SOME
EL KİTABI

OKAN YILDIZ

Kapak : Ertuğrul ÜNGÖR

İçindekiler

SOME Nedir 5

Hizmet Alanları ve Organizasyon Şeması 5

SOME'lerin Görevleri 7

Kurumsal SOME'lerin görev ve sorumlulukları: 8

Sektörel SOME'lerin görev ve sorumlulukları 9

Bilişim Suçları 10

Bilişim sistemine girme 10

Sistemi engelleme, bozma, verileri yok etme veya değiştirme 11

Banka veya kredi kartlarının kötüye kullanılması 11

Tüzel kişiler hakkında güvenlik tedbiri uygulanması 12

Haberleşmenin engellenmesi 12

Haberleşmenin gizliliğini ihlâl 12

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması 13

Özel hayatın gizliliğini ihlâl 13

Kişisel verilerin kaydedilmesi 13

Verileri hukuka aykırı olarak verme veya ele geçirme 14

Nitelikli hâller 14
Nitelikli hırsızlık 14
Nitelikli dolandırıcılık 14
Devletin güvenliğine ilişkin belgeler 15
Devletin güvenliğine ilişkin bilgileri temin etme ... 15
Siyasal veya askerî casusluk 15
Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama 16
Gizli kalması gereken bilgileri açıklama 16
SOME'ler İçin Tavsiyeler 17
1. DNS Güvenliği 17
DNS Nedir ve Nasıl Çalışır 17
DNS Üzerinden Tehditler: 18
DNS Tehditleri 18
DNS güvenliği için öneriler: 20
2. Kurumsal Ağ Güvenliği 21
Ağ Güvenliği Nedir: 21
Ağ Güvenliği Nasıl Sağlanır: 21
Alınması Gereken Önlemler: 23
3. DoS/DDoS Saldırıları ve Korunma Yolları 26
DoS/DDoS Nedir 26
Bazı Saldırı Çeşitleri 28

DDoS Saldırılarına Karşı Alınabilecek Tedbirler 29

4. Web Uygulamaları Güvenliği....31

Web Uygulamalarına Yönelik Saldırılar:....31

Alınabilecek Önlemler: 33

5. Web Servisleri Güvenliği....35

Web Servisi Nedir: 35

Web Servisleri Güvenliği:....36

6. Zararlı Yazılımlar 42

Zararlı Yazılım Nedir: 42

Zaralı Yazılım Türleri:....43

Alınabilecek Önlemler: 45

7. Ransomware Saldırıları: 46

Ransomware Nedir: 46

Verilerin Rehin Alınması: 47

Alınabilecek Tedbiler:....48

8. Sosyal Mühendislik Saldırıları:....48

Sosyal Mühendislik Nedir: 48

Sosyal Mühendisin Hedefindeki Personeller 50

Sosyal Mühendislik Saldırılarında Kullanılan Yöntemler:....51

Sosyal Mühendislik Saldırılarına Önlemler: 52

9. Phishing (Oltalama) Saldırıları:.....53
Phishing Saldırısı Nedir:.....53
Phishing Saldırısının Amaçları Nelerdir:.....54
Alınması Gereken Önlemler:.....55
10. Kurumsal Sosyal Medya Hesabı Güvenliği 56
Alınması Gereken Önlemler:.....57
11. Parola Güvenliği 62
Parola Güvenliği İçin Tavsiyeler:.....64
Linux/Windows Dosyaları ve Komutları: 65
Linux: 65
Linux Dosyaları ve Kullanım Amaçları:.....67
Windows Komutları:.....69
Kaynakçalar: 72

SOME Nedir

SOME, kurumsal ve sektörel olmak üzere ikiye ayrılan Siber Olaylara Müdahale Ekiplerinin kısaltmasıdır. Bilişim Teknoloji ve İletişim Kurumu'na bağlı olarak kurulan SOME'ler , siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar.

Ulusal Siber Güvenlik Strateji ve 2013-2014 Eylem Planı oluşturulmuş ve 20/06/2012 tarihinde Bakanlar Kurulu kararı olarak yayınlanmıştır. Söz konusu eylem planı kapsamında temel görevi kordinasyon ve işbirliği olan Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurularak, faaliyetlerine başlamıştır. Eylem planı çerçevesinde kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekiplerinin (SOME) oluşturulması öngörülmüştür.

Hizmet Alanları ve Organizasyon Şeması

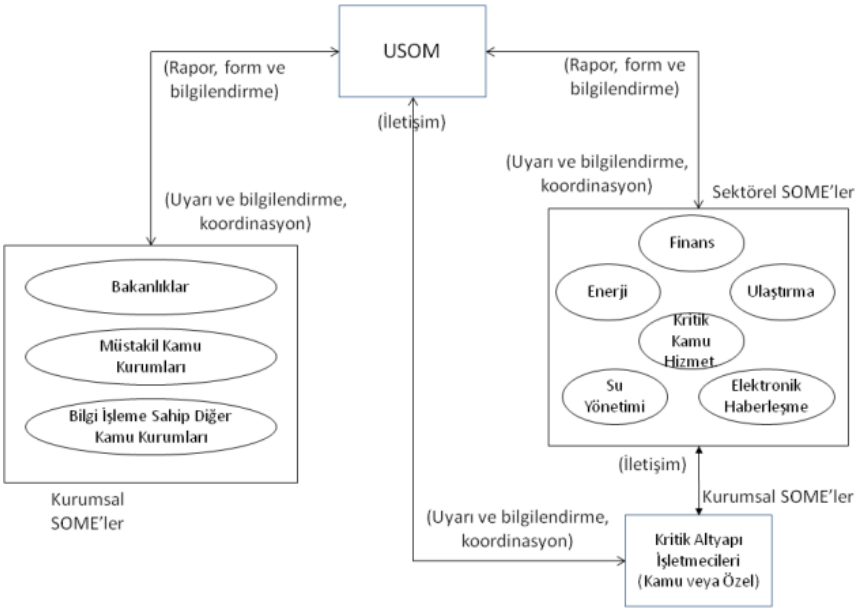
Siber olaylara müdahalelerde kurulmuş üç temel kurum USOM,Sektörel SOME'ler ve Kurumsal SOME'lerdir. Bu üç kurumun hizmet alanları aşağıdaki tabloda verilmiştir.

Organizasyon	Kurulduğu Kurum / Kuruluş	Hizmet Alanı
USOM	BTK / Telekomünikasyon İletişim Başkanlığı (TİB)	Ulusal siber ortam
Sektörel SOME	• Kritik sektörü düzenleyici ve denetleyici kurumlar • Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili bakanlık	Kritik altyapı sektörü
Kurumsal SOME	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumlar	Kamu kurum, kuruluşları ve kritik altyapı sektörlerindeki özel kurumların siber ortamları

Kritik altyapıları için, Sektörel SOME'nin kurulacağı kurum aşağıda verilmiştir.

Kritik Altyapı Sektörü	Sektörel SOME'nin Kurulacağı Kurum
Enerji	İlgili düzenleyici ve denetleyici kurum
Elektronik Haberleşme	
Finans	
Su yönetimi	Düzenleyici ve denetleyici kurumlar kuruluncaya kadar ilgili bakanlık
Kritik Kamu Hizmetleri	
Ulaştırma	

Ülkemiz kamu kurumlarını ve kritik altyapıları içine alan siber olaylara müdahale organizasyonu aşağıda verilmiştir.



