gizlilik Bilgi Merkezi de dahil olmak üzere bilgisayar güvenliği ve gizlilik savunucularının tepkisine neden olmuştur.

Kötü amaçlı reklam yazılımları veya casus yazılımlar, ücretsiz yazılımlar, paylaşılan yazılım programları ve internetten indirilen yardımcı programlarla birlikte paketlenmiş olabilir veya kullanıcı virüslü bir web sitesini ziyaret ettiğinde kullanıcının cihazına gizlice yüklenebilir. Söz konusu reklam yazılımı kötü amaçlı olsun ya da olmasın, reklam yazılımları genellikle kötü amaçlı yazılım önleme programları tarafından potansiyel olarak istenmeyen program olarak işaretlenir.

Algılama ve kaldırma araçları

Veri kullanımında bir artış, kullanıcının web tarayıcısında yeni araç çubuklarının ortaya çıkması , kullanıcının internet aramalarının reklam web sitelerine yeniden yönlendirilmesi, pop-up'ta istenmeyen reklamların görünmesi, kolayca kapatılamayan pencereler veya cihaz yavaş olması durumunda bir kullanıcının cihazına kötü amaçlı reklam yazılımı bulaşmış olabilir..

Uç nokta güvenlik paketlerinin çoğu, reklam yazılımı, casus yazılım ve diğer kötü amaçlı yazılım programlarını tarama ve kaldırma yeteneğine sahiptir. Adblocker yazılımları ile kötü amaçlı reklam yazılımlarının aramasına ve kaldırmasına yardımcı olmak için ücretsiz olarak sunulmaktadır.

Önleme

Reklam yazılımı bulaşmasını önlemek için, kullanıcılar çevrimiçi olarak indirdikleri yazılım türlerini ayırt etmeli, yazılım yazarlarının cihazlarında bilgi toplama işlemi yapıp yapmayacağını öğrenmek için ücretsiz yazılımı indirmeden önce son kullanıcı lisans sözleşmelerini okumalı , bir açılır pencere kullanmalıdır. beklenmedik pencerelerin açılmasını önlemek için reklam engelleyici ve güvenilen bir sitede görüntülenmiyorlarsa reklamlara tıklamaktan kaçınmalıdır.

Casus Yazılım(Spyware): Casus yazılım bir tür kötü amaçlı yazılımdır (veya "kötü amaçlı yazılım") kullanıcının izni olmadan bir bilgisayar veya ağ hakkında bilgi toplayan ve paylaşan. Orijinal yazılım paketlerinin gizli bir bileşeni olarak veya aldatıcı reklamlar, web siteleri, e-posta, anlık mesajlar ve doğrudan dosya paylaşım bağlantıları gibi geleneksel kötü amaçlı yazılım vektörleri aracılığıyla yüklenebilir. Diğer kötü amaçlı yazılım türlerinden farklı olarak, casus yazılımlar yalnızca suç örgütleri tarafından değil, aynı zamanda vicdansız reklamcılar ve casus yazılımları kullanıcıların rızaları olmadan pazar verilerini toplamak için kullanan şirketler tarafından da yoğun bir şekilde kullanılmaktadır. Casus yazılım, kaynağı ne olursa olsun, kullanıcıdan gizlenir ve tespit edilmesi genellikle zordur, ancak sistem performansının düşmesi ve yüksek sıklıkta istenmeyen davranışlar (açılır pencereler, yeniden yönlendirilen tarayıcı ana sayfası, arama sonuçları vb.) Gibi belirtilere yol açabilir. .

Resim 21: Casus Yazılım(Spyware)

Casus yazılım, ağ oluşturma yetenekleriyle de dikkate değerdir. Casus yazılım bu bilgiyi saldırgana geri

veremezse, bilgi bulmak için virüslü bir sistemi kullanmak çok az değerlidir. Sonuç olarak, casus yazılım, şüpheye neden olmayacak veya ağ güvenliği ekiplerinden dikkat çekmeyecek bir şekilde saldırganla iletişime geçmek için çeşitli teknikler kullanır.

Bir reklam aracı olarak casus yazılım, kullanıcı bilgilerini toplamak ve ilgilenen reklam verenlere veya diğer ilgili taraflara satmak için kullanılır. Casus yazılımlar, web'de gezinme alışkanlıkları ve indirme etkinliği dahil hemen hemen her tür veriyi toplayabilir. Belki de casus yazılımla ilgili en büyük endişe, varlığının tespit edilip edilmediğine bakılmaksızın, kullanıcının hangi bilgilerin yakalandığı, gönderildiği veya kullanıldığına dair herhangi bir fikrinin veya bulmak için herhangi bir mekanizmanın veya teknolojinin olmamasıdır.

Casus yazılımlar, kullanıcının adı, adresi, parolaları, banka ve kredi bilgileri ve sosyal güvenlik bilgileri gibi kişisel ayrıntıları elde etmek için tuş kaydedicileri kullanabilir. Dosyaları sistemin sabit sürücüsüne tarayabilir, diğer uygulamaları izleyebilir, ek casus yazılımlar yükleyebilir, tanımlama bilgilerini okuyabilir ve sistemin internet ayarlarını ve dinamik olarak bağlantılı kitaplıkları (DLL) değiştirebilir. Bu, güvenlik ayarlarının düşürülmesine (daha fazla kötü amaçlı yazılım davet etmek için) ve internette ve bilgisayarda, ister çevrimiçi ister çevrimdışı olsun, sayısız açılır reklamdan sistemin İnternet ayarlarından kaynaklanan bağlantı arızalarına kadar değişen arızalara neden olabilir. Bu değişikliklerin çoğunun, etkilenen cihazı yeniden görüntülemeden geri döndürmek veya kurtarmak zordur.

Casus yazılımların virüs bulaşmış bilgisayarlara oluşturduğu belirtilen tehditlere ek olarak, genellikle işlemci gücünü, RAM'i, diskleri ve ağ trafiğini saran sistem kaynaklarının büyük bir tüketicisi de olabilir. Ortaya çıkan performans düşüşü, çökmelere veya genel sistem kararsızlığına neden olabilir. Bazı casus yazılımlar, rakip casus yazılım programlarını devre dışı bırakır veya ortadan kaldırır ve kullanıcının onu kaldırma girişimlerini algılayabilir ve durdurabilir.

Casus yazılımlar, uç nokta ve ağ güvenlik kontrollerinin bir kombinasyonu yoluyla önlenebilir. Casus yazılım önleme özellikleri, genellikle uç noktada koruma sağlayan modern antivirüs yazılım ürünlerine entegre edilir. Casus yazılımların ağ üzerinden iletişim kurma ihtiyacı göz önüne alındığında, casus yazılımlar, casus yazılım iletişimlerinin algılanıp engellenebildiği ağ güvenlik katmanında da giderek daha fazla kontrol edilmektedir. Ek olarak, kullanıcının izni olmadan dosyaların indirilmesini engelleyen yeni nesil ağ kontrollerinin yanı sıra tarayıcının açılır pencere engelleyicisi kullanılarak son noktada arabadan indirme korumaları da uygulanabilir.

Casus yazılım türleri

• İzleme tanımlama bilgileri (Tracking cookies): Daha az müdahaleci olma eğiliminde olsalar da reklam yazılımlarına benzerler.

• Tuş kaydediciler (Keyloggers): Çevrimiçi hesaplarınızda oturum açtığınızda kullandığınız tuş vuruşları da dahil olmak üzere, yanlış bir kullanıcının klavyenizdeki her tuş vuruşunu yakalamasına izin verir.

• Takip yazılımı (Stalkerware): Genellikle bir cep telefonuna yüklenir, böylece telefonun sahibi üçüncü bir şahıs tarafından izlenebilir.

• Hırsızlık Yazılımı (Stealware): Ürün sayfalarına trafik gönderen web sitelerine kredi veren çevrimiçi alışveriş sitelerinden yararlanmak için tasarlanmıştır. Bir kullanıcı bu sitelerden birine gittiğinde, hırsızlık yazılımı isteği durdurur ve kullanıcıyı oraya göndermek için sorumluluk alır.

• Sistem monitörleri (System monitors): Tuş vuruşlarından, e-postalardan ve sohbet odası diyaloglarından ziyaret edilen web sitelerine, başlatılan programlara ve yapılan telefon görüşmelerine kadar bir cihazda olan her şeyi kaydeder ve bunu bir meraklı veya siber suçluya gönderir. Ayrıca bir sistemin süreçlerini izleyebilir ve sistemdeki güvenlik açıklarını belirleyebilirler.

Casus Yazılım Nasıl Önlenir?

Dosyaları indirirken de dikkatli olunmalıdır. Dosyalar yalnızca güvenilir sitelerden indirilmelidir. İyi bir virüsten koruma veya kötü amaçlı yazılım önleme programınız varsa, çoğu durumda virüs bulaşmış indirmeleri işaretler. Güvenlik yazılımınızın saygın bir satıcıdan geldiğinden emin olun. Kötü amaçlı yazılım yazarlarının, mallarını sahte antivirüs uygulamalarına gömdükleri bilinmektedir.

Cep telefonları için, uygulamaları Android telefonlar için Google Play'den ve iOS cep telefonları için App Store'dan indirmek en iyisidir. Casus yazılımlarla ilgili endişeleriniz varsa, bir Android telefonun "köklenmesi" veya bir iPhone'un "hapse atılması" da önlenmelidir. Kurumsal bir ortamda, bunu bir politika haline getirmek akıllıca olacaktır. İndirmeyi yalnızca onaylı uygulamalarla sınırlayan mobil cihaz yönetimi (MDM) yazılımını kullanmak da iyi bir seçenektir.

Ayrıca, birisinin telefonunuza casus yazılım yüklemek için fiziksel olarak erişmesi olası olmasa da, telefonunuz için her zaman yalnızca sizin bildiğiniz bir kilit kodu oluşturun. Bu, birçok kurumsal ortamda bir gerekliliktir.

Tıkladığınız bağlantılar, açtığınız ekler ve indirdiğiniz dosyalar konusunda dikkatli olsanız bile, yine de arabayla gelen bulaşmalar tarafından hedeflenmiş olabilirsiniz. Arabadan geçme saldırıları genellikle kurbanlarını etkilemek için tarayıcı güvenlik açıklarına dayandığından, tarayıcı sürümünüzü güncel tutarak arabadan geçme bulaşma riski azaltılabilir.

Casus yazılımlar sıklıkla açılır pencerelere ve reklamlara bağlı olduğundan, bu kötü amaçlı yazılım kanallarını ele alabileceğiniz birkaç adım vardır. Hem Mozilla Firefox hem de Google Chrome, yerleşik açılır pencere engelleyicilere sahiptir. Tüm açılır pencereleri engelleyecek veya bir web sitesi bir açılır pencere başlatmak istediğinde sizi uyaracak şekilde yapılandırılabilirler, böylece onu görmek isteyip istemediğinize karar verebilirsiniz. Ayrıca güvenilir sitelerden pop-up'lara otomatik olarak izin verebilirsiniz.

Kötü amaçlı reklam tehditleri, zaten bu özelliğe sahip değilse, tarayıcınıza bir reklam engelleyici yüklenerek giderilebilir. AdBlock Plus, reklamları engellemek için en popüler programlardan biridir. Ghostery gibi izleme önleyici yazılımlar, casus yazılım bulaşma riskini azaltmak için değerli bir tarayıcı eklentisi olabilir.

Kurumsal bir ortamda, iyi bir uç nokta koruma çözümü çoğu reklam yazılımını algılayacaktır. Yine de en etkili olabilecek şey, çalışanlara reklam yazılımlarından ve diğer kötü amaçlı yazılım bulaşmalarından nasıl kaçınacaklarını öğreten güçlü bir güvenlik bilinci programıdır.

Casus yazılım nasıl kaldırılır?

Bilgisayarınız alışılmadık derecede yavaş görünüyorsa veya çok sık çöküyorsa, tarayıcınız açılır pencerelerle doluysa veya şüpheli sabit sürücü etkinliği görmeye başlarsanız, casus yazılımlardan kaçınma çabalarınız başarısız olmuş olabilir. Bu durum enfeksiyonu gidermeniz gerektiği anlamına gelir.

Her türlü kötü amaçlı yazılımı manuel olarak kaldırmak zordur, ancak casus yazılımlarda daha da fazla olabilir. Kötü amaçlı yazılım gizli olacak şekilde tasarlanmıştır. Bu, simgeler gibi varlığının açık işaretlerini gizleyeceği anlamına gelir. Sistem kaynaklarını kontrol etmek de çıkmaz bir yol olabilir. Casus yazılım yazarları, kimliklerini gizlemek için genellikle dosyalarını gerçek sistem dosyalarının adlarını taklit edecek şekilde adlandırırlar.

Bazıları ücretsiz olan bir dizi program casus yazılımları algılayabilir ve kaldırabilir. SUPERAntiSpyware, Malwarebytes, Avast Free Antivirus, AVG AntiVirus, Adaware, Trend Micro HouseCall, SpywareBlaster ve SpyBot Search & Destroy içerir. Ayrıca, Actiance Security Labs, binlerce casus yazılım programını sistemlerden kaldırmaya yönelik araçlara bağlantılar içeren bir

Casus Yazılım Kılavuzu tutar.

Smishing: Smishing, kurbanları aldatmak için yanıltıcı metin mesajları kullanan bir siber saldırıdır. Amaç, sizi güvendiğiniz bir kişi veya kuruluştan bir mesaj geldiğine inanmanız için kandırmak ve ardından sizi saldırgana istismar edilebilir bilgiler (örneğin banka hesabı oturum açma kimlik bilgileri gibi) veya mobil cihazınıza erişim sağlayan bir işlem yapmaya ikna etmektir.

Smishing, 1990'lardan beri var olan e-posta tabanlı kimlik avı dolandırıcılıklarının metin mesajı merkezli bir çeşididir . Ancak insanlar genellikle telefonlarındaki şüpheli mesajlara bilgisayarlarından daha az dikkat ederler: potansiyel olarak şüpheli bir metin mesajı açma olasılıkları bir e-posta mesajına göre daha yüksektir ve kişisel cihazları genellikle kurumsal bilgisayarlarda bulunan güvenlik türünden yoksundur. Eski bir numaraya yapılan bu kötücül yeni yaklaşım giderek yaygınlaşıyor.

Spoofing (Adres Sahteciliği): Adres sahteciliği, bilinmeyen bir kaynaktan gelen bir iletişimi bilinen, güvenilir bir kaynaktan geliyormuş gibi gizleme eylemidir. Adres sahteciliği, e-postalara, telefon aramalarına ve web sitelerine uygulanabilir veya bir IP adresi sahtekarlığı yapan bir bilgisayar, Adres Çözümleme Protokolü (ARP) veya Etki Alanı Adı Sistemi (DNS) sunucusu gibi daha teknik olabilir.

Adres sahteciliği, bir hedefin kişisel bilgilerine erişmek, kötü amaçlı yazılımları virüslü bağlantılar veya ekler aracılığıyla yaymak, ağ erişim denetimlerini atlamak veya bir hizmet reddi saldırısı gerçekleştirmek için trafiği yeniden dağıtmak için kullanılabilir. Adres sahteciliği, genellikle kötü bir aktörün gelişmiş bir kalıcı tehdit veya ortadaki adam saldırısı gibi daha büyük bir siber saldırıyı gerçekleştirmek için erişim sağlama yoludur.

Kuruluşlara yönelik başarılı saldırılar, virüs bulaşmış bilgisayar sistemlerine ve ağlarına, veri ihlallerine ve / veya gelir kaybına yol açabilir - bunların tümü kuruluşun kamusal itibarını etkileme eğilimindedir. Ayrıca, internet trafiğinin yeniden yönlendirilmesine yol açan sahtekarlık, ağları bunaltabilir veya müşterileri / müşterileri bilgi çalmayı veya kötü amaçlı yazılımları dağıtmayı amaçlayan kötü amaçlı sitelere yönlendirebilir.

Spoofing (Adres Sahteciliği) Türleri

• E-posta Sahtekarlığı

E-posta sahtekarlığı, bir saldırgan bir alıcıyı kandırmak için bir e-posta mesajı kullandığında, bunun bilinen veya güvenilir bir kaynaktan geldiğini düşünmesi durumunda ortaya çıkar. Bu e-postalar, kötü amaçlı web sitelerine veya kötü amaçlı yazılım bulaşmış eklere bağlantılar içerebilir veya alıcıyı hassas bilgileri özgürce ifşa etmeye ikna etmek için sosyal mühendislik kullanabilir.

Gönderen bilgilerinin yanıltılması kolaydır ve iki yoldan biriyle yapılabilir:

• Orijinalinden yalnızca biraz farklı görünmek için güvenilir bir e-posta adresini veya etki alanını alternatif harfler veya sayılar kullanarak taklit etmek

• 'Kimden' alanını bilinen ve / veya güvenilir bir kaynağın tam e-posta adresi olacak şekilde gizleme

• Arayan Kimliği Sahtekarlığı

Günümüzde en çok kullanılan yöntemlerden bir tanesi olan arayan kimliği sahtekarlığı ile saldırganlar, telefon aramalarının belirli bir numaradan geliyormuş gibi görünmesini sağlayabilir ya alıcı tarafından bilinen veya güvenilen bir numara ya da belirli bir coğrafi konumu gösteren bir numara ile arama yapmaktadır. Saldırganlar daha sonra hedeflerini telefon üzerinden parolalar, hesap bilgileri, sosyal güvenlik numaraları ve daha fazlası gibi hassas bilgileri sağlamaya ikna etmek için genellikle bir banka, polis, savcı veya müşteri desteğinden biri gibi görünen sosyal mühendisliği kullanabilir.