SOME'lerin Görevleri

11 Kasım 2013 tarihinde resmi gazetede yayınlanan Kurumsal ve Sektörel SOME'lerin görev ve sorumlulukları aşağıda verilmiştir.

Kurumsal SOME'lerin görev ve sorumlulukları:

(1) Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılmasımuhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelikçalışmaları yapmak veya yaptırmakla yükümlüdürler.

(2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusundaöneri sunarlar.

(3) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini varsa birlikte çalıştığı sektörel SOME ile eşgüdüm içerisinde yürütürler. Durumdan gecikmeksizin USOM'u haberdar ederler.

(4) Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar. Bunun mümkün olmaması halinde varsa birlikte çalıştığı sektörel SOME'den ve/veya USOM'dan yardım talebinde bulunabilirler.

(5) Kurumsal SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.

(6) Kurumsal SOME'ler kurumlarına yapılan siber olayları raporlar ve gecikmeksizin USOM ve birlikte çalıştığısektörel SOME'ye bildirirler.

(7) Kurumsal SOME'ler USOM ve/veya birlikte çalıştığı sektörel SOME tarafından iletilen siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirleri alırlar.

(8) Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lereve USOM'a bildirirler.

Sektörel SOME'lerin görev ve sorumlulukları

(1) Sektörel SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütürler.

(2) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde ya şanan siber olayları gecikmeksizin USOM'a bildirirler.

(3) Sektörel SOME'ler siber olaylara ilişkin USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları SOME'lerde gerekli tedbirlerin alınmasına yönelik çalışmaları yürütürler.

(4) Sektörel SOME'ler birlikte çalıştıkları SOME'lerin yap ılanması konusunda düzenleyici faaliyetleri yürütürler.

(5) Sektörel SOME'ler ilgili oldukları sektörde, bilgilendirme, bilinçlendirme ve eğitim faaliyetleri ile siber güvenlikle ilgili kabiliyetlerinin geliştirilmesi ve önlemlerin alınması konusunda gerekli düzenleyici faaliyetleri yürütürler.

(6) Sektörel SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek
birlikte çalıştıkları SOME'lere veUSOM'a bildirirler.

(7) SOME'ler 7/24 erişilebilir olan iletişim
bilgilerini Sektörel SOME'lere ve USOM'a bildirirler.

(8) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde ya şanan siber olaylarda imkânları ölçüsünde gerekli desteği sağlarlar. Sektörel SOME'ler, imkânlarının yetersiz olması durumunda USOM'dan destek alırlar.

(9) Sektörel SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.

(10) Sektörel SOME'ler gerekmesi durumunda birlikte çalıştıkları SOME'ler arasındaki işbirliğini koordine ederler.

Bilişim Suçları

Bilişim sistemine girme

MADDE 243. - (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren ve orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.

(2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi hâlinde, verilecek ceza yarı oranına kadar indirilir.

(3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur.

Sistemi engelleme, bozma, verileri yok etme veya değiştirme

MADDE 244. - (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır.

(4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunur.

Banka veya kredi kartlarının kötüye kullanılması

MADDE 245. - (1) Başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse, kart sahibinin veya kartın kendisine verilmesi gereken kişinin rızası olmaksızın bunu kullanarak veya kullandırtarak kendisine veya başkasına yarar sağlarsa, üç yıldan altı yıla kadar hapis cezası ve adlî para cezası ile cezalandırılır.

(2) Sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi, fiil daha ağır cezayı gerektiren başka bir suç oluşturmadığı takdirde, dört yıldan yedi yıla kadar hapis cezası ile cezalandırılır.

Tüzel kişiler hakkında güvenlik tedbiri uygulanması

MADDE 246. - (1) Bu bölümde yer alan suçların işlenmesi suretiyle yararına haksız menfaat sağlanan tüzel kişiler hakkında bunlara özgü güvenlik tedbirlerine hükmolunur.

Haberleşmenin engellenmesi

MADDE 124. - (1) Kişiler arasındaki haberleşmenin hukuka aykırı olarak engellenmesi hâlinde, altı aydan iki yıla kadar hapis veya adlî para cezasına hükmolunur.

(2) Kamu kurumları arasındaki haberleşmeyi hukuka aykırı olarak engelleyen kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır.

(3) Her türlü basın ve yayın organının yayınının hukuka aykırı bir şekilde engellenmesi hâlinde, ikinci fıkra hükmüne göre cezaya hükmolunur.

Haberleşmenin gizliliğini ihlâl

MADDE 132. - (1) Kişiler arasındaki haberleşmenin gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Bu gizlilik ihlâli haberleşme içeriklerinin kaydı suretiyle gerçekleşirse, bir yıldan üç yıla kadar hapis cezasına hükmolunur.

(2) Kişiler arasındaki haberleşme içeriklerini hukuka aykırı olarak ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır.

(3) Kendisiyle yapılan haberleşmelerin içeriğini diğer tarafın rızası olmaksızın alenen ifşa eden kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(4) Kişiler arasındaki haberleşmelerin içeriğinin basın ve yayın yolu ile yayınlanması hâlinde, ceza yarı oranında artırılır.

Kişiler arasındaki konuşmaların dinlenmesi ve kayda alınması

MADDE 133. - (1) Kişiler arasındaki alenî olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki aydan altı aya kadar hapis cezası ile cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aya kadar hapis veya adlî para cezası ile cezalandırılır.

(3) Yukarıdaki fıkralarda yazılı fiillerden biri işlenerek elde edildiği bilinen bilgilerden yarar sağlayan veya bunları başkalarına veren veya diğer kişilerin bilgi edinmelerini temin eden kişi, altı aydan iki yıla kadar hapis ve bin güne kadar adlî para cezası ile cezalandırılır. Bu konuşmaların basın ve yayın yoluyla yayınlanması hâlinde de, aynı cezaya hükmolunur.

Özel hayatın gizliliğini ihlâl

MADDE 134. - (1) Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi hâlinde, cezanın alt sınırı bir yıldan az olamaz.

(2) Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Fiilin basın ve yayın yoluyla işlenmesi hâlinde, ceza yarı oranında artırılır.

Kişisel verilerin kaydedilmesi

MADDE 135. - (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasî, felsefî veya dinî görüşlerine, ırkî kökenlerine; hukuka aykırı olarak ahlâkî eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına

ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır.

Verileri hukuka aykırı olarak verme veya ele geçirme

MADDE 136. - (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Nitelikli hâller

MADDE 137. - (1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle,

İşlenmesi hâlinde, verilecek ceza yarı oranında artırılır.

Nitelikli hırsızlık

MADDE 142. - (1) Hırsızlık suçunun;

e) Bilişim sistemlerinin kullanılması suretiyle, İşlenmesi hâlinde, üç yıldan yedi yıla kadar hapis cezasına hükmolunur. Suçun, bu fıkranın (b) bendinde belirtilen surette, beden veya ruh bakımından kendisini savunamayacak durumda olan kimseye karşı işlenmesi halinde, verilecek ceza üçte biri oranına kadar artırılır.

Nitelikli dolandırıcılık

MADDE 158. - (1) Dolandırıcılık suçunun;

f) Bilişim sistemlerinin, banka veya kredi kurumlarının araç olarak kullanılması suretiyle,

g) Basın ve yayın araçlarının sağladığı kolaylıktan yararlanmak suretiyle,

İşlenmesi hâlinde, iki yıldan yedi yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur.

Devletin güvenliğine ilişkin belgeler

MADDE 326. - (1) Devletin güvenliğine veya iç veya dış siyasal yararlarına ilişkin belge veya vesikaları kısmen veya tamamen yok eden, tahrip eden veya bunlar üzerinde sahtecilik yapan veya geçici de olsa, bunları tahsis olundukları yerden başka bir yerde kullanan, hileyle alan veya çalan kimseye sekiz yıldan oniki yıla kadar hapis cezası verilir.

(2) Yukarıdaki yazılı fiiller, savaş sırasında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye koymuş ise müebbet hapis cezası verilir.

Devletin güvenliğine ilişkin bilgileri temin etme

MADDE 327. - (1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgileri temin eden kimseye üç yıldan sekiz yıla kadar hapis cezası verilir.

(2) Fiil, savaş sırasında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye koymuşsa müebbet hapis cezası verilir.

Siyasal veya askerî casusluk

MADDE 328. - (1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından, niteliği itibarıyla, gizli kalması gereken bilgileri, siyasal veya askerî casusluk maksadıyla temin eden kimseye onbeş yıldan yirmi yıla kadar hapis cezası verilir.

(2) Fiil;

a) Türkiye ile savaş hâlinde bulunan bir devletin yararına işlenmişse,

b) Savaş sırasında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye sokmuşsa,

Fail, ağırlaştırılmış müebbet hapis cezası ile cezalandırılır.

Devletin güvenliğine ve siyasal yararlarına ilişkin bilgileri açıklama

MADDE 329. - (1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından niteliği itibarıyla gizli kalması gereken bilgileri açıklayan kimseye beş yıldan on yıla kadar hapis cezası verilir.

(2) Fiil, savaş zamanında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeye koymuşsa, faile on yıldan onbeş yıla kadar hapis cezası verilir.

(3) Fiil, failin taksiri sonucu meydana gelmiş ise birinci fıkrada yazılı olan hâlde, faile altı aydan iki yıla, ikinci fıkrada yazılı hâllerden birinin varlığı hâlinde ise üç yıldan sekiz yıla kadar hapis cezası verilir.

Gizli kalması gereken bilgileri açıklama

MADDE 330. - (1) Devletin güvenliği veya iç veya dış siyasal yararları bakımından niteliği itibarıyla gizli kalması gereken bilgileri siyasal veya askerî casusluk maksadıyla açıklayan kimseye müebbet hapis cezası verilir.

(2) Fiil, savaş zamanında işlenmiş veya Devletin savaş hazırlıklarını veya savaş etkinliğini veya askerî hareketlerini tehlikeyle karşı karşıya bırakmış ise, faile ağırlaştırılmış müebbet hapis cezası verilir.

SOME'ler İçin Tavsiyeler

1. DNS Güvenliği

DNS Nedir ve Nasıl Çalışır

Alan adı sistemi olan DNS (Domain Name System), isim sunucu ve çözümleyicilerden oluşur, internete açılan kapılardır. İsim sunucular, host isimlerine karşılık gelen ip adreslerinin ismini tutar. Çözümleyiciler ise DNS istemciler olarak bilinir ve bu istemcilerde, DNS sunucu yada diğer sunucuların bilgisini tutar.

Web siteleri, URL olarak adlandırılan kolay adres ve IP adresine sahiptir. Kullanıcılar web sitelerini bulmak için URL'leri, bilgisayarlar ise IP adreslerini kullanır. DNS URL'leri IP adreslerine dönüştürür (veya tam tersi). Örneğin, web tarayıcınızdaki adres çubuğuna http://www.alanadi.com yazarsanız, bilgisayarınız DNS sunucusuna bir istek gönderir. DNS sunucusu URL'yi IP adresine dönüştürerek bilgisayarınızın Microsoft web sunucusunu bulabilmesini sağlar.

DNS sistemine ait bazı bileşenler aşağıda verilmiştir;

- **A** ➔ Domain Name den IP adresine dönüşüm yapar.
- **MX**➔ Belli bir Domain' e gelen e-postaların hangi makineye dağıtılacağını bulur
- **NS**➔ Alan adınızın sorgulanmasında kullanılacak olan isim sunucularıdır.
- **PTR**➔ Verilen ip adresinin, isim karşılığını bulur.
- **HINFO** ➔ Bilgisayarın donanım ve işletim sistemi gibi bilgilerini yazmak için kullanılır.

- **TXT➔** Bilgi vermek amacı ile kullanılır.

DNS Üzerinden Tehditler:

DNS 30 yılı aşkın süreden bu yana gelişmeyi sürdüren ve internetin çekirdek bileşenlerinden bir tanesidir. Bu sebeplerden dolayı saldırganlar ve kötücül yazılım yayınlayanların hedeflerinden bir tanesidir. DNS altyapsının çökmesi ya da saldırganlar tarafında kötüye kullanılması, büyük ölçekli hizmetlerin kesilmesi ve ya DNS üzerinden dışarıya veri sızdırma olaylarıyla sonuçlanabilir.
Cisco'nun 2014 Yıllındaki Güvenklik Raporuna göre inceleme yapılan ağların %96'sında çalınan sunuculara doğru trafik akışı olduğu görüldü ve %92'sinde ise herhangi bir içeriği bulunmayan sitelere doğru trafik olduğu tespit edildi. DNS üzerinde gerçekleşen saldırılar arasında en yaygın olanları aşağıda verilmiştir;

- **DNS tünelleme**
- **DoS ve DDoS saldırıları**
- **Ön bellek zehirlenmesi**
- **DNS yeniden yönlendirme (MITM) saldırıları**:
- **İleri Seviye Tehditler (APT)**

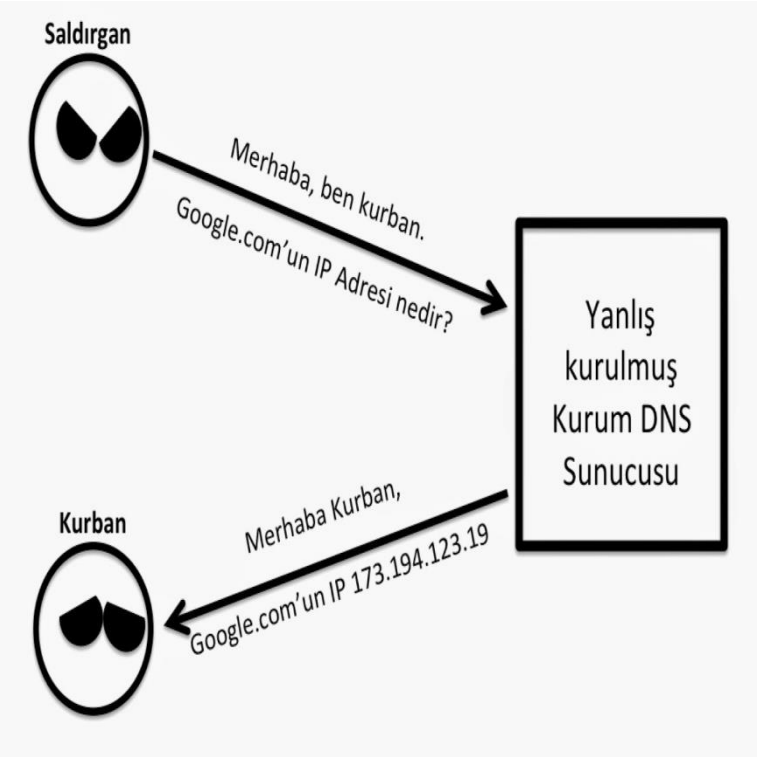
DNS Tehditleri

Saldırganlar DNS sunucularını kullanarak 4 temel saldırı türünü gerçekleştirebilir.