• Web Sitesi Sahtekarlığı

Web sitesi sahtekarlığı, bir web sitesinin kullanıcı tarafından bilinen veya güvenilen mevcut bir siteyi taklit edecek şekilde tasarlanması anlamına gelir. Saldırganlar, kullanıcılardan oturum açma ve diğer kişisel bilgileri almak için bu siteleri kullanır.

• IP Sahtekarlığı

Saldırganlar, bir bilgisayarın IP adresini gizlemek için IP (İnternet Protokolü) sahtekarlığını kullanabilir. Böylece gönderenin kimliğini gizleyebilir veya başka bir bilgisayar sistemini taklit edebilir. IP adresi sahtekarlığının bir amacı, IP adreslerine dayalı olarak kullanıcıların kimliğini doğrulayan ağlara erişim sağlamaktır.

Bununla birlikte, saldırganlar, kurbanı trafiğe boğmak için daha sık olarak, hizmet reddi saldırısında hedefin IP adresini taklit eder. Saldırgan, paketleri birden çok ağ alıcısına gönderir ve paket alıcıları bir yanıt ilettiğinde, hedefin sahte IP adresine yönlendirilir.

• ARP Sahtekarlığı

Adres Çözümleme Protokolü (ARP), veri iletimi için IP adreslerini Ortam Erişim Kontrolü (MAC) adreslerine çözen bir protokoldür. ARP sahtekarlığı, bir saldırganın MAC'ini meşru bir ağ IP adresine bağlamak için kullanılır, böylece saldırgan, bu IP adresiyle ilişkilendirilmiş sahibine yönelik verileri alabilir. ARP sahtekarlığı genellikle verileri çalmak veya değiştirmek için kullanılır. Ancak aynı zamanda hizmet reddi ve ortadaki adam saldırılarında veya oturum kaçırmada da kullanılabilir.

• DNS Sunucusu Sahtekarlığı

DNS (Alan Adı Sistemi) sunucuları, URL'leri ve e-posta adreslerini karşılık gelen IP adreslerine çözümler. DNS sahtekarlığı, saldırganların trafiği farklı bir IP adresine yönlendirmesine izin vererek kurbanları kötü amaçlı yazılım yayan sitelere yönlendirir.

Cyberbullying (Siber Zorbalık): Siber zorbalık, cep telefonları, bilgisayarlar ve tabletler gibi dijital cihazlarda gerçekleşen zorbalıktır. Siber zorbalık; SMS, Metin ve uygulamalar aracılığıyla veya insanların içeriği görüntüleyebileceği, katılabileceği veya paylaşabileceği sosyal medyada, forumlarda veya oyunlarda çevrimiçi olarak gerçekleşebilir. Siber zorbalık, başka biri hakkında olumsuz, zararlı, yanlış veya kaba içerik göndermeyi, yayınlamayı veya paylaşmayı içerir. Başkası hakkında utanç veya aşağılanmaya neden olan kişisel veya özel bilgilerin paylaşılmasını içerebilir. Bazı siber zorbalık, çizgiyi aşarak yasa dışı veya suç teşkil eden davranışlara dönüşür.

Siber zorbalığın meydana geldiği en yaygın yerler şunlardır:

• Facebook, Instagram, Snapchat ve Tik Tok gibi Sosyal Medya

• Mobil veya tablet cihazlarda yazılı mesajlaşma ve mesajlaşma uygulamaları

• İnternet üzerinden anında mesajlaşma, doğrudan mesajlaşma ve çevrimiçi sohbet

• Reddit gibi çevrimiçi forumlar, sohbet odaları ve mesaj panoları

• E-posta

• Çevrimiçi oyun toplulukları

Spear Phishing (Hedefli Kimlik Avı) : Hedefli kimlik avı, hesap kimlik bilgileri veya belirli bir kurbandan mali bilgiler gibi hassas bilgileri genellikle kötü niyetli nedenlerle çalmaya yönelik hedefli bir girişimdir. Mağdurun arkadaşları, memleketleri, işverenleri, sık sık bulundukları yerler ve son zamanlarda çevrimiçi olarak ne satın aldıkları gibi kişisel ayrıntıları elde ederek elde edilir. Saldırganlar daha sonra, genellikle e-posta veya diğer çevrimiçi mesajlaşma yoluyla hassas bilgileri elde etmek için kendilerini güvenilir bir arkadaş veya varlık olarak gizler. Bu saldırıların % 91'ini oluşturan, internet üzerinden gizli bilgi edinmenin en başarılı şeklidir.

Phishing ve Spear Phishing Arasındaki Fark

Spear Phishing (hedefli kimlik avı), Phishing (kimlik avıyla) kolayca karıştırılabilir. Çünkü her ikisi de gizli bilgileri elde etmeyi amaçlayan kullanıcılara yönelik çevrimiçi saldırılardır. Kimlik avı, kurbanları kötü niyetli nedenlerle parolalar, kullanıcı adları ve kredi kartı bilgileri gibi hassas bilgileri paylaşmaları için kandırmaya yönelik herhangi bir girişim için daha geniş bir terimdir. Saldırganlar genellikle kendilerini güvenilir bir varlık olarak gizler ve hedefleriyle e-posta, sosyal medya, telefon görüşmeleri (genellikle sesli kimlik avı için "vishing" olarak adlandırılır) ve hatta metin mesajları (genellikle SMS ile kimlik avı için "smishing" olarak adlandırılır) aracılığıyla iletişim kurarlar.

Spear-phishing saldırılarının aksine, phishing saldırıları kurbanlarına göre kişiselleştirilmez ve genellikle aynı anda kitlelere gönderilir. Kimlik avı saldırılarının amacı, gerçek bir kuruluştan çok sayıda kişiye geliyormuş gibi görünen sahte bir e-posta (veya başka bir iletişim) göndererek, birinin bu bağlantıya tıklayıp kişisel bilgilerini sağlama şansına güvenmektir.

Phishing(Kimlik Avı): Kimlik avı, bireyleri kişisel olarak tanımlanabilen bilgiler, bankacılık ve kredi kartı bilgileri ve parolalar gibi hassas verileri sağlamaya teşvik etmek için meşru bir kurum gibi davranan biri tarafından bir hedef veya hedefle e-posta, telefon veya kısa mesaj yoluyla iletişime geçildiği bir siber suçtur.

Kimlik Avı E-postalarının Ortak Özellikleri

1. Gerçek Olamayacak Kadar İyi: Karlı teklifler ve göz alıcı veya dikkat çekici ifadeler, insanların dikkatini hemen çekmek için tasarlanmıştır. Örneğin, birçoğu bir iPhone, bir piyango veya başka bir lüks ödül kazandığınızı iddia ediyor.

2. Aciliyet Duygusu: Siber suçlular arasında en sevilen taktik sizden hızlı davranmanızı istemektir. Çünkü süper fırsatlar yalnızca sınırlı bir süre için geçerlidir. Hatta bazıları size yanıt vermek için yalnızca birkaç dakikanız olduğunu söyleyecektir. Bu tür e-postalarla karşılaştığınızda, onları görmezden gelmek en iyisidir. Bazen, kişisel bilgilerinizi hemen güncellemediğiniz sürece hesabınızın askıya alınacağını söylerler. Güvenilir kuruluşların çoğu, bir hesabı sonlandırmadan önce bolca zaman ayırır ve kullanıcılardan kişisel bilgilerini İnternet üzerinden güncellemelerini asla istemezler. Şüphe duyduğunuzda, e-postadaki bir bağlantıya tıklamak yerine doğrudan kaynağı ziyaret edin.

3. Köprüler(Linkler) : Bir bağlantı göründüğü kadarıyla olmayabilir. Bir bağlantının üzerine gelmek, tıkladığınızda yönlendirileceğiniz gerçek URL'yi gösterir. Tamamen farklı olabilir veya yanlış yazım içeren popüler bir web sitesi olabilir.

4. Ekler: Bir e-postada beklemediğiniz veya bu mantıklı olmayan bir ek görürseniz, açmayın! Genellikle fidye yazılımı veya diğer virüsler gibi yükler içerirler. Tıklanması her zaman güvenli olan tek dosya türü bir .txt dosyasıdır.

5. Olağandışı Gönderen: Tanımadığınız birinden ya da tanıdığınız birinden geliyormuş gibi görünse de, herhangi bir şey olağan dışı, beklenmedik, karakter dışı veya genel olarak şüpheli görünüyorsa, üzerine tıklamayın!

GÜVENLİK TESTİ TÜRLERİ

Dinamik Uygulama Güvenliği Testi (DAST) : Bu otomatik uygulama güvenlik testi, yasal güvenlik değerlendirmelerine uyması gereken dahili olarak karşılaşılan, düşük riskli uygulamalar için en iyisidir. Orta riskli uygulamalar ve küçük değişiklikler geçiren kritik uygulamalar için, DAST'ı yaygın güvenlik açıklarına yönelik bazı manuel web güvenlik testleriyle birleştirmek en iyi çözümdür.

Statik Uygulama Güvenliği Testi (SAST) : Bu uygulama güvenliği yaklaşımı, otomatik ve manuel test teknikleri sunar. Bir üretim ortamında uygulamaları yürütmeye gerek kalmadan hataları tanımlamak için en iyisidir. Ayrıca, geliştiricilerin kaynak kodunu taramasına ve yazılım güvenlik açıklarını sistematik olarak bulup

EĞLENELİM ÖĞRENELİM

R A Q X S S W O I T Y B E R N S O W
M S P E A R O O F Y E C D I E P N G
R A F C Y I U P K L Y M R N B E V C
A T G T Y E W Q A B F T O H J A J L
N Y N X C B M M E N B V W G H R Y P
S Z I Q A U E R I E O O S E A P M Z
O W F I E T H R T U M N S B V H S S
M F O G K E L C B Z O O A Q W I E R
W T O P R Y U I O U P A P S D S F G
A L P O A C G N I V L M N L K H D H
R K S S M I S H I N G L S E K I S T
E S P O E P H N D W O E Y A Y N O N
T Q I U G N I H S I H P B I F G E M
E U H O W M U G W O R D S S N I N G
H I D O R E H R E B S L E V I G U W

Aşağıdaki siber güvenlik kavramlarını bulunuz.

- ○ SMISHING
- ○ SPOOFING
- ○ CYBERBULLYING
- ○ SPEAR PHISHING
- ○ RANSOMWARE
- ○ PASSWORD
- ○ CYBERHERO
- ○ PHISHING

ortadan kaldırmasına olanak tanır.

Penetrasyon Testi : Bu manuel uygulama güvenlik testi, özellikle büyük değişiklikler geçiren kritik uygulamalar için en iyisidir. Değerlendirme, gelişmiş saldırı senaryolarını keşfetmek için iş mantığını ve rakip tabanlı testleri içerir.

Çalışma Zamanı Uygulaması Kendi Kendini Koruması (RASP) : Bu gelişen uygulama güvenliği yaklaşımı, saldırıların gerçek zamanlı olarak yürütülürken izlenebilmesi ve ideal olarak engellenebilmesi için bir uygulamayı araç olarak kullanmak için bir dizi teknolojik tekniği kapsamaktadır.

SIZMA TESTİ

Penetrasyon testi olarak da bilinen sızma testi, istismar edilebilir güvenlik açıklarını kontrol etmek için bilgisayar sisteminize karşı simüle edilmiş bir siber saldırıdır. Web uygulaması güvenliği bağlamında sızma testi genellikle bir web uygulaması güvenlik duvarını (WAF) artırmak için kullanılır.

Sızma testi, kod yerleştirme saldırılarına açık olan temizlenmemiş girdiler gibi güvenlik açıklarını ortaya çıkarmak için herhangi bir sayıda uygulama sisteminin (örneğin, uygulama protokol arabirimleri (API'ler), ön uç / arka uç sunucuları) ihlal edilmeye çalışılmasını içerebilir.

Sızma testi tarafından sağlanan içgörüler, WAF güvenlik politikalarınızda ince ayar yapmak ve tespit edilen güvenlik açıklarını yamalamak için kullanılabilir.

Penetrasyon testi aşamaları

Sızma testi süreci beş aşamaya ayrılabilir.

Resim 22: Penetrasyon Testi Aşamaları

1. Planlama ve keşif

İlk aşama şunları içerir:

• Ele alınacak sistemler ve kullanılacak test yöntemleri dahil olmak üzere bir testin kapsamını ve hedeflerini tanımlama.

• Bir hedefin nasıl çalıştığını ve potansiyel güvenlik açıklarını daha iyi anlamak için istihbarat toplamak (örneğin, ağ ve alan adları, posta sunucusu).

2. Tarama

Bir sonraki adım, hedef uygulamanın çeşitli izinsiz giriş girişimlerine nasıl yanıt vereceğini anlamaktır. Bu genellikle şu şekilde yapılır:

• Statik analiz: Çalışırken nasıl davrandığını tahmin etmek için bir uygulamanın kodunu inceleme. Bu araçlar, kodun tamamını tek geçişte tarayabilir.

• Dinamik analiz: Çalışır durumda bir uygulamanın kodunu inceleme. Bu, bir uygulamanın performansına gerçek zamanlı bir görünüm sağladığı için daha pratik bir tarama yöntemidir.

3. Erişim Sağlamak

Bu aşama, bir hedefin güvenlik açıklarını ortaya çıkarmak için siteler arası komut dosyası oluşturma, SQL injection ve arka kapılar gibi web uygulaması saldırılarını kullanır. Test uzmanları daha sonra neden olabilecekleri zararı anlamak için genellikle ayrıcalıkları artırarak, verileri çalarak, trafiğe müdahale ederek vb. bu güvenlik açıklarından yararlanmaya çalışır.

4. Erişimi Sürdürmek

Bu aşamanın amacı, güvenlik açığının, kötü bir aktörün derinlemesine erişim elde etmesi için yeterince uzun süre, sömürülen sistemde kalıcı bir varlık elde etmek için kullanılıp kullanılamayacağını görmektir. Buradaki fikir, bir kuruluşun en hassas verilerini çalmak için genellikle aylarca sistemde kalan gelişmiş kalıcı tehditleri taklit etmektir.

5. Analiz

Sızma testinin sonuçları daha sonra aşağıdaki ayrıntıları içeren bir rapor halinde derlenir:

• Sömürülen belirli güvenlik açıkları

• Erişilen hassas veriler

• Penetrasyon test cihazının sistemde tespit edilmeden kaldığı süre

Bu bilgiler doğrultusunda güvenlik açıklarını yamalamak ve gelecekteki saldırılara karşı korumak için bir kuruluşun WAF ayarlarını ve diğer uygulama güvenlik çözümlerini yapılandırmaya yardımcı olmak için güvenlik personeli tarafından analiz edilir.

Penetrasyon Testi Yöntemleri

1. Harici test

Harici sızma testleri, bir şirketin internette görünen varlıklarını, örneğin web uygulamasının kendisini, şirketin web sitesini ve e-posta ve alan adı sunucularını (DNS) hedefler. Amaç, erişim sağlamak ve değerli verilere ulaşmaktır.

2. Dahili test

Dahili bir testte, güvenlik duvarının arkasındaki bir uygulamaya erişimi olan bir test cihazı içeriden kötü niyetli bir kişinin saldırısını simüle eder. Burada amaç mutlaka kötü amaçlı bilgi hırsızı bir çalışanı simüle etmek değildir. Yaygın bir başlangıç senaryosu, kimlik avı saldırısı nedeniyle kimlik bilgileri çalınan bir çalışan olabilir.

3. Kör test

Kör testte, test uzmanına yalnızca hedeflenen kuruluşun adı verilir. Güvenlik personeline gerçek bir uygulama saldırısının nasıl gerçekleşeceğine dair gerçek

zamanlı bir bakış sağlar.

4. Çift kör test

Çift kör testte, güvenlik personelinin simüle edilmiş saldırı hakkında önceden bilgisi yoktur. Gerçek dünyada olduğu gibi, bir ihlal girişiminden önce savunmalarını güçlendirmek için zamanları olmayacak.

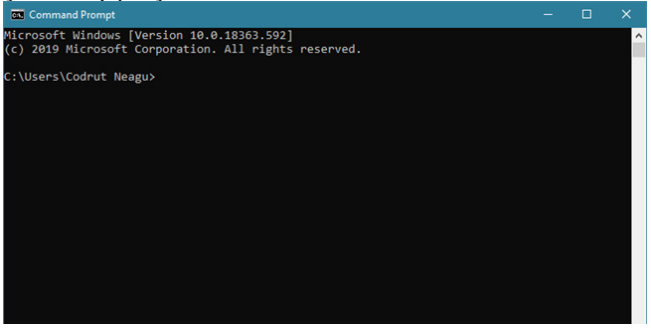
5. Hedeflenen test

Bu senaryoda, hem test cihazı hem de güvenlik personeli birlikte çalışır ve hareketlerini birbirlerini değerlendirir. Bir bilgisayar korsanının bakış açısından gerçek zamanlı geri bildirim sağlayan bir güvenlik ekibine sağlayan değerli bir eğitim alıştırmasıdır.

SİBER GÜVENLİK CMD KOMUTLARI

Komut İstemi nedir?

Komut İstemi ve CMD , Windows işletim sistemlerinde bulunan bir uygulamadır. Teknik açıdan, Komut İstemi bir komut satırı yorumlayıcısıdır ve amacı, özel bir sözdizimi kullanarak komutlar girmenize izin vermektir. Komut İstemi'ne gönderilen komutlar , klavyenizde Enter tuşuna basar basmaz işletim sistemi tarafından çalıştırılan metin satırları olarak girilir. Başlatmak için çalıştır kısmına cmd.exe yazabilir veya Başlat menüsünü açın ve tüm programların arasında göreceğiniz Komut İstemini ister sağ tıklayıp yönetici isterseniz de normal çift tıklayıp açabilirsiniz.



Resim 23: CMD Sistemi Arayüzü

Şimdi ağ ve siber güvenlik için kullanılan cmd komutlarını inceleyelim:

 # 1 Ping

Bu komut, bazı veri paketlerini belirli bir web adresine göndermek için internet bağlantınızı kullanır ve ardından bu paketler bilgisayarınıza geri gönderilir. Test, belirli bir adrese ulaşmak için geçen süreyi gösterir. Basit bir deyişle, ping attığınız sunucunun hayatta olup olmadığını bilmenize yardımcı olur. Ping komutunu, ana bilgisayarın TCP / IP ağına ve onun kaynaklarına bağlanabildiğini doğrulamanız gerektiğinde kullanabilirsiniz. Örneğin, Google'a ait olan Komut istemi ping 8.8.8.8'i yazabilirsiniz.

"8.8.8.8" i "www.google.com" olarak veya ping atmak istediğiniz başka bir şeyle değiştirebilirsiniz.

 # 2 nslookup

Herhangi bir belirli DNS kaydı için alan adı veya IP adresi eşlemesi elde etmenize yardımcı olan bir ağ yönetimi komut satırı aracıdır. Bir web sitesi URL'niz olduğunu, ancak IP Adresini öğrenmek istediğinizi varsayalım, CMD yazabilirsiniz.

nslookup www.google.com (Google.com'u IP adresini bulmak istediğiniz web sitenizin URL'si ile değiştirin)

 # 3 tracert

Trace Route, adı gibi, kullanıcıların bir hedefe ulaşmak için paketlenmiş bir IP'den daha rotayı izlemelerine izin verdiğini söyleyebilirsiniz. Komut, her atlamanın bir hedefe ulaşmak için geçen süreyi hesaplar ve görüntüler. Sadece yazman gerekiyor

tracert xxxx (IP Adresini biliyorsanız) veya tracert www.google.com yazabilirsiniz (IP adresini bilmiyorsanız)

 # 4 arp

Bu komut, ARP önbelleğini değiştirmenize yardımcı olur. Her bilgisayarda arp-a komutunu çalıştırarak, bilgisayarların aynı alt ağda başarılı bir şekilde ping atmak için birbirleri için listelenen doğru MAC adreslerine sahip olup olmadıklarını görebilirsiniz. Bu komut aynı zamanda kullanıcıların LAN'larında arp zehirlenmesi yapıp yapmadığını öğrenmelerine yardımcı olur. Komut isteminde arp-a yazmayı deneyebilirsiniz.

 # 5 ipconfig

Bu, yararlı olan her şeyi gösteren komuttur. Size IPv6 adresini, geçici IPv6 adresini, IPv4 adresini, Alt Ağ Maskesini, Varsayılan ağ geçidini ve bilmek istediğiniz diğer her şeyi gösterecektir. "İpconfig" veya " ipconfig / all " komut istemini yazabilirsiniz

 # 6 netstat

Bilgisayarınızla kimin bağlantı kurduğunu öğrenmek istiyorsanız, "netstat -a" komut istemini yazmayı deneyebilirsiniz, tüm bağlantı görüntülenecek ve aktif bağlantılar ve dinleme portları hakkında bilgi sahibi olacaksınız.Komut istemine " netstat -a " yazın

 # 7 route

Microsoft Windows işletim sisteminde IP yönlendirme tablosunu görüntülemek ve işlemek için kullanılan bir komuttur. Bu komut size yönlendirme tablosunu, metriği ve arayüzü gösterecektir. Komut istemine " yönlendirme yazdırma " yazabilirsiniz

 # 8 Net View

Bu komut, belirtilen bilgisayar tarafından paylaşılan tüm kaynakların, bilgisayarların veya etki alanlarının listesini görüntüler. " Net görünüm xxxx veya bilgisayaradı " komut istemini yazabilirsiniz.

 # 9 Net User

Bu komut, bir bilgisayardaki hesapları kullanmak için değişiklikleri değiştirmek için kullanılır. Bu komut yardımıyla kullanıcı ekleyebilir, kaldırabilirsiniz.

 # 10 Net Use

Bu komut, ağ yazıcıları ve diğer eşlenen sürücüler gibi paylaşılan kaynaklara bağlantıları bağlamak, kaldırmak ve yapılandırmak için kullanılır. Bu komutun kullanımı biraz karmaşıktır. Bu nedenle, bu komutu nasıl kullanacağınızla ilgili tüm ayrıntıları almak için Microsoft sitesini ziyaret etmenizi öneririz.

 # 11 Tasklist

Bu komut, komut isteminde tüm bir görev yöneticisini açar. Kullanıcıların CMD'de görev listesine girmeleri yeterlidir ve çalışan tüm işlemlerin listesini göreceklerdir. Tüm yanlışları bu komutlarla çözebilirsiniz. Ayrıca komut, herhangi bir işlemi zorla kapatmanız gerektiğinde de kullanılabilir. Örneğin, PID 1532 sürecini yok etmek istiyorsanız, şu komutu girebilirsiniz: taskkill / PID 1532 / F

 # 12 iexplore

Hepimizin bildiği gibi, bilgisayar korsanları genellikle web tarayıcıları gibi bazı uygulamaları çalıştırmaya çalışır. Bu nedenle, bilgisayar korsanları uygulamaları ve web sayfalarını yürütmek için iexplore seçeneğini kullanır. Örneğin, komut istemine iexplore www.techviral.net girerseniz, URL'yi Internet Explorer'da açacaktır. Sadece bunlar değil, aynı zamanda herhangi bir IP adresinde çalışan siteleri bulmak için iexplore <IP adresi> ' ni de kullanabilirsiniz. Komut, bilgisayar korsanları tarafından çeşitli şekillerde kullanılır.

 # 13 pathping

Yol verme komutu, tracert'e oldukça benzer, ancak daha ayrıntılı bilgi gösterir. Komutlar, alınan rotayı analiz ettiği ve paket kaybını hesapladığı için tamamlanması birkaç dakika sürer. Windows komut isteminde aşağıdaki komutu yazmanız yeterlidir. pathping techviral.net (techviral.net'i ping yapmak istediğiniz ile değiştirin)

 # 14 Getmac

Getmac komutları çoğunlukla MAC Adresini almak için kullanılır. Hepimizin bildiği gibi, MAC adresleri üretici tarafından atanır ve donanımda saklanır. Ağa bağlı her adaptörle ayrı bir MAC adresi alırsınız. Örneğin, Ethernet'iniz, WiFi'nizin ayrı bir MAC adresi olacaktır. Bu nedenle getmac komutu, cihazın donanımında depolanan MAC adresini almak için kullanılır.

 # 15 Netsh

Netsh komutuyla, ağ bağdaştırıcınızın hemen hemen her bölümünü yapılandırabilirsiniz. Ağ kabuğu komutuyla ilgili en iyi şey, makalede listelenen tüm diğerlerine kıyasla ağ bağdaştırıcılarınız hakkında daha ayrıntılı bilgi sağlamasıdır. Netsh komutunu girerseniz, teşhis amacıyla ihtiyaç duyduğunuz tüm yönlendirme ve DHCP ile ilgili komutları listeleyecektir.

ÖLÇELİM DEĞERLENDİRELİM-3

1. Herhangi bir belirli DNS kaydı için alan adı veya IP adresi eşlemesi elde etmenize yardımcı olan bir ağ yönetimi komutu hangisidir?

A) ping B) netsh C) pathping D) nslookup

2. Penetrasyon(Sızma) Testi aşamalarını yazınız.

1)

2)

3)

4)

5)

3. Phishing(Kimlik avı) nedir, hangi yöntemler kullanılır.

CEVAP: .....

.....

.....

4. Casus yazılım türleri nelerdir?

CEVAP: .....

.....

.....

5. Siber zorbalığın en sık görüldüğü ortamları yazınız.

CEVAP: .....

.....

.....

KÖTÜ AMAÇLI YAZILIM ALGILAMA VE KALDIRMA

Web uygulama sunucularındaki mevcut enfeksiyonları ayıklarken kötü amaçlı yazılım kurulumunu önleyen bir dizi hizmete sahiptir.

Web Uygulama Güvenlik Duvarı (WAF): Ağınızın ucunda konuşlandırılan web siteleriniz ve web uygulamalarınız üzerindeki tüm kötü amaçlı yazılım yerleştirme saldırılarını engellemek için imza, davranış ve itibar analizi kullanır.

Arka Kapı Koruması: Web sunucunuzdaki arka kapı kabukları ile iletişim girişimlerini engelleyen bir hizmet. Hizmet, bu istekleri takip ederek, bulut güvenlik hizmetlerine giriş yapmadan çok önce web sunucunuza yüklenmiş olsa bile en yüksek düzeyde gizlenmiş kötü amaçlı yazılımları tespit edebilir.

Oturum Açma Koruması: Sıfır entegrasyon gerektiren ve bulut korumalı herhangi bir URL adresine anında dağıtılabilen esnek bir iki faktörlü kimlik doğrulama (2FA) çözümü kullanılabilir. Hizmet, faillerin ağ erişimi elde etmek ve web sunucularınıza rootkit ve arka kapılar yüklemek için çalınan oturum açma kimlik bilgilerini kullanmasını engeller.

Antivirüs Programları: Güncel bir antivirüs programı sayesinde bilgisayarınıza herhangi bir virüsün bulaşması engellendiği gibi daha önceden bulaşmış bir virüs temizlenecektir. Reklam yazılımı, spam mailler gibi web ortamında sizleri koruyacak olan antivirüsler aynı zamanda usb, bulut ortamı gibi saklama alanlarındaki virüsleri de temizleyecektir.

Windows Güvenlik Duvarı: Güvenlik duvarı bilgisayarımızda açık olduğu sürece virüsleri ilk karşılayan yapılardır. Bu yapı sayesinde izinsiz girişler Windows

tarafından engellenecektir. Özellikle Windows 10 ile beraber daha da güçlendirilmiş bir Windows güvenlik duvarı oluşturuldu. Kullanıcı izni olmadan herhangi bir girişe izin verilmeyen ve her türlü kötü amaçlı yazılıma karşı uyarı veren bir sistem geliştirilmiştir.

İNTERNET GÜVENLİĞİ YÖNETİM TEKNİKLERİ VE ARAÇLARI

İnternet ortamında güvenliğimizi sağlamak için aşağıdaki konularda daha dikkatli olarak önlemlerimizi almamız gereklidir.

• Kişisel bilgiler ebeveyn izni olmadan asla verilmemelidir. Bu, soyadını, ev adresini, okul adını, telefon numarasını veya kredi kartı numarasını paylaşmamak anlamına gelir.

• Şifreler gizli tutulmalıdır. Hiç kimsenin şifrenizi bilmesine gerek yoktur. Biri sizden bir parola sorarsa, çocuklara durumu önce sizin tarafınızdan yürütmelerini söyleyin. İlgili bir notta, bir kütüphane veya okul bilgisayarı kullanıyorsanız, cihazı kullanmadan önce her zaman tüm kişisel sitelerden çıkış yaptığınızdan emin olun.

• Bir sosyal medya sitesinde yayınlanan her şeyin İnternette sonsuza kadar kalacağını varsayın. Sosyal ağlar, çocukların zamanlarının çoğunu geçirdikleri bir yerdir. Pek çok çocuk bunu bilmiyor ve farkında olmadan daha sonra herkese açık olmasını istemeyecekleri paylaşımlar yapabilirler. Çocuklarınızla paylaşmanın neyin paylaşılmaması gerektiğini konuşun. Bu, kimliklerini, itibarlarını ve geleceklerini korumak için son derece önemlidir.

• İnternetteki yabancılarla asla yüz yüze görüşmeyin. Birisi internette zararsız görünebilir, ancak gerçek hayatta tamamen farklı bir kişi olabilir. Çocuklara, uygun internet görgü kuralları ve herhangi bir kökene sahip yabancılarla gerçek yaşam etkileşiminin tehlikeleri hakkında rehberlik edilmelidir.

• Siber zorbalık, çocuklar için en büyük risklerden biridir. Çocuklarınıza siber zorbalığa karşı koymaları için güven verin. Onlara asla kaba veya aşağılayıcı mesajlar göndermemelerini veya bunlara yanıt vermemelerini öğretin. Siber zorbalığın kurbanı olurlarsa veya başkalarının incitici mesajlar gönderip almaktan bahsettiklerini duyarlarsa, bu davranışı bir yetişkine bildirmelidirler. Çevrimiçi ortamda kendilerini rahatsız veya korkutan bir şey olursa, durum hakkında hemen bir yetişkinle konuşmaları gerekir.

Günümüzde işletmeler dijital olarak her zamankinden daha gelişmiş durumda ve teknoloji geliştikçe kuruluşların güvenlik duruşları da geliştirilmelidir. Kablolu, kablosuz veya hücresel ağlar üzerinden birbiriyle iletişim kuran birçok cihazla sağlanacak ağ güvenliği önemli bir kavramdır.

Hacklemek	Etik hackleme
Bir sisteme veya ağa Yetkisiz İzinsiz Giriş.	Sistemin güvenlik açıklarını bulmak için yetkili yöntem.
Yasadışı.	Yasaldır.
Siyah şapka korsanları bilgisayar korsanlığı yapar.	Beyaz şapka korsanları etik hackleme gerçekleştirir.
Organizasyondan veri, para çalmak isteyen bir grup insan tarafından yapılır.	Gerçek zamanlı hacklemeyi önlemek için kuruluşun çalışanı tarafından gerçekleştirilir.

Tablo 1: Hacklemek ve Etik Hacklemek Karşılaştırma

ETİK HACKLEME

Etik bir bilgisayar korsanı (beyaz şapkalı korsan olarak da bilinir) en üst düzey güvenlik uzmanıdır. Etik bilgisayar korsanları, çeşitli sistemlerdeki güvenlik açıklarını ve zayıflıkları nasıl bulacaklarını ve bunlardan nasıl yararlanacaklarını bilirler - tıpkı kötü niyetli bir bilgisayar korsanı (veya siyah şapkalı bir bilgisayar

EĞLENELİM ÖĞRENELİM

Aşağıda yer alan anakartın içerisinde kötü amaçlı bir kişi bulunmaktadır. Bu kişi sizin bilgilerinize sızmaya çalışan birisidir. O kişiyi işaretleyerek bilgilerin çalınmasını engelleyiniz.

korsanı) gibi. Aslında ikisi de aynı becerileri kullanıyor; ancak etik bir bilgisayar korsanı, bu becerileri meşru ve yasal bir şekilde kullanarak zayıf noktaları bulmaya ve kötü adamlar oraya girip içeri girmeye çalışmadan önce bunları düzeltmeye çalışır.

Etik bir hacker'ın rolü, penetrasyon test cihazına benzer, ancak daha geniş görevleri içerir. Yasal ve etik olarak sistemlere girerler. Bu yasallık, etik bilgisayar korsanları ile gerçek bilgisayar korsanları arasındaki temel farktır.

Nasıl Etik Hacker Olunur?

BT güvenliği işleri , bilgisayar ve teknoloji uzmanlığı gerektirir. BT niteliklerine sahipseniz, mesleği öğrenmeyi ve iş bulmayı daha kolay bulacaksınız. Zaten BT sektöründe çalışıyorsanız, bu iş için anahtar olan ağ temelleri, işletim sistemleri, komut dosyası dili hakkında deneyim ve bilgiye sahip olacaksınız.

Etik bir bilgisayar korsanının işi, aynı zamanda çeşitli araçları nasıl kullanacağını anlamayı ve bilmeyi gerektirir. Aşağıdakiler çok önemlidir:

• NMap, güvenlik denetimleri yapmak için.

• Wireshark, veri sızıntısını tespit etmek için ağları izlemek için.

• BadMod, web uygulaması güvenliğini ölçmek için.

Bu alanlarda daha yetkin olabilmek için Red Team Certified Professional, Licensed Penetration Tester (LPT), Certified Ethical Hacker (CEH), Cisco ağ sertifikaları ve altyapıları, Microsoft tarafından MCP profesyonel sertifikaları, vb. Gibi özel kurslara kaydolabilirsiniz. Etik bir bilgisayar korsanı olmak kolay değil, kısa vadeli bir hedef de değil. Ayrıca, BT, teknoloji ve güvenlik dünyası hızla değişiyor, bu nedenle her zaman yeni beceriler edinmeye devam etmeniz gerekiyor.

SİBER GÜVENLİK MÜHENDİSİ NE YAPAR?

Ülkemizde henüz Bilgisayar Mühendisliği veya Yazılım Mühendisliğinin bir alanı olarak kabul edilen ve özel bir bölümü bulunmayan Siber Güvenlik Mühendisliği geleceğin meslekleri içerisinde yer almaktadır. Siber Güvenlik Mühendisi, bilgisayar korsanlarına, siber saldırılara ve diğer kalıcı tehditlere karşı savunmak için tasarlanmış güvenli ağ çözümleri tasarlar ve uygular. Ayrıca, bu sistemlerin test edilmesine ve izlenmesine katılırlar, sürekli olarak tüm sistem savunmalarının güncel olduğundan ve doğru şekilde çalıştığından emin olurlar.

Genellikle, bir Siber Güvenlik mühendisinin pozisyonuna veri güvenliği mühendisi, BT güvenlik mühendisi veya Web güvenlik mühendisi gibi başka bir şey denir. Ayrıca, bazen, bir Siber Güvenlik mühendisinin rolü, özellikle bir Siber Güvenlik uzmanını karşılayamayan daha küçük şirketlerde farklı bir BT pozisyonuna getirilir.