Bilgi Toplama: Özünde bir saldırı olmasa da hedef hakkında bilgi toplamak geçerli saldırıları belirlemek, planlamak ve yürütmek için önemlidir. Saldırganlar hedefin dışarıya bakan ağını nasıl düzenlediği ve yönettiğini DNS üzerinden bilgi toplayarak anlayabilir.

Hizmet dışı bırakma: Alanadı sunucusuna kapasitesinin çok üstünde talep gönderen saldırganlar hedef DNS sunucusunun iş görmez hale gelmesine neden olabilir.

Sahte kaynaktan talep gönderme: Yanlış ayarlanmış bir alanadı sunucusu başka bir hedefe hizmet dışı bırakma saldırısı düzenlenmek için kullanılabilir. Saldırganların hedef ağdan geliyor gibi düzenleyip göndereceği paketlere cevap veren alanadı sunucusu istemeden karşıdaki sunucuyu hizmet veremez hale getirebilir.



Kayıt yönlendirme: Kurumdan çıkan DNS taleplerini kendi kontrolündeki bir sunucuya yönlendiren saldırgan bu sayede kullanıcıları zararlı içerik barındıran bir siteye veya sosyal mühendislik saldırılarına uygun olarak hazırladığı başka bir siteye yönlendirebilir.

Yukarıda portlarını koruduğunuz bildiğimiz hedefin Alanadı Sunucusuna saldırgan gözüyle bakacak olursak aşağıdaki bilgileri elde edebildiğimizi görebiliriz.

DNS güvenliği için öneriler:

Alanadı sunucunuzun güvenliğini sağlamak için kullanabileceğiniz tek bir hap ne yazık ki yoktur. Bilgi güvenliğiyle ilgili diğer bütün konularda olduğu gibi gizlilik, bütünlük ve erişilebilirlik başlıkları ayrı olarak değerlendirilmelidir. Güvenlik seviyesini hızlıca arttırmanızı sağlayacak bazı öneriler şunlar olabilir;

DNS sunucunuz sadece kurumunuza hizmet etmelidir ve DNS sunucunuza sadece yetkisi olanlar erişebilmelidir.

DNS taleplerinin trafiğinin denetlenmesi gereklidir: Bu sayede hem DNS'e gelebilecek saldırıları fark eder hem de saldırganların DNS tüneli benzeri yöntemlerle kurum dışına veri kaçırdığını tespit edebilirsiniz.

DNS sunucularınız güncel tutulmalıdır: Diğer bütün sistemlerde olduğu gibi DNS yazılımları için güvenlik güncellemeleri ve yamaları yayınlanır, bunların zamanında kurulması çok önemlidir.

DNS sunucunuz üzerinde çalışan servisleri sınırlayın: DNS sunucunuz üzerinde FTP, HTTP, SMTP gibi hizmetleri kaldırmakta fayda var.

2. Kurumsal Ağ Güvenliği

Ağ Güvenliği Nedir:

Kurum içerisinde birden fazla bilgisayarların birbileri ile veri alışverişinde bulunabilmesine imkan veren bu alt yapıyı kurumsal ağ olarak adlandırıyoruz. Kurumsal ağlara bir çok farklı sebepten ötürü saldırılar düzenlenebilir. Saldırganlar bilgiye ulaşmada ağların zayıf noktalarını kullanarak yasadışı yollar denemektedirler. Sadece yapılan saldırılarla değil, aynı zamanda kullanıcıların(en zayıf halkaların) yaptıkları hatalar nedeniyle birçok kurum içi bilgi sızdırılabilir veya içeriği değiştirilebilir. Kurumlarda oluşan kayıplar maddi olabileceği gibi güven yitirme ve kurumu küçük düşürme gibi manevi zararlar da olabilmektedir. Bu tür durumlarla başa çıkabilmek için bazı kuralların belirlenmesi gerekmektedir. Bu kuralların sağlanmasına ağ güvenliği denir.

Ağ Güvenliği Nasıl Sağlanır:

- ***Fiziksel Güvenlik:***

Kurumun fiziksel güvenlik önlemlerinin sağlanmasıdır. Bu güvenlik önlemleri sadece kuruma izinsiz erişimler, personel kimlik kartı gibi konular düşünülmemelidir (bu konuyu sosyal mühendislik başlığı altında ele alacağız) . Bu başlık altında asıl ele aldığımız konu kurum içindeki cihazların sıcaklık,nem, toz, arıza, elektrik kesintileri gibi durumlara karşı önlem almaktır. Kurum içerisindeki ağda ki veri iletişimi sağlayan bu cihazlarda oluşacak bir hata veri akışının kesilmesine yol açabilir. Kurum içerisinde bu cihazlar için bir güvenlik protolü oluşturulması lazım.

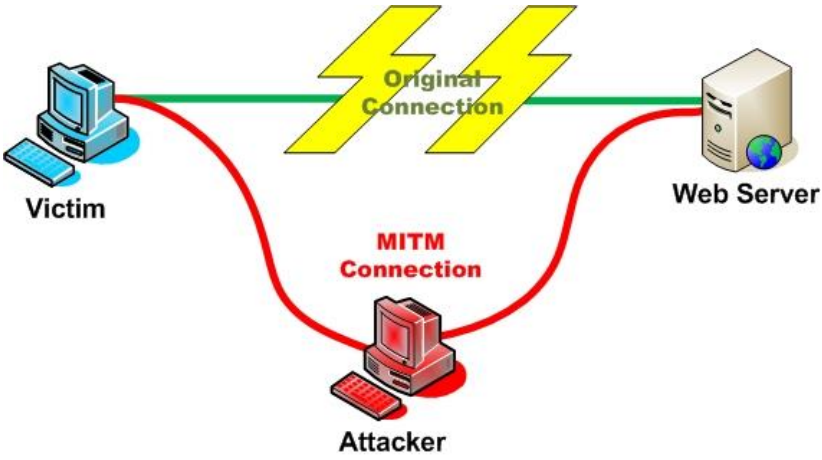
- ***Veri Gizliliği:***

Kurum içi önemli olabilecek verileri sınıflandırın (sosyal mühendislik kolu ilgili konu başlığında değinelecek) ve kurum içi gizli ve önemli olabilecek verileri dışardan müdahale ile ya

da ağ üzerinde akan verilerde arayan giren kişinlerin yetkisiz erişimelerine karşı engellendiğinden ve kurumda sadece yetkili kişinin erişimine açık olduğundan emin olun.

- ***Veri Bütünlüğü:***

Verilerin dışarıdan yapılabilecek olan müdahalerle silinmesi ya da değiştirilmesinin engellenmesidir.



Yukarıda verilen resimdeki gibi sunucu ile kurban arasında akan verinin arasına giren kurban verinin değiştirilmesine ve silinmesine sebep olur. Özellikler kurumsal ağlarda **Man in The Middle** gibi verilerin yetkisiz erişim sağlanıp, bütünlüğünün bozulmasına sebep olacak saldırılar için önlemler alınması lazım.

Şifreleme:

Kurumsal ağlarda , fiziksel güvenliğin kurum tarafından kontrol edilemeyen hatlar üzerinden akan verilerin özellikle gizlilik derecesi yüksek olan verilerin kriptolu bir şekilde yollanması verinizin bütünlüğüne gelebilecek olan saldırıları engelleyebilir.

Süreklilik:

Bilgi ve bilgi sistemlerinin sürekl hazır ve 7/24 hazır kesintisiz bir şekilde çalışıyor olması. Saldırganlar bir takım amaçlar ile yapacağı saldırlarla hizmette kesin yaratmaktır. Bu amaçla bir alt konu başlığında da ele aldığımız DoS/DDoS saldırılarının yanı sıra sürekliliği bozmak için elektrik sistemlerize kadar saldırılar düzenlenebilir. Dışarıdan müdahalerle oluşabilecek hizmet kesintilerine karşı bir kurum politikası oluşturulmalı.

Alınması Gereken Önlemler:

Kullanım politikaları: Ağ üzerinde izin verilen ve verilmeyen davranışların ve trafik türlerinin belirlenmesi gerekir. Örneğin Skype benzeri anlık mesajlaşma uygulamalarına izin verilip Torrent trafiği yasak olabilir. Buna ihtiyaçlarınıza olarak karar vermeniz gerekiyor.

Eposta ve iletişim faaliyetleri: E-posta eklerinin oluşturduğu tehditlerin ele alınması gerekiyor.

Antivirüs politikası: Zararlı yazılımların oluşturduğu tehditlere karşı.

Erişim politikaları: Ağ kaynaklarına kimin ve nasıl erişebileceğinin belirlenmesi.

Parola kuralları: Kullanıcıların güçlü parola seçmesive kurum genelinde parolaların ne sıklıkla değiştirilmesi gerektiği.

Şifreleme kuralları: Ağ üzerindeki verinin ve veri trafiğinin hangi durumlarda ve nasıl şifrelenmesi gerektiği.

Uzaktan erişim kuralları: Kurumsal ağ dışından kurum kaynaklarına kimlerin nasıl ulaşacağının belirlenmesi.

Ağ güvenliği sağlamak için aşağıdaki güvenlik önlemlerine ihtiyacınız var. Bunlar en temel ve “olmazsa olmaz” cihazlardır.

Güvenlik duvarı (firewall): Ağınıza izinsiz erişimleri engellemek için.

Sızma tespit ve engelleme sistemi (IPS/IDS): Ağınıza sızma girişimlerini tespit edip engellemek için.

Kablosuz ağ güvenliği: Kablosuz ağınıza kimlerin nasıl bağlanabileceğini denetlemek için.

Ağ güvenliği için yapılması gerekenler

Ağ üzerindeki cihazların envanterini çıkartmak: Ağ üzerinde hangi cihazların olduğu, bunların fiziksel olarak bulundukları yer gibi bilgilerin listelenmesi önemlidir.

Standart konfigürasyon: Ağ üzerindeki cihazların türlerine göre hazırlanmış standart konfigürasyonları olmalıdır. İlk aşamada zor gibi görünse de yönetim kolaylığı ve bütünlük açısından önemlidir.

Yönetim arabirimleri: Statik IP belirlenmeli ve mümkün olan en güvenli bağlantı yöntemi kullanılmalıdır. Telnet ve benzeri, kullanmadığınız diğer bağlantı yöntemlerini devre dışı bıraktığınızdan emin olun.

SNMP: SNMP kullanıyorsanız fabrika çıkışı ayarlarını mutlaka değiştirin, kullanmıyorsanız SNMP bağlantısını kapatın.

Yedekleme: Cihaz konfigürasyon dosyalarını düzenli olarak yedekleyin.

Yazılım: Cihazlarınızın yazılımı olduğunu unutmamak ve yazılımları düzenli olarak güncellemek çok önemlidir.

VLAN: Sunucu, istemci yedek alma ve benzeri gruplara göre trafik türlerini ayırmak için VLAN ayrımı yapılmalıdır.

Kullanılmayan portlar: Cihazlar üzerinde kullanılmayan portların aktif olmadığından emin olun. Ağ üzerinde hub benzeri cihazların kullanımını sınırlandırın.

İstemci ve Sunucu güvenliği

Envanter: Ağınızdaki istemcilerin ve sunucuların envanterinin çıkartılması, hangi bilgisayarın nerede, hangi işletim sistemiyle ve kimin tarafından kullanıldığını listeleyin.

Ağ ayarları: İstemcilerin ve sunucuların hangi ağlara, hangi VLAN'lara ve nasıl bağlanacağının belli olması önemlidir.

Yama yönetimi: Yazılım üreticileri tarafından yayınlanan güncellemelerin ve yamaların düzenli olarak yüklenmesi çok önemlidir.

Antivirüs: Hem istemcileri hem de sunucular üzerinde antivirüs kullanılması çok önemlidir.

Host-based IPS: Antivirüs üreticilerinin bir kısmı istemci seviyesinde sızma tespit ve engelleme sistemini antivirüs çözümlerine entegre etmiştir. Bunlardan faydalanabileceğiniz gibi başka yöntemlerle de istemcilerin ve sunucuların gerekmedikçe kendi aralarında iletişim kurmasını sınırlandırmalısınız.

Admin kullanıcısı: Sızma testleri sırasında "büyük ikramiye" olarak görebileceğimiz ve ağ genelinde bütün (veya birçok) makinede geçerli olabilecek bir admin kullanıcısı kullanmayın. Her istemci ve sunucu için farklı bir admin kullanıcısı ve parolası oluşturun. İdeal olarak hiç bir kullanıcı kendi makinesinde admin yetkili kullanıcı hesabı kullanmamalıdır.

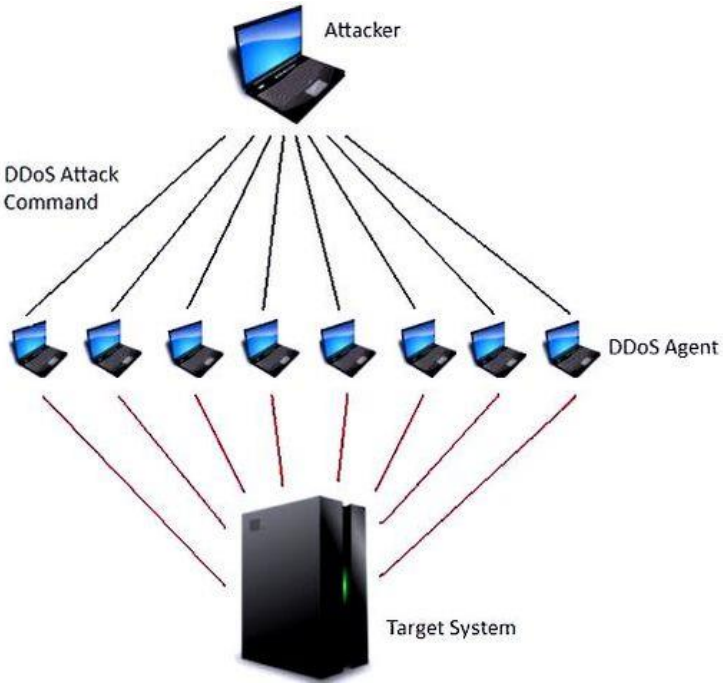
Yedekleyin: Düzenli olarak yedekleyin.