Resim 24: Siber Güvenlik Mühendisi

Siber Güvenlik mühendisinin rolleri ve sorumlulukları şunları içerir:

• Kuruluşun güvenlik ihtiyaçlarını değerlendirin ve buna göre en iyi uygulamaları ve standartları belirleyin.

• Kuruluşların verilerini, sistemlerini ve ağlarını korumak için gereken tüm güvenlik önlemlerini tasarla-

mak, uygulamak, sürdürmek, denetlemek ve yükseltmek.

• Ağa ve ilgili sistemlere yönelik tüm güvenlik ihlallerine yanıt vermek.

• Tüm ağ ve güvenlik sorunlarını ve olaylarını giderin.

• Düzenli olarak penetrasyon(girişim) testi yapın.

• Kuruluşun altyapısının ve mevcut verilerin güvenliğini sağlamak için uygun güvenlik önlemlerinin alınması.

• Ağ ve sistemdeki güvenlik açıklarını tespit etmek için test ve tarama yapmak.

• Değişim yönetimi sürecinde aktif rol almak.

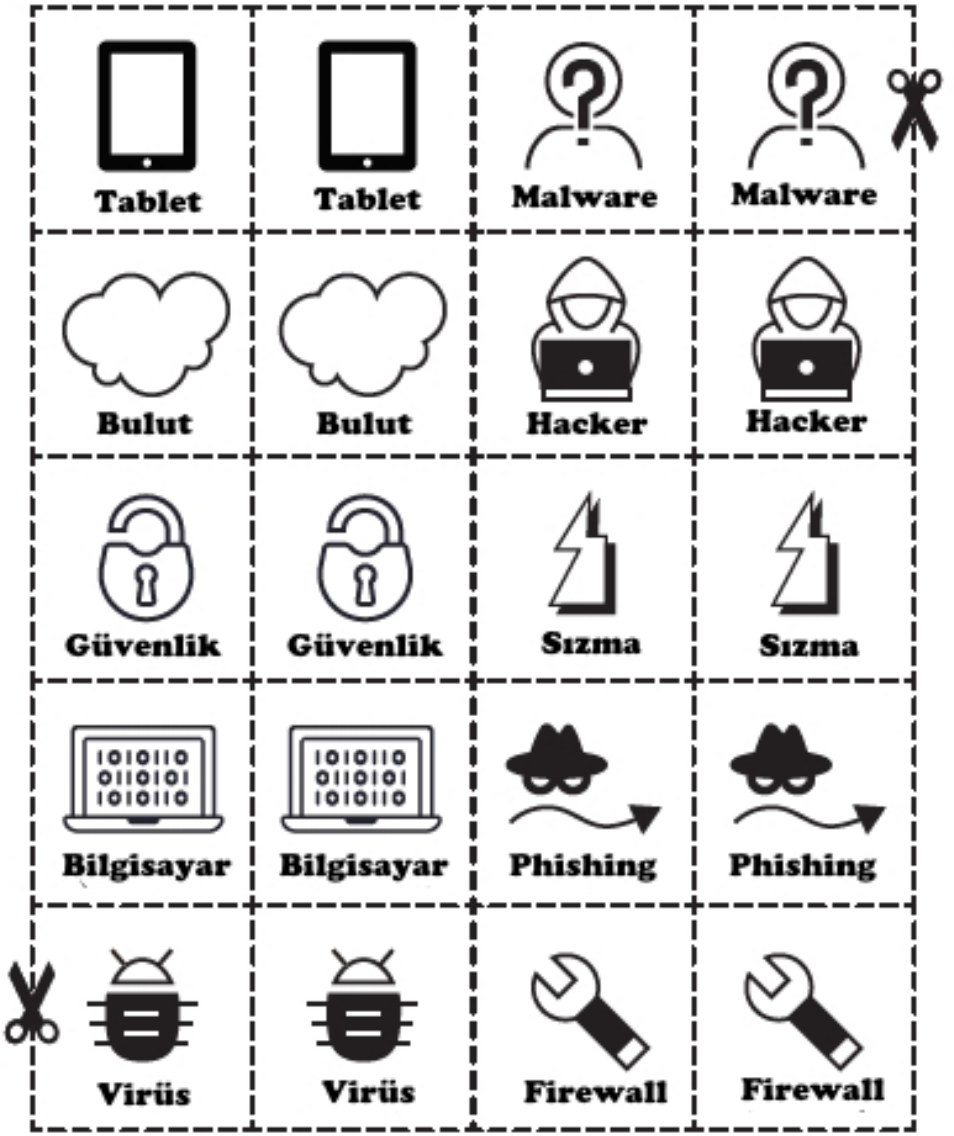
• Herhangi bir güvenlik ihlali soruşturmasına yardımcı olun.

• Kuruluşun uygun departmanları ile raporlama ve açık iletişim hatlarını koruma gibi rutin günlük idari görevleri yerine getirmek.

Bir Siber Güvenlik mühendisi işinin ve sorumluluklarının bir güvenlik analistinin görevlerine çok yakın olduğunu unutmayın. Bir Siber Güvenlik mühendisi sistemleri tasarlar ve inşa ederken, bir güvenlik analisti sistemi kırmaya çalışırken daha çok onun hızına oturtmakla ilgilenir. Bununla birlikte birçok Siber Güvenlik mühendisi rutin olarak stres testleri yapıyor ve zayıf noktaları tahmin etmeye ve test etmeye çalışıyor. Bir Güvenlik Mühendisi / Analisti için iş listelerini görmek, her iki pozisyonu da etkili bir şekilde bir araya getirmek sıra dışı değildir.

EĞLENELİM ÖĞRENELİM

Aşağıdaki “eşleştirme oyununu” belirtilen yerlerden keserek arkadaşınızla beraber siber güvenlik kavramlarını ters kapatınız ve eşleştirmeye çalışınız.



ETKİNLİK 2

Etkinlik Adı

Siber Saldırı Engelliyorum

Etkinlik Süresi

2 Ders Saati

Etkinlik Modülü

Siber Güvenlik Eğitimi

Etkinlik Kazanımları

• Öğrenciler kodlama, parola koruması, sosyal mühendislik ve ağ güvenliği ile ilgili bilgisayar bilimi terminolojisini açıklayabilecektir.

• Öğrenciler, gizliliği korumak için şifrelemenin nasıl çalıştığını açıklayabilecekler

• Öğrenciler, son ağ güvenliği ihlallerini ve şirketlerin bunlara karşı nasıl savunduğunu tanımlayabilecekler.

• Öğrenciler, "hacker" teriminin neden son derece esnek olduğunu ve bilgisayar korsanlarının oynadığı rollerin çeşitliliğini açıklayabilecekler

• Öğrenciler, ortaya çıkan güvenlik ihlalleri raporlarını analiz edebilecek ve güvenlik ağları konusundaki anlayışlarını bunlara uygulayabilecektir.

Ön Bilgi

Cybersecurity Lab, insanlara dijital yaşamlarını nasıl güvende tutacaklarını, siber dolandırıcılıkları nasıl tespit edeceklerini, kodlamanın temellerini nasıl öğreneceklerini ve siber saldırılara karşı nasıl savunma yapacaklarını öğretmek için tasarlanmış bir oyundur. Oyuncular, giderek daha karmaşık hale gelen siber saldırıların hedefi olan yeni kurulan bir sosyal ağ şirketinin baş teknoloji sorumlusu rolünü üstleniyor. Oyunda, oyuncular siber savunmalarını güçlendirmek ve saldırganlarını engellemek için zorlukları tamamlamalıdır. Laboratuvar ayrıca gerçek dünya siber saldırı hikâyeleri, bir siber terimler sözlüğü ve siber güvenlik ihtiyacını, gizliliğe karşı güvenlik, kriptografi (siber kodlar) ve bilgisayar korsanlarının tam olarak ne olduğunu açıklayan kısa animasyonlu videolar içerir.

Laboratuarın dört ana oyun bileşeni vardır:

• Kodlama Zorluğu: Çok temel kodlama becerilerine giriş. Oyuncular, sürükle ve bırak komutlarını kullanarak bir labirentte gezinmesi için bir robot programlar.

• Şifre Kırma Mücadelesi: Bir dizi "şifre düelloları", oyunculara saldırganların şifrelerini nasıl kırmaya çalışabilecekleri ve nasıl daha iyi, daha güvenli şifreler oluşturabileceklerinin temellerini öğretir.

• Sosyal Mühendislik Mücadelesi: Oyunculara görünüşte benzer iki e-posta veya web sitesi sunulur. Önce aralarındaki farkları belirlemeli ve ardından hangisinin bilgilerini veya parasını çalmaya çalışan bir aldatmaca olduğuna karar vermelidirler. Bu zorluk aynı zamanda bir dizi ses kaydını ve telefon görüşmelerinin dökümünü içerir; oyuncuların arayan kişiye güvenip güvenmemesi gerektiğine karar vermesi gerekir.

• Ağ Saldırıları: Şirketleri büyüdükçe, oyuncular kendilerini bir dizi siber saldırıya karşı savunmak için savunma satın almalıdır. Oyuncular üç mücadelede ne kadar başarılı olursa, savunma satın almak için o kadar çok kaynak gerekir.

Yöntem

Siber Güvenlik Laboratuvarı, öğrencilerine çevrimiçi ortamda güvende kalmak için en iyi uygulamaları öğretmek ve onlara bilgisayar bilimi ilkelerini ve çevrimiçi ağların mimarisini tanıtmak isteyen eğitimciler için harika bir kaynaktır. Ek olarak, okul teknolojisi ve medya uzmanları, Siber Güvenlik Laboratuvarı'nı, çevrimiçi kaynakları kullanmaya başlamadan önce öğrenciler için bir oryantasyon etkinliği olarak kullanabilir. İngilizce ve sosyal bilgiler eğitimcileri, öğrencilerin metinsel kanıtlar bulmaları, çıkarımlar yapmaları ve Sosyal Mühendislik Zorluğundaki kaynakların geçerliliği hakkında yargılarda bulunmaları gerektiğinden, metinsel analiz becerilerini güçlendirmek için Siber Güvenlik Laboratuvarı'nı da kullanabilir. Öğrenciler online yazılım sayesinde ;

• Öğrenciler, Kodlama Yarışmasında Blockly kodunu kullanarak bir labirentte bir robotta gezinebilecekler.

• Öğrenciler, Sosyal Mühendislik Mücadelesinde kimlik avı girişimlerini, dolandırıcı web sitelerini ve telefon dolandırıcılarını ayırt etmek için analitik okuma becerilerini kullanacaklar.

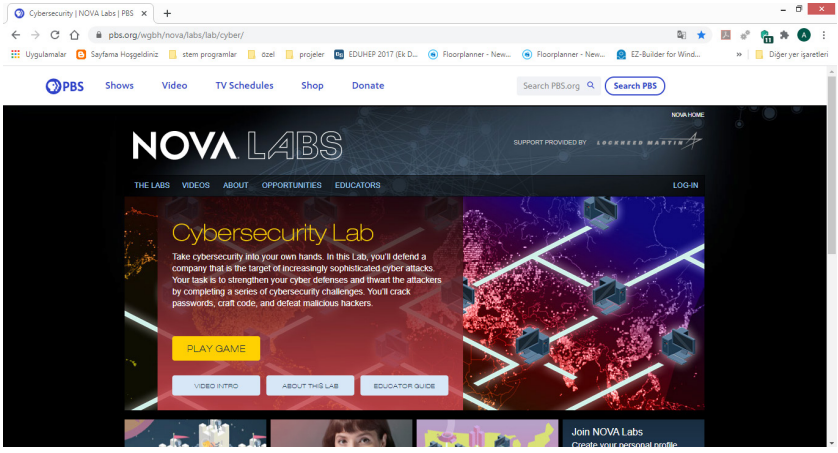
- Öğrenciler, Şifre Kırma Sınamasında güçlü şifreler oluşturmak için mantıksal akıl yürütme kullanacaklardır.

Siber güvenlik alanında çok çeşitli işler ve bunları yapmak için gereken özel becerilere sahip ciddi bir insan sıkıntısı var. Hayatlarımız İnternet ile daha da iç içe geçtikçe, bu alandaki fırsatlar daha da genişleyecektir. NOVA'nın Siber Güvenlik Laboratuvarı, yeni nesil siber savunuculara ilham vermek için bir başlangıç noktasıdır.

Programın Yüklemesi ve Arayüz

Etkinliğimizi gerçekleştirmek için NOVA tarafından geliştirilen Siber Güvenlik Laboratuarını kullanacağız. Web adresi https://www.pbs.org/wgbh/nova/labs/lab/cyber/ olan yapımızı web tarayıcımızın url kısmına yazıyoruz veya karekodumuzu okutarak web sayfamıza yönlendiriliyoruz.

Web sayfamızı açtığımızda karşımıza aşağıdaki ekran gelecektir.



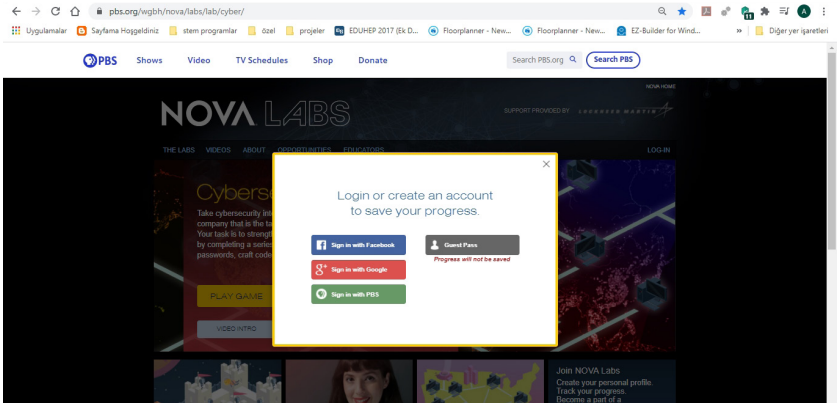
Resim 25: Siber Güvenlik Laboratuvarı Ana Sayfa

Ana sayfamızda yer alan uygulamaya giriş yapmak için "Play Game" kısmına tıklıyoruz ve uygulamamıza başlıyoruz.

Etkinlik Yapımı

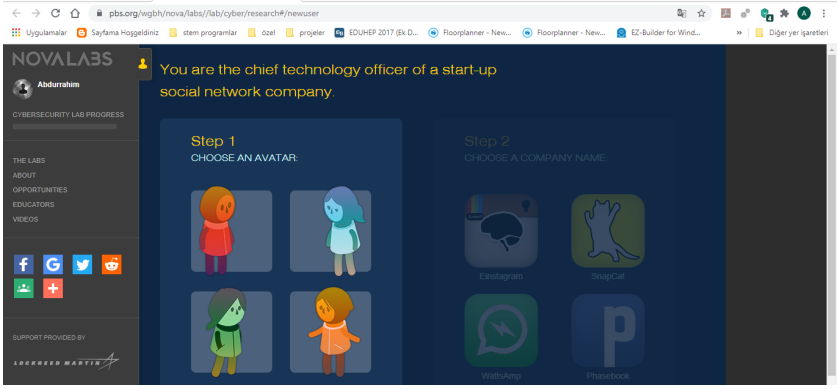
Etkinliğimizi gerçekleştirirken oyun mantığıyla bir siber güvenlik ya-

pısı kuracağız. Saldırılara karşı kalkanlar kuracağız ve bu kalkanları kurarken puanımızın olması gerekmektedir. Bu puanları kodlama yaparak ve siber güvenlik yapılarını kullanarak kazanacağız. “Play Game” seçeneğini seçtikten sonra bizden yaptığımız uygulamanın kaydedilmesi için giriş yapmamız istenecektir. Sosyal ağlarla veya misafir kullanıcı olarak giriş yapabilirsiniz. Misafir olarak giriş yaptığınızda uygulamalarını kaydedilmeyecektir.



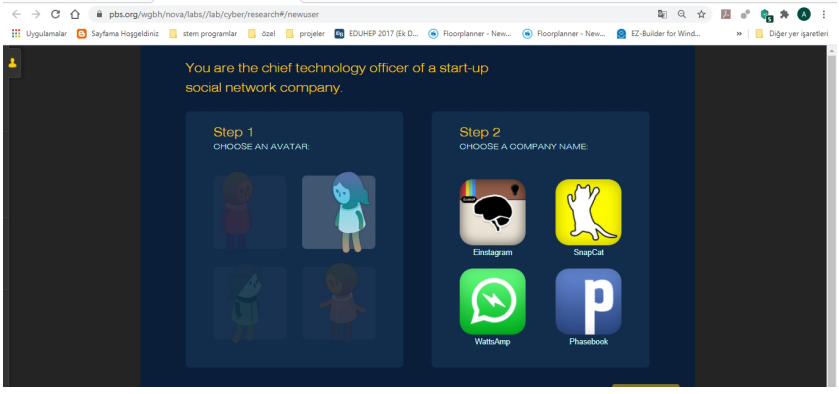
Resim 26: Siber Güvenlik Laboratuvarı Kullanıcı Girişi

Misafir olarak giriş yaptıktan sonra adım adım siber güvenliğini sağlayacağımız şirket yapımızı oluşturacağız. İlk adımda avatar oluşturarak sosyal ağ şirketinizin baş teknoloji sorumlusunu seçiyorsunuz.