3. DoS/DDoS Saldırıları ve Korunma Yolları

DoS/DDoS Nedir

DoS: Temel olarak hedeflediği sistemin ya da sunucunun işleyişini engellemeye yönelik olan **DoS** saldırıları web uygulamarından ziyade sunucuları hedef alır. Bu saldırılarda hedef sisteme paket gönderme ve ani trafik doldurma gibi yöntemler ile sisteme karmaşık paketler yollar ve yanıt bekler. Çok büyük oranda iletilen bu paketlere sunucu cevap veremez ve bu durum sunucunun çalışmamasına neden olur. Bu saldırı sırasında gönderilen paketler işlemci, hafıza ve bant genişliği gibi sistem kaynaklarını tüketir. Bu saldırıların amacı yayın akışını kesmek, belirli bir süre yayını engellemek ya da sunucuyu yorma, yıpratma ve zarar vermektir.

DDoS: Bu saldırının DoS saldırılarından farkı birden fazla noktadan tek bir hedefe yapılıyor olmasıdır.


Attacker
DDoS Attack
Command
DDoS Agent
Target System

Bazı Saldırı Çeşitleri

Arabellek Aşımı Saldırıları:

DOS saldırılarının en yaygın çeşitidir. Arabellek aşımı saldırıları; bir internet sitesine, sitenin programcısının gelmesinin beklediği ve bu amaçla veri akışı için planladığı arabellek değerinin karşılayamayacağı kadar çok trafik yollanması sonucu oluşur.

Smurf Saldırıları:

Smurf Saldırılarında, saldırgan kurban olarak seçtigi bilgisayardan ping isteğinde bulunur. Ancak ping paketi, hedef makinenin IP'sinden geliyormuş gibi görünecek şekilde hazırlanmıştır. Bu durumda ağ üzerindeki bütün makineler, hedef makineye ping atar. Hedef makine bu trafiği karşılayamaz ve bağlantı kesilir.

Fraggle Saldırıları:

Bu saldırı tipinin smurf saldırılarından farkı, Smurf saldırıları TCP alt yapısını kullanıyorken Fraggle saldırıları UDP alt yapısını kullanır.

SYN Saldırıları:

Bu saldırı biçiminde bir saldırgan sistemin yasal trafiğini isteklere cevap veremeyecek duruma getirmek için yeterli sunucu kaynaklarını tüketme girişiminde bulunarak, hedef alınan sisteme ardışık SYN istekleri (SYN requests) gönderir.

Teardrop Saldırıları:

Bir bilgisayara internet üzerinden gelen paketler, bilgisayarda bölünerek aktarılır. Paket verilere ayrıştırılırken, pakette bulunan ofsetler kullanılır. Bu ofset bilgilerinin çakışmaması gerekmektedir. Teardrop saldırılarında, paketi gönderen saldırgan, pakete üst üste gelecek ofsetler ekler. Paketi alan

bilgisayar, böyle bir durumu kontrol edebilecek mekanizmaya sahip değilse, sistem çöker.[1]

Servislere Aşırı Yüklenme:

Bu saldırı tipi belirli kullanıcı ve servisleri hizmet dışı bırakmak için kullanılır. Saldırgan özel port ve kullanıcıya bir çok ICMP paketi gönderir.

DDoS Saldırılarına Karşı Alınabilecek Tedbirler

Sakin olun

Bu saldırı türüne karşı %100 etkili bir çözüm maalesef yok. Bu nedenle saldırı altındayken alım kararı vermeyin, ağınıza yeni cihazlar eklemeyin. Sadece kuruluşunuzu hedef alan bir DDoS saldırısı olması durumunda internet servis sağlayıcınızla görüşüp bant genişliğinizi arttırmayı veya servis sağlayıcınızdan DDoS saldırılarına karşı koruma hizmeti talep edebilirsiniz.

Bilgilendirin

DDoS saldırıları kuruluşunuzun müşteri veya vatandaşların ulaştığı kaynaklarını devre dışı bıraktığı için sorun üst yönetimi yakından ilgilendirmektedir. Bu nedenle yönetime konuyla ilgili, teknik ayrıntılara girmekten mümkün olduğunca kaçınarak, bilgi verilmesi çok önemlidir.

Mevcut durum

Envanterinizde bulunan firewall, vb. cihazların, bu iş için üretilmemiş olmalarına rağmen, DDoS saldırılarına karşı etkili olabilecek bazı özellikleri olabilir (rate limit, SYN cookie, vb.) bunları devreye alabilirsiniz. Özellikle eski cihazların kapasitesinin internet bant genişliğinizden az olabileceğini

unutmayın. Cihaz özelliklerinin kontrol edilmesinde fayda olacaktır.

Aktif savunma

DDoS saldırılarını engellemek mümkün olmasa da etkilerinin azaltılması için bazı tedbirler alınabilir. Bu tedbirler arasında etkili olabilecekler;

- Saldırının geldiği IP adresini kullanan başka servisler (VoIP, mail, vb.) varsa bunları farklı IP adreslerine ve, mümkünse, farklı internet bağlantılarına/yerlere, taşıyarak internet sayfanızı hedef alan bir saldırıdan etkilenmemelerini sağlayabilirsiniz.
- DNS TTL sürelerinizi azaltın. DNS (alanadı sunucusu) kayıtlarınızın güncellenme sürelerini kısaltarak, IP adresi ve alanadı gibi konularda yapacağınız değişikliklerin daha hızlı devreye girmesini sağlayabilirsiniz.
- Gelen saldırı paketlerinin ortak özelliklerini tespit etmeye çalışın (zaman damgası olmaması, kaynak port, başlık bilgisi, vb.) ve ağınıza bu paketlerin erişmesini engelleyin (firewall kuralı yazılması, vb. tedbirler düşünülebilir)
- Hedef alınan IP adresini DNS kayıtlarınızdan çıkartın
- Kullanılmayan IP bloklarını engelleyin (çalışmadığınız ülkeler, 192.168.0.0/16 veya 10.0.0.0/8 gibi internette olmaması gereken IP adresi blokları vb.)
- Dışarıya açık ve işiniz açısından kritik olmayan servisleri (ssh, rdp, vb.) kapatın
- DDoS saldırısından faydalanarak port taraması veya daha önemli bir saldır da yapılıyor olabilir. Bunu anlamak için kaynak IP adresi bazında bir analiz yapılarak birden fazla ve farklı paket gönderen IP adresleri çıkartılmalıdır

Kayıtlar

Saldırının kayıt altına alınması hem saldırı sırasında doğru kararları verebilmek, hem de saldırı sonrasında yapılacak

analizlerden doğru sonuçların çıkarılabilmesi çok önemlidir. Ağ girişinde bulunan bir cihazdan Wireshark benzeri ücretsiz bir yazılımla saldırı trafiği kaydedilebilir.

4. Web Uygulamaları Güvenliği

Web Uygulamalarına Yönelik Saldırılar:

Aşağıda OWASP tarafından yayınlanan belgede, 2010 ve 2013 yılı üzerinden web uygulamaları üzerinde en çok görülen 10 zafiyeti listelemiştir.

OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

A1-Injection:

Uygulamanın arka planında çalışan bir veritabanı sorgusu ya da işletim sistemi komutuna, kullanıcıdan alınan ve 'güvenilmeyen veri' olarak tabir ettiğimiz veriler, herhangi bir doğrulama ve filtreleme işleminden geçmeden geliyorsa SQL Injection, Command Injection ya da LDAP Injection gibi zafiyetler doğabilir. Saldırganlar da uygulamada ki bu zafiyetleri kullanarak uygulama sunucusu ya da veritabanı

sunucusunda komutlar çalıştırarak yetkilendirilmedikleri halde verilere erişim sağlayabilirler.

A2 - Broken Authentication and Session Management:

Kimlik doğrulama ve oturum yönetimi ile ilgili süreç ve fonksiyonların yanlış implementasyonu sonucu saldırganların, kullanıcıların kimlik bilgileri, şifreleri, oturum anahtarları vs gibi değerlerine ulaşması mümkündür.

A3 - Cross Site Scripting (XSS):

Web uygulamasında, kullanıcıdan girdi beklenen noktalarda, kullanıcıdan gelen girdiyi kontrol etmesi gereken fonksiyonların var olmaması ya da doğru implemente edilmemesi nedeniyle XSS açıklıkları doğabilir. Saldırganlar da bu zafiyeti sömürüp hedef kullanıcıların internet tarayıcıları üzerinde JavaScript kodları çalıştırarak oturum bilgilerini alabilir ya da zararlı yazılım içeren başka web sitelerine yönlendirebilirler.

A4 - Insecure Direct Object References:

Özellikle query string ile URL üzerinden taşınan değerler için tip, doğruluk ve benzeri gibi kontrollerin yapılmaması nedeniyle saldırganlar bu değerleri manipüle ederek uygulamaya zarar verebilir.

A5 - Security Misconfiguration:

Uygulama sunucusu, uygulamanın geliştirildiği uygulama çatısı (framework), web sunucusu, veritabanı sunucusu ve benzeri platformların güvenlik gerekliliklerinin yerine getirilmemesi nedeniyle ortaya çıkan zafiyetlerdir.

A8 - Cross Site Request Forgery:

CSRF atakları sayesinde saldırganlar tarafından hazırlanan HTTP istekleri, hedef kullanıcının internet tarayıcısı aracılığıyla uygulamaya gönderilecek ve bu isteklere otomatik olarak ilgili

kullanıcının oturum bilgileri dahil edileceğinden uygulama istekleri meşru olarak değerlendirecek ve saldırgan istediği sonuca ulaşabilecektir.

A-10 - Unvalidated Redirects and Forwards:

Web uygulamaları sıklıkla kullanıcıları başka sitelere ya da mevcut uygulama üzerinde başka sayfalara yönlendirmektedirler. Bu yönlendirme işlemleri, herhangi bir doğrulama sürecinden geçmiyorsa, saldırganlar bu yönlendirme süreçlerini manipüle ederek hedef kullanıcıları zararlı yazılım içeren web sitelerine yönlendirebilmektedirler.

Alınabilecek Önlemler:

- Uygulama ile son kullanıcı arasındaki kullanıcı adı, parola, kredi kartı no, adres gibi hassas veriler HTTPS protokolü üzerinden aktarılmalıdır.
- Kullanılan parolalar ve parolamı unuttum kontrol soru cevapları gibi diğer hassas veriler açıkmetin olarak saklanmamalıdır.
- SQL enjeksiyonuna karşı prepared statement/parameterized query/bind variables/pozitif veri kontrolü yöntemlerinden biri veya bir kaçı kullanılmalıdır.
- Kullanıcıdan gelen tüm girdilere sunucu tarafında pozitif veri kontrolü uygulanmalıdır.
- Kullanıcıdan gelen verilerin işletim sistemi komut satırına girmeden kontrol edilmesi ve düzgünleştirme işleminden (escape) geçirilmesi gerekmektedir.
- Kullanıcıdan gelen ve dosya erişim işlemlerinde kullanılan girdiler normalizasyon işlemine tabi tutulmalıdır.
- GET veya POST isteklerindeki HTTP parametreleri değiştirilerek üçüncü şahısların bilgilerine yetkisiz olarak erişilmemelidir.

- SOAP, Restful, XML-RPC gibi teknolojilerle geliştirilmiş web servislerine erişimlerde kimlik doğrulama kontrolü uygulanmalıdır.
- Kullanıcıdan veri alarak LDAP'a bağlanan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri LDAP düzgünleştirme işleminden (escape) geçirmelidirler.
- Güvensiz kaynaklardan veri alarak XPath sorguları yapan uygulamalar, gerekli girdi kontrollerini gerçekleştirmeli ve bu girdileri XPath düzgünleştirme işleminden (escape) geçirmelidirler.
- Karşıdan dosya yükleme işlemlerinde yüklenilen dosya üzerinde isim, boyut, tip ve içerik kontrolü yapılmalıdır.
- DoS saldırısı barındıracak veya şifre deneme-yanılma gibi kaba kuvvet saldırılarına açık tüm formlara CAPTHCA veya farklı anti-otomasyon güvenlik kontrolleri uygulanmalıdır.
- Güvenli web trafiği için (SSL) güçlü şifreleme algoritmaları kullanılmalıdır, güçsüz algoritmalar inaktif hale getirilmelidir.
- Uygulama çatısı/veritabanı/uygulama sunucusu/web sunucusu gibi kullanılan yazılımların güvenlik yamaları en üst seviyede olmalıdır.
- Kritik işlemlerde CSRF saldırılarına karşı güvenlik önlemleri alınmalıdır.
- Uygulama üzerinden yapılan hassas işlemler hem uygulama seviyesinde hem de sunucu seviyesinde kayıt altına alınmalıdır.
- Uygulamaların üzerinde koştukları sunucuları, servis verdikleri dizinlerin içeriklerini listelememelidir.

- Güvensiz kaynaklardan veri alarak aritimetik işlem yapan uygulamalar, gerekli tam sayı üst sınır ve alt sınır kontrollerini gerçekleştirmelidirler.
- Uygulamayı çalıştıran sistem kullanıcısının, hizmet verilen dizin dışındaki yetkileri kaldırılmalıdır
- Veritabanı kullanıcısının sadece uygulamanın kullandığı veritabanı kaynaklarına erişim hakkı olmalıdır.
- Hassas bilgiler içeren web sayfalarının tarayıcılarda belleğe alınmaması için autocomplete, cache-control, pragma gibi gerekli HTTP/HTML başlıkları kullanılmalıdır.
- Uygulama domain isimlerine ait hassas bilgilerin google/bing gibi arama motorları tarafından indexlenmediği kontrol edilmelidir.
- . Parola unuttum formları, gizli soru, doğum tarihi gibi birden fazla parametre ile desteklenmelidir .
- Uygulamada oluşan hatalar veya uygulama sunucu varsayılı hata mesajları kullanıcıya detaylı olarak gösterilmemelidir.
- Kullanılan COOKIE değerleri için HTTPOnly parametresinin tanımlı olduğu kontrol edilmelidir.
- Flash uygulamalarında crossdomain.xml yapılandırma dosyası uygulanan politikanın güvenli olduğu kontrol edilmelidir.