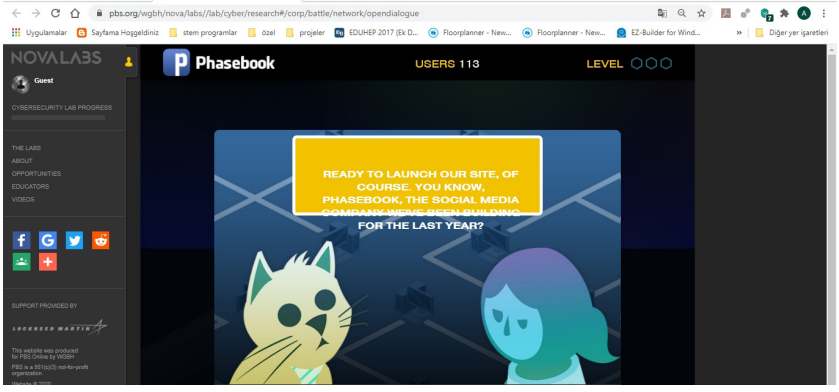
Resim 27: Siber Güvenlik Laboratuvarı Avatar Seçimi

İkinci adımda sosyal ağ şirketimizin adını belirliyoruz. Bu kısımda 4 adet kopya firma isimleri bulunmaktadır. Firma isimleri günlük hayatta en çok kullanılan sosyal ağların benzeri şeklinde oluşturulmuştur. Burada seçim yaptıktan sonra next butonuna basınız.



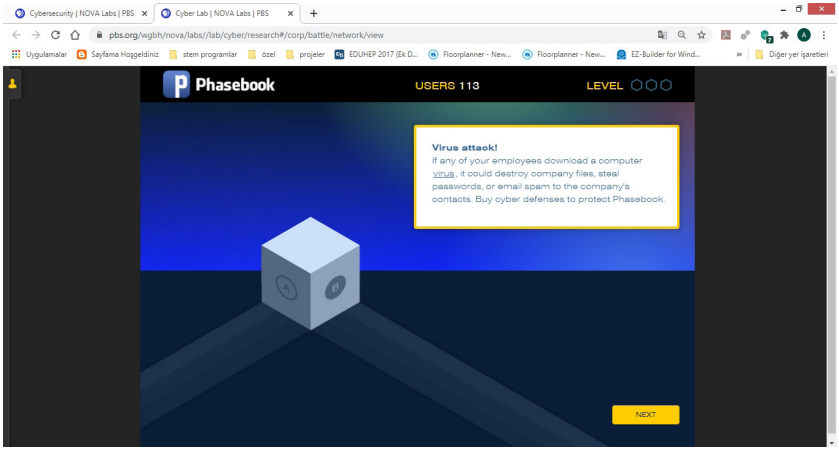
Resim 28: Siber Güvenlik Laboratuvarı Sosyal Ağ Firma Seçimi

Artık sosyal ağ şirketimizin verilerini ve kaynaklarını siber saldırılara karşı korumaya hazırız. Bir diğer aşamada güvenliği sağlamaya yönelik bizlere ön bilgi verilmektedir.



Resim 29: Siber Güvenlik Laboratuvarı Sosyal Ağ Firma Seçimi

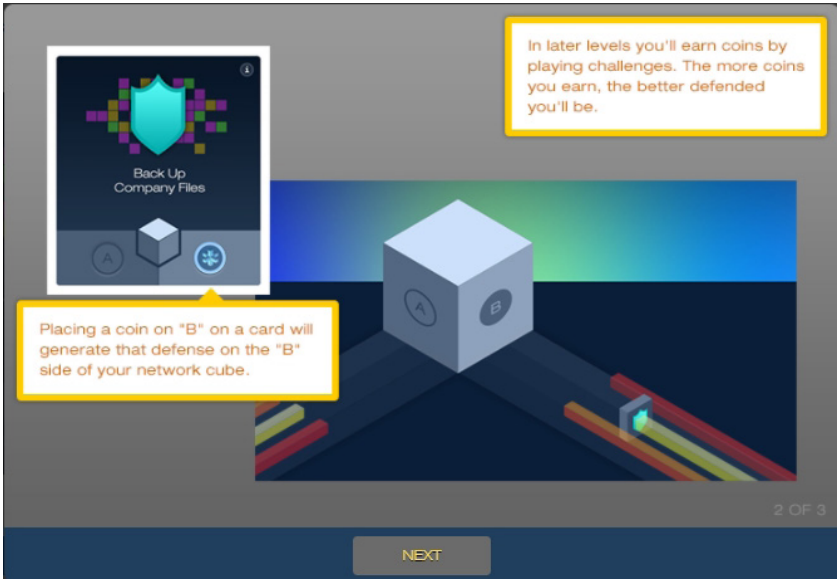
Ön bilgilendirme kısmında sosyal ağ şirketi çalışanlarının virüs indirebileceği veya sızma olabileceği konusunda bilgi verilerek bir siber savunma yapısı oluşturulması istenmektedir.



Resim 30: Siber Güvenlik Laboratuvarı Saldırı Sayfası

"Phasebook" isimli klon şirketimizin 113 adet kullanıcı bulunmaktadır. Başlangıç seviyesinde siber savunma kurmamız gerekmektedir. Çalışanlarınızdan herhangi biri bir bilgisayar virüsü indirirse, bu şirket dosyalarını yok edebilir, parolaları çalabilir veya şirketin kişilerine e-posta gönderebilir. Phasebook'u korumak için siber savunma satın almamız istenmektedir. Şirketimizin kullanımda olan ve kullanıcıların kolayca erişebildiği dosyalarının hepsi "A" olarak belirtilmiştir. Arkaplanda çalışan uygulama ve veritabanları da "B" yüzü olarak adlandırılmıştır. Önemli dosyalar ve yedeklemeler genellikle "B" alanında bulunmaktadır. Bu bilgiler doğrultusunda 3 adet koruma yapısı ilk olarak bizlere sunulmaktadır. "Upgrade Antivirüs Software(Yükseltilmiş Antivirüs Yazılımı)" , "Back Up Company Files(Yedeklenen Şirket Dosyaları)" ve "Phishing e-mail Detecting Training(E-mail Dolandırıcılık Tespit Sistemi)" kısımlarını sunmaktadır. A ve B koruma alanlarında bu 3 alana ait koruma sağlayacağız.

Resim 31: Siber Güvenlik Laboratuvarı Şirket Koruma Alanları Tanıtımı

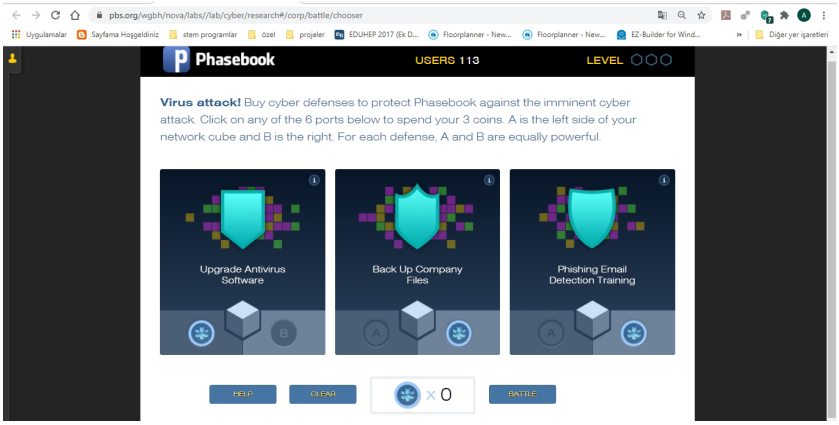


Resim 32: Siber Güvenlik Laboratuvarı Şirket Koruma "A" ve "B" Alanları

Şirketimizin koruma sistemine 3 adet saldırı gerçekleşebilmektedir. Bunlar güçlü atak(kırmızı renkte) , orta düzeyde atak (turuncu) ve basit atak (sarı renkte) temsil edilmektedir. Burada savunma sistemini kurarken mutlaka coin denilen jetonumuzun olması gerekir. Coin kazanabilmek için kodlama yapmamız gerekecek, şifre kırmamız veya sosyal mühendislik deneyi yapmamız gerekecektir.

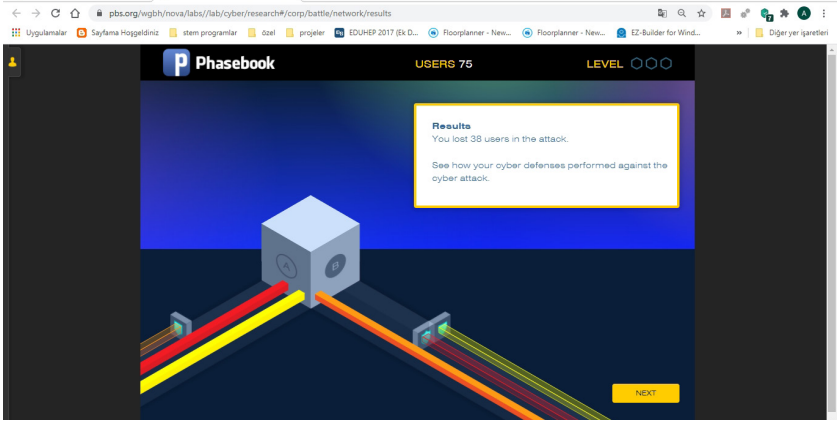
Resim 33: Siber Güvenlik Laboratuvarı Şirkete Saldırı Türleri

Şimdi savunmamızı oluşturma zamanı gelmiştir. Savunmamızı oluşturabileceğimiz 3 adet jetonumuz bulunmaktadır. Bunu istediğimiz bir yüze yani A yüzü veya B yüzüne yerleştirerek siber saldırıya hazırlanalım. Örnek olarak aşağıdaki savunma sistemini oluşturduk.



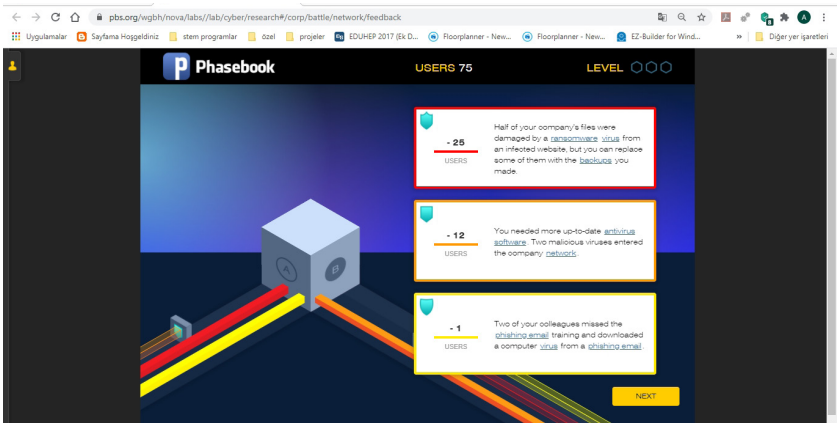
Resim 34: Siber Güvenlik Laboratuvarı Siber Saldırı Koruma Yapısı Oluşturma

"Battle" kısmına tıklıyoruz ve savunma sistemimizi siber saldırı karşısında deniyoruz.



Resim 35: Siber Saldırı Sonrası Savunma Sistemi

Örnekte de görüldüğü gibi 38 kullanıcı siber saldırı mağduru oldu. Savunma sistemimizin daha dikkatli oluşturulması gerekmektedir. "Next" butonuna bastığımızda saldırılara yönelik detaylı bilgi almaktayız.



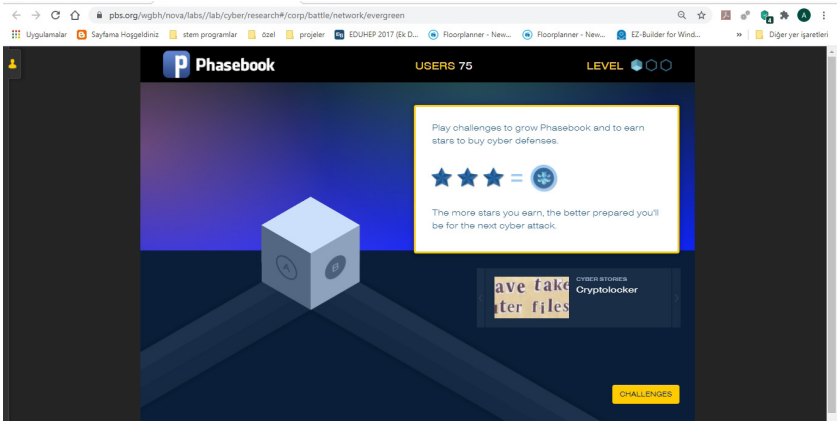
Resim 36: Siber Saldırı Sonrası Savunma Sistemi

• 25 Kullanıcı : Şirketinizin dosyalarının yarısı, virüslü bir web sitesinden fidye yazılımı virüsünden zarar gördü , ancak bazılarını yaptığınız yedeklemelerle değiştirebilirsiniz .

• 12 Kullanıcı : Daha güncel bir virüsten koruma yazılımına ihtiyacınız vardı . Şirket ağına iki kötü amaçlı virüs girdi.

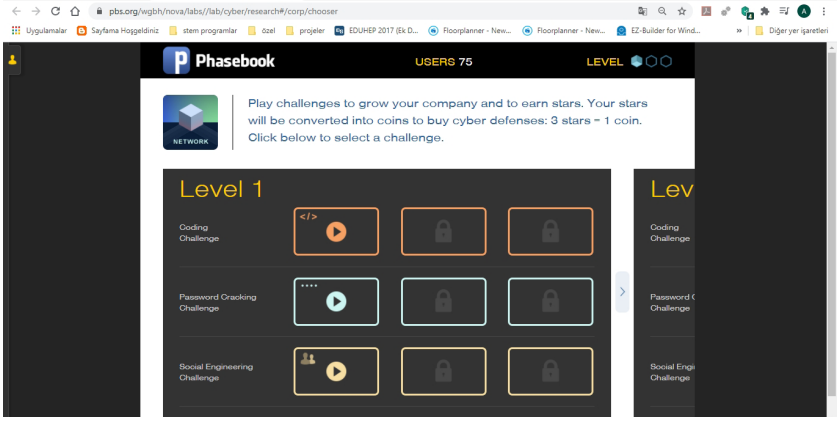
• 1 Kullanıcı : Meslektaşlarınız ikisi cevapsız phishing e-posta eğitim ve bilgisayar indirilen virüs bir gelen Phishing e-postasını .

Bir sonraki adımda nasıl yaklaşması gerektiği hakkında bilgiler verilmektedir. Fakat burada önemli olan noktaların başında gelen coin yapısı ilk savunma sisteminde tamamen kullanılmıştır. Yeni coin yani jeton kazanmak için 3 yöntem bulunmaktadır. Bunun için “challenges” seçeneğine tıklıyoruz. Burada kriptografya hakkında bilgi kutucuğu mevcut onu isterseniz okuyabilirsiniz.



Resim 37: Siber Saldırı Sonrası Savunma Sistemi Jeton Kazanma

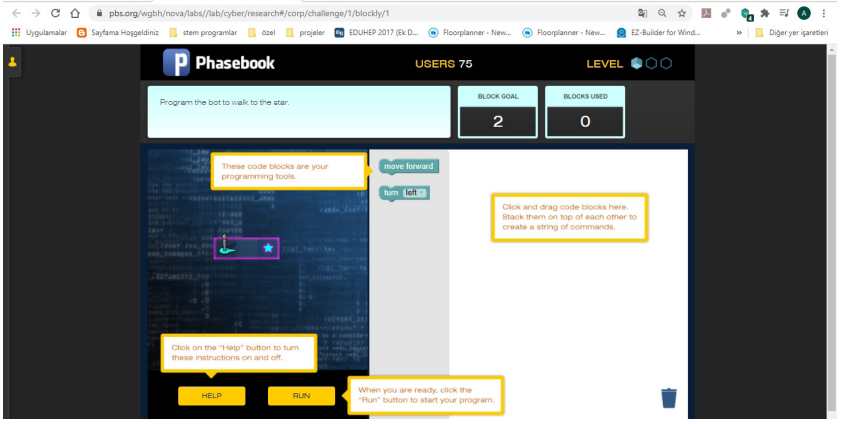
Bu bölümden jeton kazanmak için etkinlikler geliştireceğiz. Toplamda 3 level yani bölümü bulunan siber güvenlik laboratuvarımız için etkinlikler oluşturarak jeton kazanacağız. Bu jetonları siber savunma sistemimiz için kullanacağız.



Resim 38: Siber Saldırı Sonrası Savunma Sistemi Jeton Kazanma-2

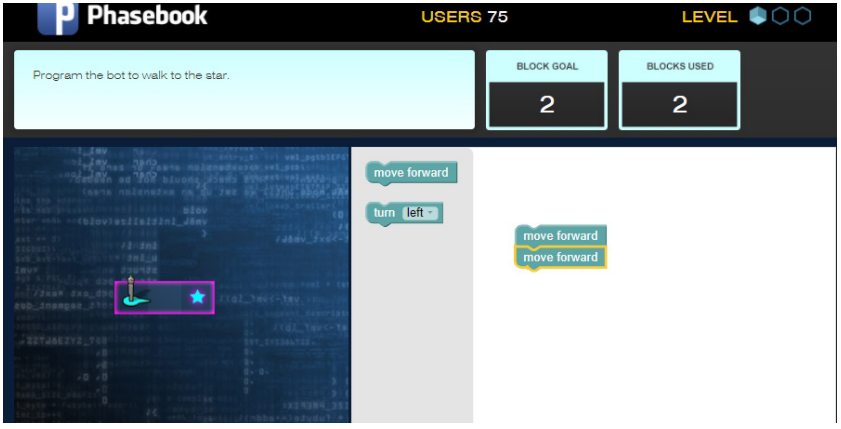
Buradaki ilk seçenekte basit düzeyde blok tabanlı kodlama ile hedefe ulaşmaya çalışacağız. İkinci seçenekte şifre kırma teknikleri ile bir şifreyi çözmeye çalışacağız. Üçüncü seçenekte de sosyal mühendislik yöntemini kullanarak virüslerin nasıl bulaştığını öğrenelim. Şimdi Level

1 düzeyinde her bir seçenek için birer adet örnek oluşturalım. Seçeneklerin üzerindeki “play” tuşuna basarak giriş yapıyoruz ve başlangıç bilgi verme yapısı karşımıza çıkmaktadır. Bilgi aldıktan sonra uygulamaya geçiyoruz.



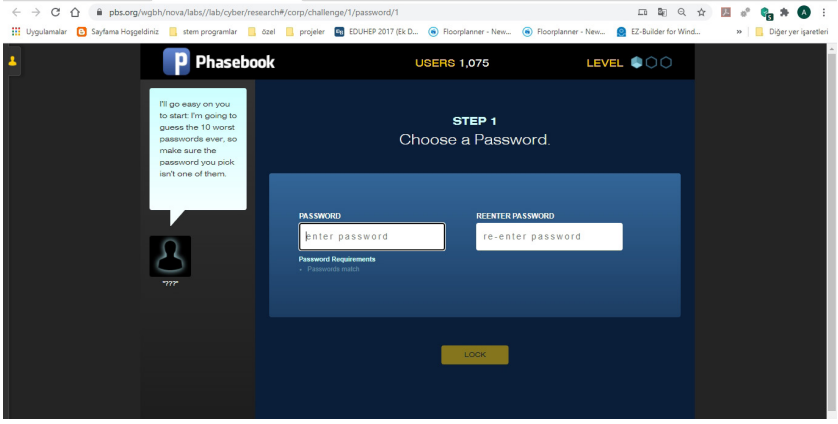
Resim 39: Siber Saldırı Sonrası Savunma Sistemi Blok Kodlama

Sol tarafta belirtilen kişiyi yıldız olan hedefe ulaştıracak kod yapısını sağ tarafta boş alana ortada bulunan kod bloklarını kullanarak oluşturunuz. “Run” seçeneği ile kodlarımızı çalıştırıyoruz. Kullanılacak blok sayısı yukarıda “Block Goal” kısmında belirtilmiştir.



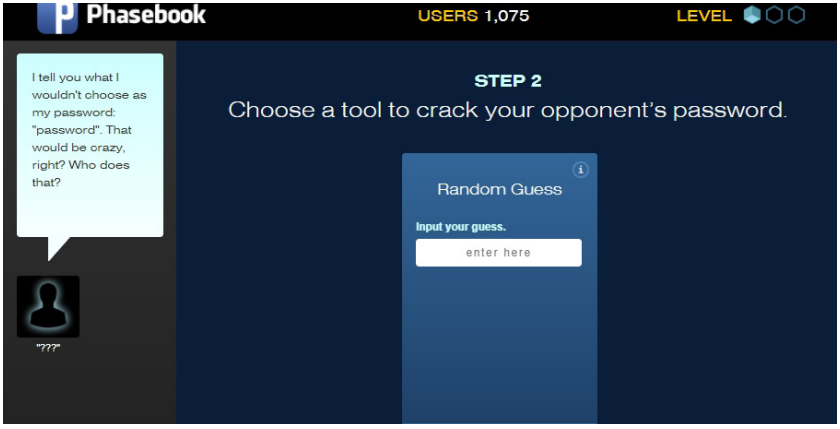
Resim 40: Blok Kodlama Kod Blokları Oluşturma

Şifre kırma etkinliğinde ise şirketinizde çalışan bir kişinin sizin şifrelerinizi bir başkasıyla paylaştığı öngörülmektedir. Bu kişinin kim olduğunu öğrenmek için biz dizi şifre kırma yarışına katılacaksınız. Karşıdaki kişi ve siz şifrelerinizi oluşturacaksınız sonra da bu şifreleri çözmeye çalışacaksınız.



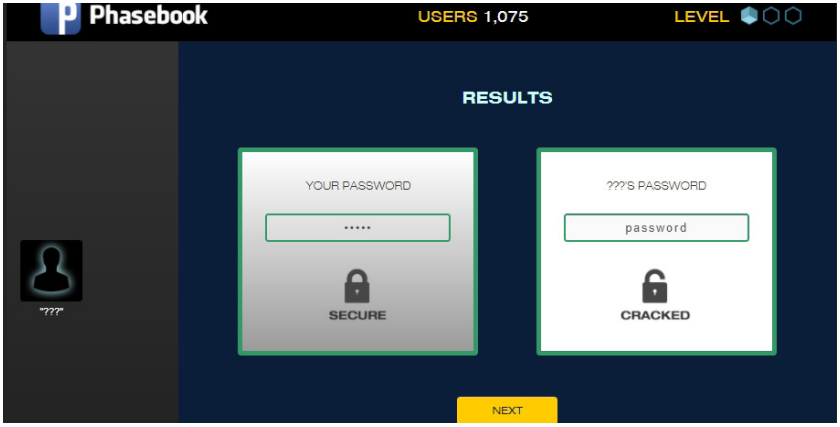
Resim 41: Şifre Kırma Yarışması için Şifre Oluşturma

Örnek olarak "S1ber" diye bir şifre girelim ve yan taraftaki kutucuğa da aynı yapıyı yazalım.



Resim 42: Şifre Kırma Yarışması için Şifre Tahmini

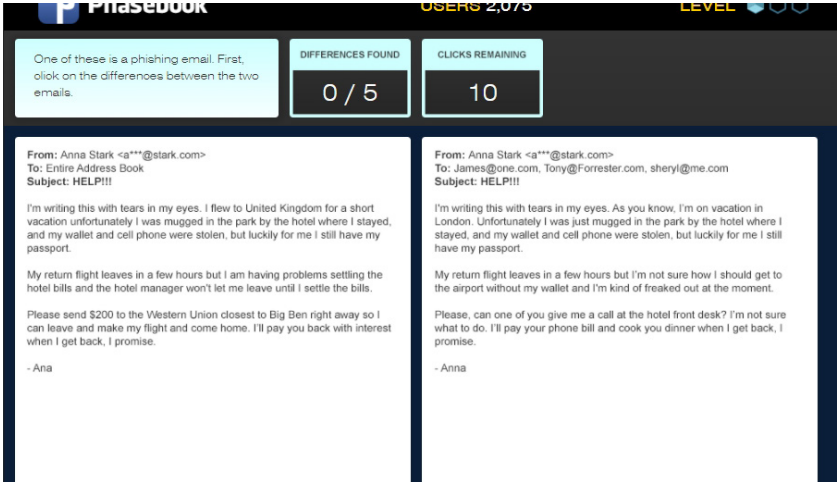
Karşı taraftaki kişinin şifresini tahmin etmek için basit bir şifre yapısı giriniz. Örnek olarak karşıdaki kişi “password” kelimesini şifre olarak kullanmayacağım demiştir. Bunu deneyelim.



Resim 43: Şifre Kırma Yarışması için Şifre Tahmini

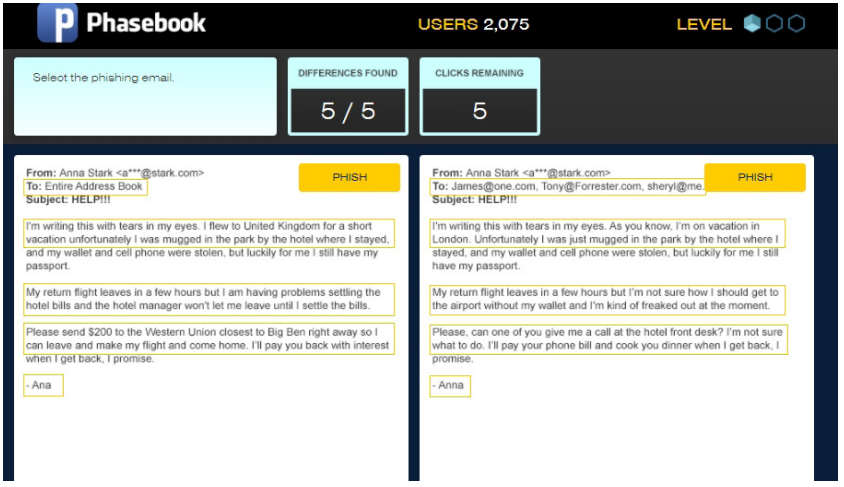
Biz kazandık basit bir şifre olan “password” yapısını kullanmıştır. Biz ise içerisinde büyük harf, rakam ve küçük harften oluşan bir şifre tanımlamıştık. Güçlü bir şifre için bunların yanı sıra çeşitli sembollerinde kullanılması gerekmektedir.

Sosyal mühendislik yarışmasında da e-maillere gelen yabancı maillerin içeriği değerlendirilecektir. Bunun için başlangıç bilgilendirilmeleri verilmektedir. Güvenilen kaynak gibi görülen e-mailler kişilerin bilgilerine ulaşmak için en sık kullanılan yapıların başında gelmektedir. Bu etkinlikte bizlere gerçek maillerle sahte mailleri ayırt edebilmemiz istenmektedir. Bunları ayırt edebilmek için çeşitli metotlar bulunmaktadır. Bunlar ; mail adresi tam ve doğru olmalıdır , konu başlığının ilgi çekici olması , bir başkası e-mail yoluyla sizden doğrudan özel bilgiler talep etmez (adı soyadı , T.C. kimlik no, anne adı , baba adı , banka iban no vb.) , takma isimler genellikle gerçek isimlerin benzeri şeklinde oluşturulmuştur. Şimdi bu özellikleri dikkate alarak sahte e-mailleri yakalayalım.



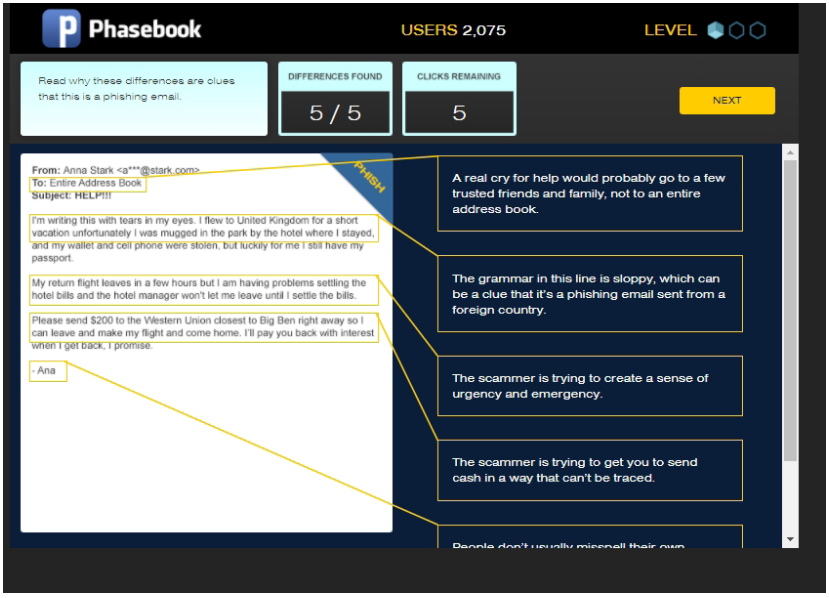
Resim 44: Sosyal Mühendislik Yapısı için E-Mail Analizi

E-mailler arasında farklı olan yapıları işaretleyelim ve böylelikle kişileri kandırmak amaçlı kullanılan yapıları ortaya çıkaralım.



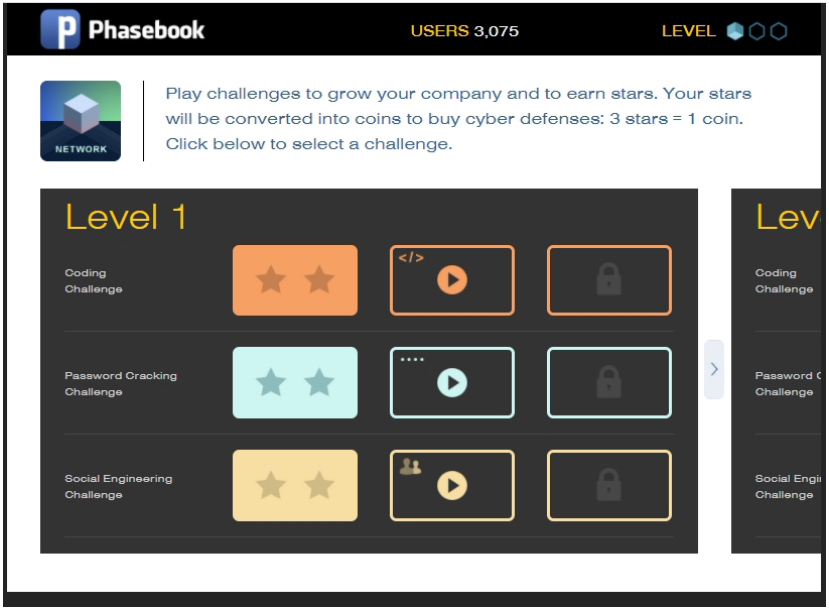
Resim 45: Sosyal Mühendislik Yapısı için E-Mail Farklı Yer İşaretleme

Şimdi hangi e-mailin sahte olduğunu seçelim. Sol taraftaki e-mailde iletilen kısmı boş , içerik olarak bilgi ve para isteyen bir yapı oluşturulmuş ve en son isim yanlış yazılmıştır. Bundan dolayı sahte e-mail sol taraftaki e-maildir.



Resim 46: Sosyal Mühendislik Yapısı için E-Mail İçerik Analizi

"Next" tuşuna basarak bu yarışmayı da tamamlıyoruz. Artık elimizde 6 yıldız yani 2 jeton oldu. Hala siber savunma için jeton kazanmamız ve güçlendirmemiz gerekmektedir. Toplamda 3 level olan ve her birisinin içerisinde örneklerini yapmış olduğumuz 3 alanda çeşitli uygulamalar zorluk seviyesine göre bulunmaktadır. Siber savunma sisteminizi "A" ve "B" alanlarından güçlendirmeniz için jeton kazanmanız yani siber saldırılarda en çok kullanılan bu yöntemleri öğrenmemiz için daha fazla uygulama yapmamız gerekmektedir.



Resim 47: Siber Savunma Sistemi İçin Jeton Kazanma Level Uygulamaları

Siz Uygulayın!

Siber savunma kalkanınızı güçlü tutmak için birçok alanda uygulamalar yaparak saldırı yapılan bütün alanlarınızı açıklardan koruyun.

KRİPTOGRAFİ NEDİR?

Resim 48: Kriptografi nedir?

Kriptografi, düşman olarak bilinen kötü niyetli üçüncü şahısların varlığında güvenli iletişim sağlar. Şifreleme, bir girişi (yani düz metin) şifreli bir çıktıya (yani şifreli metin) dönüştürmek için bir algoritma ve anahtar kullanır. Belirli bir algoritma, aynı anahtar kullanılırsa her zaman aynı düz metni aynı şifreli metne dönüştürür.

Algoritmalar, bir saldırgan şifreli metin göz önüne alındığında düz metin veya anahtarın herhangi bir özelliğini belirleyemezse güvenli kabul edilir. Saldırgan, anahtarı kullanan çok sayıda şifresiz metin / şifreli metin kombinasyonu verildiğinde bir anahtar hakkında hiçbir şey belirleyememelidir.

Simetrik kriptografide, aynı anahtar hem şifreleme hem de şifre çözme için kullanılır. Bir gönderen ve bir alıcının zaten her ikisi tarafından da bilinen paylaşılan bir anahtarı olmalıdır. Anahtar dağıtımı zor bir sorundur ve asimetrik kriptografi geliştirmek için itici güçtür.

Asimetrik kripto ile şifreleme ve şifre çözme için iki farklı anahtar kullanılır. Asimetrik bir şifreleme sistemindeki her kullanıcının hem bir genel anahtarı hem de bir özel anahtarı vardır. Özel anahtar her zaman gizli tutulur, ancak açık anahtar serbestçe dağıtılabilir.

Simetrik genellikle çok hızlıdır ve büyük miktarda veriyi şifrelemek için idealdir (örneğin, tüm disk bölümü veya veritabanı). Asimetrik çok daha yavaştır ve yalnızca anahtar boyutundan daha küçük (tipik olarak

2048 bit veya daha küçük) veri parçalarını şifreleyebilir. Bu nedenle, asimetrik kripto genellikle daha sonra çok daha büyük veri bloklarını şifrelemek için kullanılan simetrik şifreleme anahtarlarını şifrelemek için kullanılır. Dijital imzalar için, asimetrik kripto genellikle mesajların tamamı yerine mesajların karmalarını şifrelemek için kullanılır.

Bir şifreleme sistemi, anahtarların üretimi, değişimi, depolanması, kullanımı, iptali ve değiştirilmesi dahil olmak üzere kriptografik anahtarların yönetilmesini sağlar.

Kriptografi Hangi Sorunları Çözer?

Güvenli bir sistem, gizlilik, bütünlük ve verilerin kullanılabilirliğinin yanı sıra özgünlük ve inkar etmeme gibi birkaç güvence sağlamalıdır. Doğru kullanıldığında, kripto bu güvencelerin sağlanmasına yardımcı olur. Kriptografi, hem geçiş halindeki verilerin hem de kullanılmayan verilerin gizliliğini ve bütünlüğünü sağlayabilir. Ayrıca gönderenlerin ve alıcıların kimliğini doğrulayabilir ve reddedilmeye karşı koruyabilir.

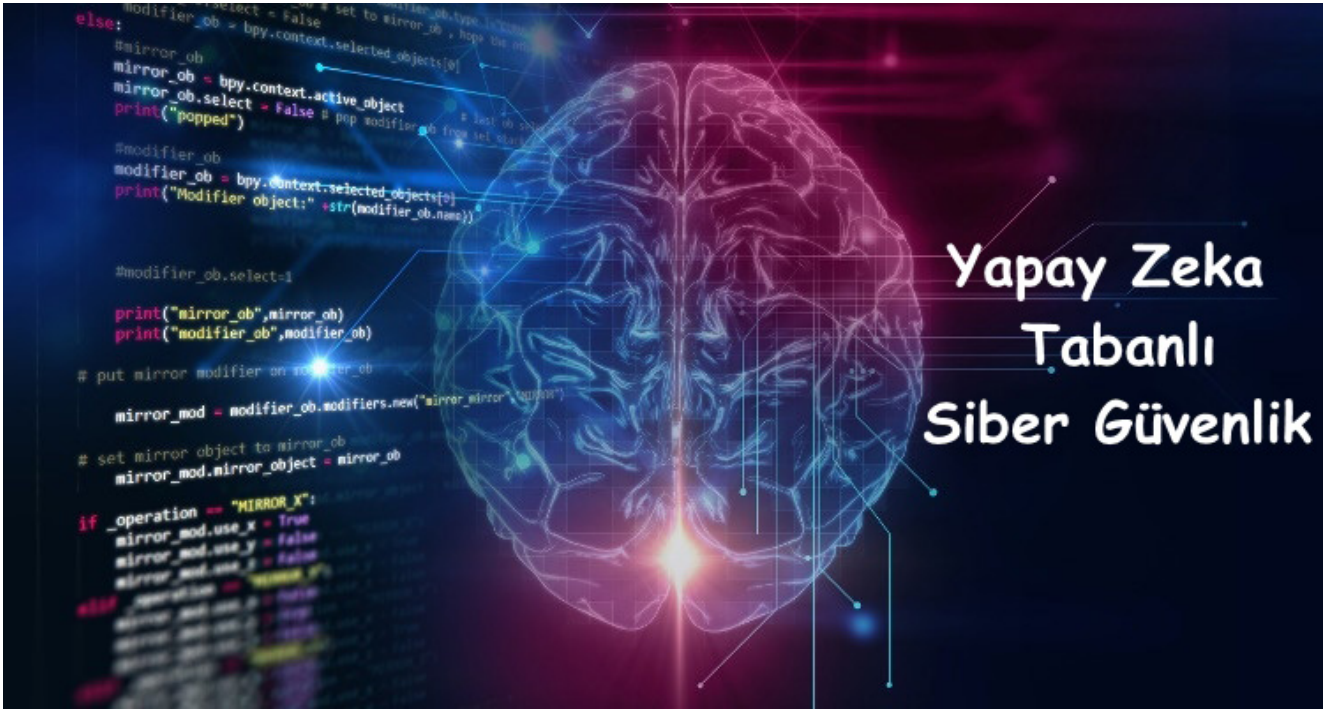
Yazılım sistemleri genellikle birden çok uç noktaya, tipik olarak birden çok istemciye ve bir veya daha fazla arka uç sunucusuna sahiptir. Bu istemci / sunucu iletişimleri, güvenilemeyen ağlar üzerinden gerçekleşir. İletişim, İnternet gibi açık, halka açık ağlar veya harici saldırganlar veya içerideki kötü niyetli kişiler tarafından tehlikeye atılabilecek özel ağlar üzerinden gerçekleşir.

Güvenilmeyen ağlardan geçen iletişimleri koruyabilir. Bir düşmanın bir ağ üzerinde gerçekleştirmeye çalışabileceği iki ana saldırı türü vardır. Pasif saldırılar, bir saldırganın yalnızca bir ağ kesimini dinlemesini ve seyahat ederken hassas bilgileri okumaya çalışmasını içerir. Pasif saldırılar çevrimiçi (bir saldırganın trafiği gerçek zamanlı olarak okuduğu) veya çevrimdışı (bir saldırganın trafiği gerçek zamanlı olarak yakaladığı ve daha sonra görüntülediği, belki de şifresini çözmek için biraz zaman harcadıktan sonra) olabilir. Etkin saldırılar, bir istemcinin veya sunucunun kimliğine bürünen, iletişimi kesen ve amaçlanan hedefe aktarmadan önce içeriği görüntüleyen ve / veya değiştiren (veya tamamen bırakan) bir saldırganın içerir. SSL / TLS gibi kriptografik protokoller tarafından sunulan gizlilik ve bütünlük korumaları, iletişimi kötü niyetli gizli dinleme ve kurcalamaya karşı koruyabilir. Orijinallik korumaları, kullanıcıların gerçekte sistemlerle amaçlandığı gibi iletişim kurduğuna dair güvence sağlar.

YAPAY ZEKA TABANLI SİBER GÜVENLİK

Gelişen teknolojiler siber güvenliği riske atıyor. Güvenlik profesyonellerinin savunma stratejilerindeki yeni gelişmeler bile bir noktada başarısız oluyor. Ayrıca, hücum-savunma stratejileri ve yenilikleri hiç bitmeyen bir döngü içinde ilerlerken, siber saldırıların karmaşıklığı ve hacmi artmıştır. Yapay zekanın (AI) gücünü siber güvenlik ile birleştiren güvenlik uzmanları, savunmasız ağları ve verileri siber saldırganlardan korumak için ek kaynaklara sahiptir. Bu teknolojiyi uyguladıktan sonra anında içgörüler sağladı ve yanıt sürelerinin kısalmasını sağladı.

Yapay zeka teknikleri, gürültünün veya istenmeyen verilerin nasıl kaldırılacağını öğrenmek ve güvenlik uzmanlarının anormal etkinliği tespit etmek için siber ortamı anlamasını sağlamak için kullanılabilir. Yapay Zeka, siber tehditler tespit edildiğinde otomatik tekniklerle siber güvenlikten yararlanabilir. Yapay Zeka, büyük miktarda veriyi analiz edebilir ve siber saldırıları azaltmak için mevcut sistemlerin ve yazılımların uygun bir şekilde geliştirilmesine izin verir. Benzer şekilde, siber güvenlik çözümleri için yapay zekanın uygulanması, kuruluşların mevcut siber tehditlerden korunmasına ve yeni kötü amaçlı yazılım türlerinin belirlenmesine yardımcı olacaktır. Ek olarak, yapay zeka tabanlı siber güvenlik sistemleri etkili güvenlik standartları sağlayabilir ve daha iyi önleme ve kurtarma stratejileri geliştirmeye yardımcı olabilir. Siber güvenlik için AI kullanımı, konumu veya ağ erişim ayrıcalıklarını değiştiren dinamik, gerçek zamanlı, küresel bir kimlik doğrulama çerçevesi oluşturmaya yardımcı olur.



Resim 49: Yapay Zeka Tabanlı Siber Güvenlik

Siber Güvenlik Çözümlerinde Hangi Tür Yapay Zeka Uygulamaları Kullanılıyor?

- Spam Filtresi Uygulamaları (spamassassin)
- Ağ İzinsiz Giriş Tespiti ve Önleme
- Dolandırıcılık tespiti
- Kredi puanlama ve sonraki en iyi teklifler
- Botnet Algılama
- Güvenli Kullanıcı Kimlik Doğrulaması
- Siber güvenlik Derecelendirmeleri
- Bilgisayar Korsanlığı Olayı Tahmini
- …

Bir yazılımı, kötü amaçlı yazılım mı yoksa yapay zeka ile normal bir yazılım mı tespit etmek mümkündür. Kötü amaçlı yazılım tespiti yapan bir yapay zeka uygulaması geliştirmek için yapılacak ilk şey bazı ayırt edici özellikleri belirlemektir. Bu özelliklere bazı zararsız yazılımlar ve bazı kötü amaçlı yazılımlara ek olarak, sistem eğitilir.

Bir yazılımın analizinde kullanılacak bazı özellikler şunlardır:

- Erişilen API'ler,
- Diskteki erişilen alanlar,
- Erişilen çevresel ürünlere (kamera, klavye vb.),
- Tüketilen işlemci gücü.

• Tüketilen bant genişliği.

• İnternet üzerinden iletilen veri miktarı.

Seçkin özellikler kullanılarak sistem kurulur. Sisteme bir test yazılımı verdiğinizde, bu ayırt edici özellikleri analiz ederek, yazılımın kötü amaçlı olup olmadığını tespit etmeye çalışır.

Günümüzün Siber Güvenliği ve Yapay Zeka ile Geleceği

Günümüzde kuruluşlar ağ güvenliklerine çok dikkat ediyor. Küçükten büyüğe her siber saldırının muazzam etkisinin farkındalar. Bu altyapıyı güvence altına almak için kuruluşlar birden çok savunma hattı kullanır. Bu çok katmanlı güvenlik sistemi genellikle ağ trafiğini kontrol edebilen ve filtreleyebilen en uygun güvenlik duvarı ile başlar. Bu katmandan sonra, ikinci savunma hattı antivirüs (AV) yazılımından oluşur. Bu AV araçları, kötü amaçlı kodları ve dosyaları bulmak ve ortadan kaldırmak için sistemi tarar. Bu iki savunma hattıyla kuruluşlar, felaket kurtarma planının bir parçası olarak düzenli olarak yedeklemeler gerçekleştirir. Şimdilik güvenlik duvarı politikaları oluşturmak, yedeklemeleri yönetmek ve bu tür birçok görev bir profesyonel gerektirir. Ancak AI(yapay zeka) geleneksel yaklaşımı değiştirecektir.

• Kuruluşlar, gelişmiş araçlar kullanarak güvenlik olaylarını izleyebilecek ve bunlara müdahale edebilecektir.

• Yeni nesil güvenlik duvarları, ağ paketlerinde bir model bulabilen ve bir tehdit olarak işaretlendiğinde bunları otomatik olarak engelleyebilen yerleşik makine öğrenimi teknolojisine sahip olacak.

• Tahmin edilebileceği gibi, yapay zekanın doğal dil yetenekleri, siber saldırıların ortaya çıkışını anlamak için kullanılacaktır. Bu teori, internet üzerinden veri taranarak uygulamaya konulabilir.

Yapay Zeka ve Makine Öğrenimi (ML) ile Geliştirilmiş Siber Güvenlik

Gizleme, polimorfizm ve diğerleri gibi karmaşık bilgisayar korsanlığı teknikleri, kötü niyetli programları tespit etmeyi gerçek bir zorluk haline getirir. Ayrıca alana özgü iş gücü sıkıntısı çeken siber güvenlik uzmanları (mühendisleri) bir başka sorundur. Yapay zekanın siber güvenliğe adım atmasıyla, uzmanlar ve araştırmacılar, sofistike siber saldırıları minimum insan müdahalesi ile belirlemek ve bunlara karşı koymak için potansiyelini kullanmaya çalışıyor. Bir AI alt kümesi olan AI ağları ve makine öğrenimi, güvenlik uzmanlarının yeni saldırı vektörleri hakkında bilgi edinmesini sağladı.

Siber güvenlikte makine öğrenimi, algoritmaların salt bir uygulamasından çok daha fazlasıdır. Siber tehditleri daha iyi analiz etmek ve güvenlik olaylarına yanıt vermek için kullanılabilir. Makine öğreniminin birkaç önemli faydası daha vardır:

• Kötü amaçlı etkinlikleri tespit eder ve siber saldırıları durdurur

• Siber tehditler için mobil uç noktaları analiz eder. (Google zaten bunun için makine öğrenimini kullanıyor.)

• Kötü niyetli saldırı tespitinden uç nokta korumasına kadar insan analizini iyileştirir

• Sıradan güvenlik görevlerini otomatikleştirmede kullanır

• Zero Day (Sıfır Gün) güvenlik açığı yok veya tamamen AI ile yok edilecektir.

Yapay zeka, kuruluşların güvenlik altyapısını güçlendirmek için zaten benimsenmiştir. Yapay zeka destekli çözümlerin siber güvenliği önemli ölçüde iyileştirdiği çok sayıda gerçek hayat örneği vardır.

• Gmail, günde 100 milyon spam'ı engellemek için makine öğrenimini kullanır . E-postaları filtrelemek ve

spam içermeyen bir ortamı verimli bir şekilde sunmak için bir sistem geliştirdi.

• IBM'in Watson bilişsel eğitimi, siber tehditleri ve diğer siber güvenlik çözümlerini tespit etmek için makine öğrenimini kullanır.

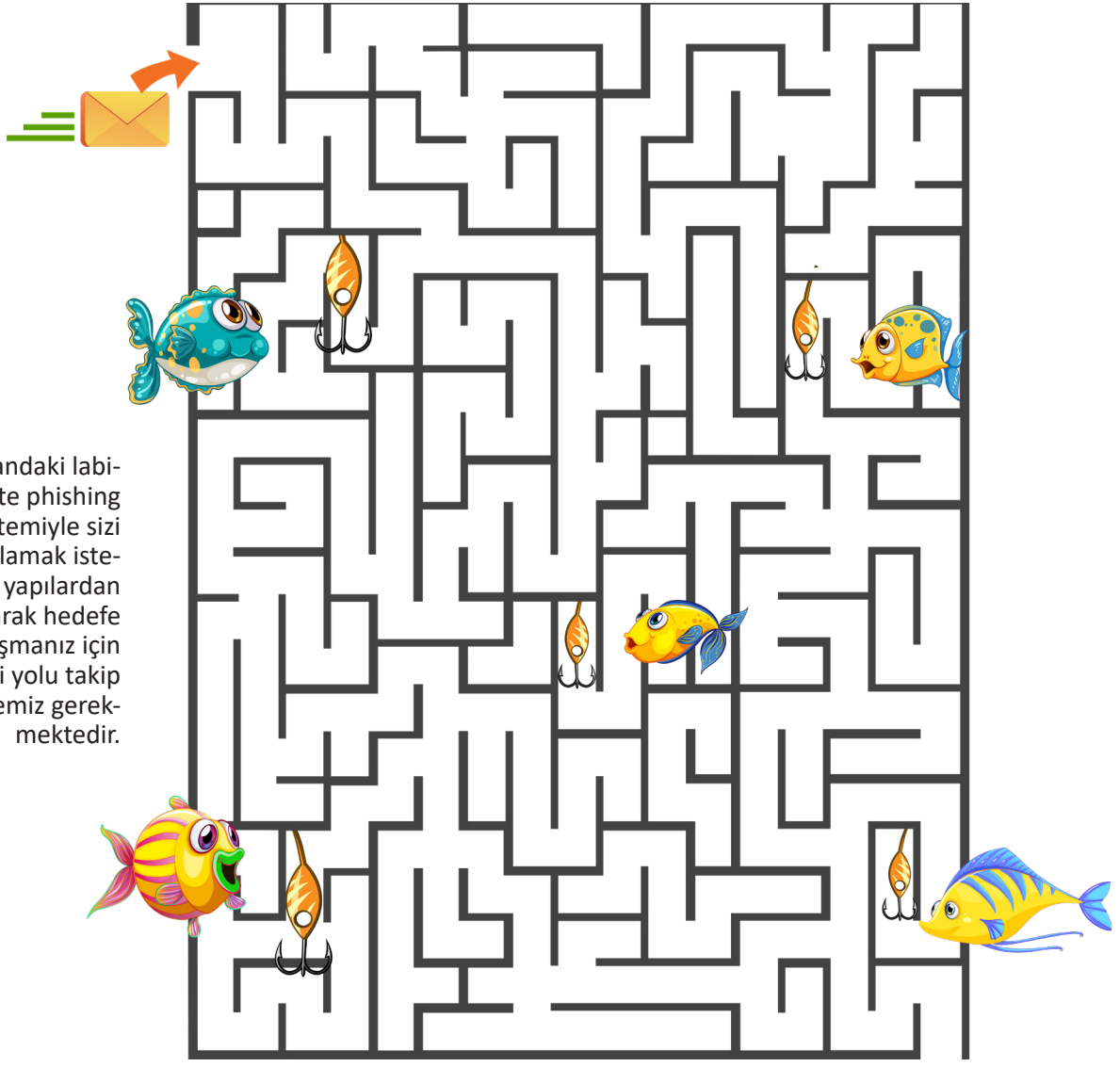
• Google, Cloud Video Intelligence platformunda Deep Learning AI kullanıyor . Bu platformda, sunucuda depolanan videolar içeriği ve bağlamına göre analiz edilir. AI algoritmaları, şüpheli bir şey bulunduğunda güvenlik uyarıları gönderir.

• Balbix platformu, BT altyapısını veri ve güvenlik ihlallerine karşı korumak için yapay zeka destekli risk tahminleri kullanır.

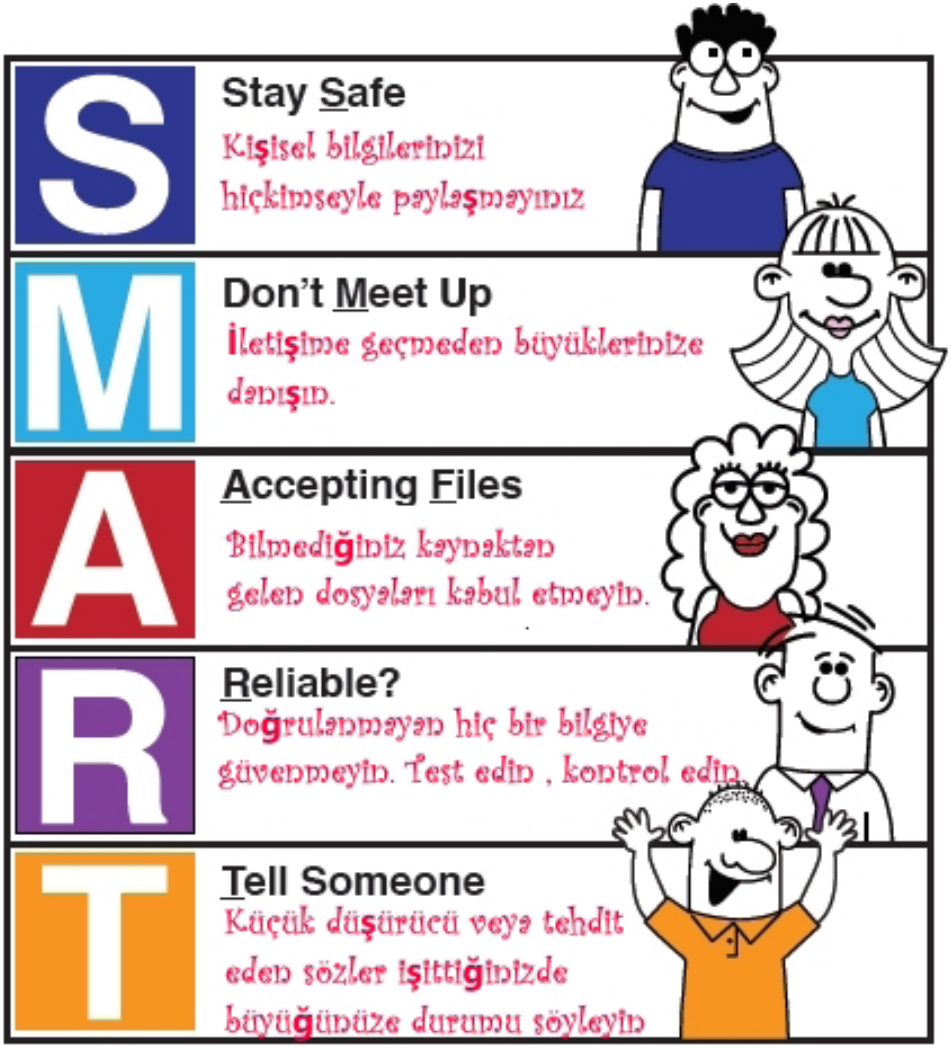
Yakın zamanda yapay zeka destekli sistemler siber güvenlik çözümlerinin ayrılmaz bir parçası olacaktır. Ayrıca siber suçlular tarafından kuruluşlara zarar vermek için de kullanılacaktır. Yapay zekayı otomatik programları kullanarak gelişmiş tehditlere duyarlı hale getirecektir. Diğer herhangi bir siber güvenlik çözümü gibi AI da% 100 kusursuz değildir. Siber saldırıları sınırlama ve sıradan rutin görevleri otomatikleştirme yeteneğine sahip iki ucu keskin bir kılıçtır ve yine de bir lütuftur. Otomasyon dalgası günlük görevleri üstlenirken, aynı teknoloji daha az insan hatası ve ihmal olasılığını artıracaktır.

EĞLENELİM ÖĞRENELİM

Yandaki labirentte phishing yöntemiyle sizi avlamak isteyen yapılardan kaçarak hedefe ulaşmanız için hangi yolu takip etmemiz gerekmektedir.



ONLİNE ORTAMDA AKILLI (SMART) OL!



Resim 50: SMART (Akıllı) Olma Açılımı

ÖLÇELİM DEĞERLENDİRELİM-4

1. Etik bir bilgisayar korsanının işi, aynı zamanda çeşitli araçları nasıl kullanacağını anlamayı ve bilmeyi gerektirir. Aşağıdaki programlar ve hangi amaçla kullanıldığını eşleştiriniz.

……. A) NMap 1.Veri sızıntısını tespit etmek için ağları izlemek için kullanılır.

……. B) Wireshark 2. Güvenlik denetimleri yapmak için kullanılır.

……. C) BadMod 3.Web uygulaması güvenliğini ölçmek için kullanılır.

2. Kriptografi nedir, açıklayınız.

CEVAP: ……

……

……

……

3. Kötü amaçlı yazılım kurulumunu önleyen hizmetler nelerdir?

CEVAP:

1)
2)
3)
4)
5)

4. Etik Hackleme özellikleri nelerdir?

CEVAP: ……

……

……

……

5. İnternet ortamında güvenliğimizi sağlamak için neler yapmalıyız?

CEVAP: .....

.....

.....

.....

SONSÖZ

Siber güvenlik, bilgisayar sistemlerini ve elektronik verileri korumak için kullanılan tüm teknolojileri ve süreçleri kapsayan genel bir terimdir. Bu tanım, siber güvenliğin tam olarak ne olduğunu açıklasa da, tek başına bir tanım, siber güvenliğin neredeyse tüm varlıkların yaşamlarında oynadığı önemi vurgulayamaz.

Hükümetimizden dünyanın en büyük şirketlerine, birey olarak sizlere, siber güvenlik kritik bir rol oynar. Siber güvenlik neden bu kadar önemli? İşletmeleri ve insanları, bilgisayar korsanlarından, kötü amaçlı yazılımlardan, casus yazılımlardan ve diğer tehlikeli korsanlık yöntemlerinden gelen kötü amaçlı saldırılardan koruyan mekanizmadır.

Hassas bilgilerin depolanması ve işlenmesi için yeni teknolojilerden yararlanmaya devam ettikçe, siber güvenliğin rolü gelecekte de hiç şüphesiz artacaktır ve hem sizin hem de işletmenizin yeni ve ortaya çıkan tehditlere karşı güvende olmasını sağlamak için şimdiki zamana benzer bir zaman yoktur.

Teknolojiye artan bağımlılığımız, siber güvenlik önlemlerinin artık bu kadar önemli olmasının nedenidir. İster kişisel hayatımızda ister işte, teknolojiyi hemen hemen her soruna çözüm olarak kullanıyoruz. Şifrelerimizi şifre tutucu veya şifre hatırlat gibi üçüncü taraf araçlarda saklıyoruz ve kredi kartı ve banka bilgilerimizi Dropbox veya Google Drive gibi bulut depolama hizmetlerinde tutuyoruz. Bunu yaparken kendimizi siber suç tehdidine açıyoruz.

Siber suçla mücadeleyi kazanmanın büyük bir adımı, bireylerden çok uluslu büyük şirketlere kadar hiç kimsenin siber suçun oluşturduğu tehditten muaf olmadığını kabul etmektir. Varsayabileceğiniz en kötü şeylerden biri, ‘asla benim başıma gelmeyecek’ olmasıdır.

Eğitim, siber suçla mücadele stratejisinin çok önemli bir parçasıdır ve CEO’dan büro personeline kadar kuruluşunuzdaki herkesin ağınızı ve uygulamalarınızı kullanırken olası riskleri anlaması önemlidir. Bu bilinçle Urfa STEM ve Bilim Merkezi ve Genç STEM Derneği olarak bünyemizde çalışan herkesin siber güvenlik eğitimi almasını sağladık. Genç STEM Derneğinde ve Urfa STEM ve Bilim Merkezinde verilen eğitimlerin bir parçası da kişisel güvenliği sağlamaya yönelik Siber güvenlik ve en önemlisi Siber Savunmaya yönelik olmaktadır. Bu kitap sayesinde siber güvenlik kavramlarını tanıyacak ve güvenliğinizi sağlamak için hangi hizmetleri kullanmanız gerektiğinin farkında olacaksınız.

Urfa STEM ve Genç STEM
Eğitmenleri adına
Halil İbrahim ÇETİN

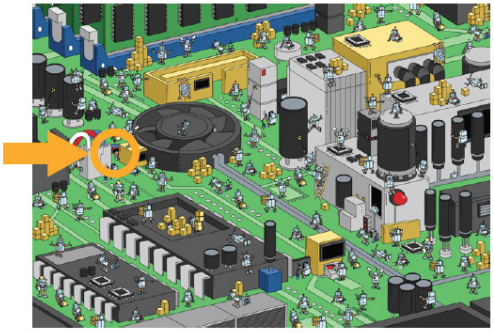
CEVAP ANAHTARI

Eğlenelim-Öğrenelim 1 Çözümü

R A Q X S S W O I T Y B E R N S O W
M S P E A R O O F Y E C D I E P N G
R A F C Y I U P K L Y M R N B E V C
A T G T Y E W Q A B F T O H J A J L
N Y N X C B M M E N B V W G H R Y P
S Z I Q A U E R I E O O S E A P M Z
O W F I E T H R T U M N S B V H S S
M F O G K E L C B Z O O A Q W I E R
W T O P R Y U I O U P A P S D S F G
A L P O A C G N I V L M N L K H D H
R K S S M I S H I N G L S E K I S T
E S P O E P H N D W O E Y A Y N O N
T Q I U G N I H S I H P B I F G E M
E U H O W M U G W O R D S S N I N G
H I D O R E H R E B S L E V B G U W

Eğlenelim-Öğrenelim 2 Çözümü

Eğlenelim-Öğrenelim 4 Çözümü



ÖLÇELİM DEĞERLENDİRELİM-1

CEVAP 1: Ağ güvenliği, Uygulama güvenliği, Uç nokta güvenliği, Veri güvenliği, Kimlik yönetimi, Veritabanı ve altyapı güvenliği, Bulut güvenliği, Mobil güvenlik, Afet kurtarma / iş sürekliliği planlaması

CEVAP 2:

1) Arama ve Belirleme

2) Koruma

3) Tespit Etme

4) Karşılık Vermek

5) Kurtarma

CEVAP 3: D) Oyun Güvenliği Şıkkı

CEVAP 4: Gizlilik , veri merkezli ekonomi , altyapı riski , küresel risk yapılarından ötürü siber güvenlik gereklidir.

CEVAP 5: Uç nokta güvenliği, bir şirketin ağına uzaktan erişimi koruma sürecidir. Kendi personellerine uzaktan erişim yetkisi vererek bir başkasının sisteme sızmasını engelleyici yapıları içermektedir.

ÖLÇELİM DEĞERLENDİRELİM-2

CEVAP 1: Bulut bilişim, farklı hizmetlerin İnternet üzerinden sunulmasıdır. Bu kaynaklar, veri depolama, sunucular, veritabanları, ağ oluşturma ve yazılım gibi araçları ve uygulamaları içerir. Bulut güvenliği, bulut bilişim platformları aracılığıyla çevrimiçi olarak depolanan verilerin hırsızlık, sızıntı ve silinmeye karşı korunmasıdır. Bulut güvenliği sağlama yöntemleri arasında güvenlik duvarları, sızma testi, gizleme, belirteçlere ayırma, sanal özel ağlar (VPN) ve genel internet bağlantılarından kaçınma yer alır.

CEVAP 2: Saldırganlar, çeşitli vektörler aracılığıyla hedeflenen bir sunucuyu veya çevresindeki altyapıyı farklı türlerde saldırı trafiğiyle aşırı yükleyebilir. Bir sunucu gelen istekleri artık etkili bir şekilde işleyemediğinde, yavaş davranmaya başlar ve sonunda yasal kullanıcılardan gelen isteklere hizmet vermeyi reddeder.

CEVAP 3:

1) Fiziksel

2) Teknik

3) İdari

CEVAP 4:

3 A) Gizlilik - 1. Bilginin güvenilir ve doğru olmasını sağlar.

2 B) Kullanılabilirlik - 2. Verilerin iş ihtiyaçlarını karşılamak için hem kullanılabilir hem de erişilebilir olmasını sağlar.

1 C) Dürüstlük - 3. Verilere yalnızca yetkili kişiler tarafından erişilmesini sağlar.

CEVAP 5: SQi, bir saldırganın bir veritabanının arama sorgularını yürütme biçimindeki güvenlik açıklarından yararlandığı bir yöntemdir. Saldırganlar, yetkisiz bilgilere erişmek, yeni kullanıcı izinlerini değiştirmek veya oluşturmak veya hassas verileri başka şekilde değiştirmek veya yok etmek için SQi'yi kullanır.

ÖLÇELİM DEĞERLENDİRELİM-3

CEVAP 1: D)nslookup Şıkkı

CEVAP 2:

1) Planlama ve Keşif

2) Tarama

3) Erişim Sağlamak

4) Erişimi Sürdürmek

5) Analiz ve WAF konfigürasyonu

CEVAP 3: Kimlik avı, bireyleri kişisel olarak tanımlanabilen bilgiler, bankacılık ve kredi kartı bilgileri ve parolalar gibi hassas verileri sağlamaya teşvik etmek için meşru bir kurum gibi davranan biri tarafından bir hedef veya hedefle e-posta, telefon veya kısa mesaj yoluyla iletişime geçildiği bir siber suçtur.

CEVAP 4: İzleme tanımlama bilgileri (Tracking cookies), Tuş kaydediciler (Keyloggers), Takip yazılımı (Stalkerware), Hırsızlık Yazılımı (Stealware), Sistem monitörleri (System monitors)

CEVAP 5: Facebook, Instagram, Snapchat ve Tik Tok gibi Sosyal Medya , Mobil veya tablet cihazlarda yazılı mesajlaşma ve mesajlaşma uygulamaları, İnternet üzerinden anında mesajlaşma, doğrudan mesajlaşma ve çevrimiçi sohbet,Reddit gibi çevrimiçi forumlar, sohbet odaları ve mesaj panoları, E-posta, Çevrimiçi oyun toplulukları

ÖLÇELİM DEĞERLENDİRELİM-4

CEVAP 1:

2 A) NMap - 1.Veri sızıntısını tespit etmek için ağları izlemek için kullanılır.

1 B) Wireshark - 2. Güvenlik denetimleri yapmak için kullanılır.

3 C) BadMod - 3.Web uygulaması güvenliğini ölçmek için kullanılır.

CEVAP 2: Kriptografi, düşman olarak bilinen kötü niyetli üçüncü şahısların varlığında güvenli iletişim sağlar. Şifreleme, bir girişi (yani düz metin) şifreli bir çıktıya (yani şifreli metin) dönüştürmek için bir algoritma ve anahtar kullanır. Belirli bir algoritma, aynı anahtar kullanılırsa her zaman aynı düz metni aynı şifreli metne dönüştürür.

CEVAP 3:

1) Web Uygulama Güvenlik Duvarı (WAF)

2) Arka Kapı Koruması

3) Oturum Açma Koruması

4) Antivirüs Programları

5) Windows Güvenlik Duvarı

CEVAP 4: Sistemin güvenlik açıklarını bulmak için yetkili yöntem, yasaldır,beyaz şapka korsanları etik hackleme gerçekleştirir, gerçek zamanlı hacklemeyi önlemek için kuruluşun çalışanı tarafından gerçekleştirilir.

CEVAP 5: Kişisel bilgiler ebeveyn izni olmadan asla verilmemelidir, şifreler gizli tutulmalıdır, bir sosyal medya sitesinde yayınlanan her şeyin İnternette sonsuza kadar kalacağını varsayın, internetteki yabancılarla asla yüz yüze görüşmeyin, siber zorbalık, çocuklar için en büyük risklerden biridir.

KAYNAKÇA

1.2020, https://www.digitalattackmap.com/understanding-ddos/

2. 2020, https://www.imperva.com/learn/application-security/penetration-testing/

3.2020, https://icssindia.in/top-15-best-cmd-commands-used-hacking-2019/#:~:text=Hacking%20in%202019-,15%20Best%20CMD%20Commands%20Used%20for%20Hacking%20in%202019,%234%20arp

4. 2020, https://www.imperva.com/learn/application-security/malware-detection-and-removal/

5. 2020, https://enterprise.comodo.com/what-is-a-trojan-virus.php

6. 2020, https://www.forcepoint.com/cyber-edu/cybersecurity

7. 2020, https://digitalguardian.com/blog/what-cyber-security

8. 2020, https://www.opencolleges.edu.au/informed/cyber-safety/

9. 2020, https://www.pbs.org/wgbh/nova/labs/lab/cyber/

10. 2020, https://www.forcepoint.com/tr/cyber-edu/data-security

11. 2020, https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint

12. 2020, https://www.paloaltonetworks.com/cyberpedia/what-is-a-cloud-security

13. 2020, https://www.ecpi.edu/blog/why-does-cyber-security-matter-to-everyone

14. 2020, https://www.apcointl.org/cybersecurity/apco-cybersecurity-resources/why-cybersecurity-matters/

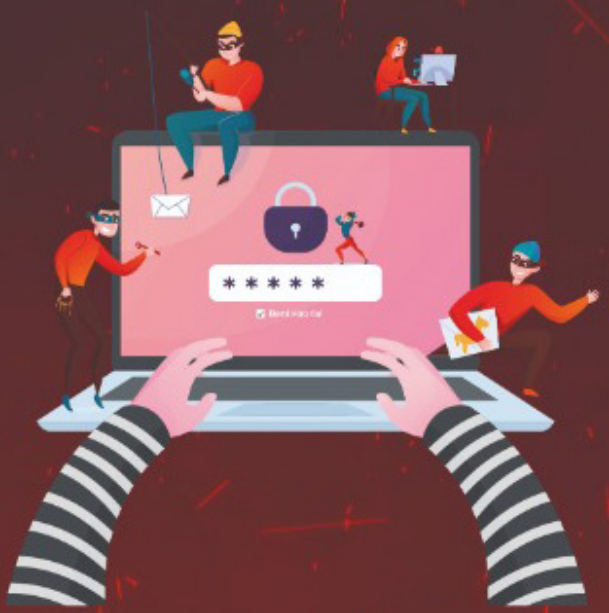
15. 2020, https://www.prilock.com/school-kids.php

16. 2020, https://edition.cnn.com/2020/05/20/tech/virtual-cyber-security-school/index.html

17. 2020, https://www.cisoplatform.com/profiles/blogs/cyber-security-for-kids-repository

18. Epic Cyber Hero Handbook,Popcorn Training 2018,6

URFA STEM



URFASTEM