5. Web Servisleri Güvenliği

Web Servisi Nedir:

Web servis, web üzerinden HTTP protokolü üzerinden XML ve JSON standartlarını kullanıp veri gönderip alarak iki uzak cihaz arasında iletişimi sağlayan haberleşme yöntemidir. Web'in gelişmesi sebebi ile farklı platformlar arasında haberleşme ihtiyacı doğmuştur. Web servisler veri alış

verişinde standartlarının olması sebebi ile platform bağımsızdır. Web servisleri verileri XML ile tutup SOAP kullanarak taşır. Web servislerinin yapısı itibariyle farklı serverlardaki farklı platformlar haberleşebilir.

Web Servisleri Güvenliği:

OWASP tarafından yayınlanan web servisleri güvenliği önerileri aşağıda verilmiştir.

İletimde Gizlilik:

Web Servislerinde bilgi iletiminin gizliliği, bilgi alış-verişi esnasında gidip gelen bilgilerin dinlenmesine (eavesdropping) ve araya girme (man in the middle) saldırılarına karşı sunucu ve istemci arasındaki web servislerin güvenli iletişimini sağlar.

Sunucu Tarafında Kimlik Doğrulaması:

Kural: Servis sağlayıcı, servis kullanıcılarının güvenliğini sağlamak için SSL/TLS güvenli protokollerini kullanmak zorundadır.

Servis kullanıcısı güvenli sertifika sağlayıcısı tarafından tescillenmiş sunucu sertifikasını doğrulamalıdır, öyle ki bu sertifikanın zamanı dolmamış, iptal edilmemiş, yürürlükten kaldırılmamış olması, servisin alan / ilgi alanı ismi (domain name) ile eşleştiğini doğrulamalıdır ve sunucu kendisinde bu açık anahtar sertifikasına dair gizli anahtarın olduğunu ispatlamalıdır.(Tamamen doğru ve dürüst bir biçimde bazı şeyleri dijital olarak imzalayarak veya başarılı bir şekilde açık

anahtar ile eşleşmiş bazı dataları deşifre ederek bunu başarabilir.)

Kullanıcı Tarafında Kimlik Doğrulaması:

Kullanıcı doğrulaması, servise bağlanmak isteyen sistemin / sistemlerin veya kullanıcıların kimliklerini doğrular. Böyle bir doğrulama işlemi, web servisini içeren mekanizmanın görevidir.

Kural: Eğer kullanılıyorsa, basit kimlik doğrulaması SSL üzerinden yütürülmek zorundadır. Fakat basit kimlik doğrulaması önerilmemektedir.

Kural: SSL kullanılarak gerçekleştirilen istemci sertifika doğrulaması, tavsiye edilen güçlü bir kimlik doğrulama şeklidir.

İletimin Kodlanması:

SOAP kodlama teknikleri, bilgileri yazılımdaki objelerden XML formatına ve XML formatından objelere taşımadır.

Kural: Bu sebepledir ki, sunucu ve istemci için her iki tarafında aynı kodlama tekniğinin kullanılmasına zorlanmalıdır.

Mesaj Bütünlüğü:

İletimde olan verilerin bütünlüğü SSL / TLS tarafından kolayca sağlanabilir. Açık anahtar şifreleme metodu kullanılırken, şifreleme güvenliği garanti eder fakat şifreleme esnasında alıcının açık anahtarı “açık” olduğundan dolayı mesajların bütünlüğünün doğruluklarını garanti etmez. Aynı sebepten dolayı, şifreleme gönderenin kimliğini de garanti etmez.

Kural: XML datalar da, mesajların bütünlüğünü sağlamak için göndericinin gizli anahtarını kullanarak XML elektronik imzalarını kullanın. Bu imzalama işleminin doğrulanması alıcı tarafından gönderenin elektronik sertifikası kullanılarak yapılır. (Açık anahtar metodolojisi.)

Mesaj Gizliliği:

Veri elemanları, kaba güç saldırılarını engellenmesi veya kaba güç saldırılarına karşı güvenli olabilmeleri ve gizli kalabilmeleri için yeterli uzunlukta ki anahtar ile güçlü bir şekilde şifrelenmelidir.

Kural: Hassas verileri içeren mesajlar güçlü bir şekilde şifrelenmelidir. Bu iletişimin şifrelenmesi veya mesajların şifrelenmesi şeklinde olabilir.

Kural: Hassas veriler içeren mesajlar güçlü bir şifreleme yöntemi ile alındı bilgisinden sonra dahi şifreli olarak kalmalıdır. Sadece iletim süresince değil.

Yetkilendirme:

Web Servisleri, web uygulamalarının kullandığı kullanıcıları yetkilendirme yoluyla, istemcilerini yetkilendirmeye ihtiyaç duyarlar. Web servisi, istemcinin talep edilen veri / veriler için kesin bir işi yapacak şekilde yetkilendirildiğinden emin olmalıdır.

Kural: Web servisi, istemci tarafından gönderilen sorguda ki metoda erişim izni olup olmadığını göz önüne alarak

istemcisini yetkilendirmelidir. Takip eden yetkilendirme de, web servisi talep edilen isteğin gerekli kaynaklara ulaşıp ulaşamayacağına dair ayrıcalıklarını/özel izinlerini kontrol etmelidir. Bu işlem her istek için yapılmalıdır.

Kural: Web servis uygulaması içinde yönetim ve idarecilik işlevselliklerinin web servisi uygulamasının yöneticilerine yönelik olarak kısıtlandırıldığından emin olunmalıdır. İdeal olan, web servisini yöneten herhangi bir yönetici işlevselliğinin/işlevselliklerinin web servisi uygulamasından tamamen farklı olmalıdır. Böylece normal kullanıcılarla yetkili kullanıcılar ve hassas işlevsellikler birbirinden tamamen ayrılmalıdır.

Şematik Doğrulama:

Şematik doğrulama, kısıtlamaları ve kodlama imlalarını şema içerisinde tanımlanan şekilde olmasına zorlar.

Kural: Web Servisleri, ilgili XML şema tanımına karşı SOAP taşıma yüklerini doğrulamak zorundadırlar.

Kural: SOAP web servisi için tanımlanan XML şeması, minimum olarak, her parametre için maksimum uzunluk ve web servise girdi ve çıktı olacak karakter setlerini tanımlamalıdır.

Kural: SOAP web servisi için tanımlanan XML şeması, tüm sabit biçemler için güçlü (ideal olarak beyaz liste) doğrulama

paterni tanımlamalıdır. (Misal olarak: zip kodları, telefon numaraları, liste değerleri vs.)

İçerik Doğrulaması:

Kural: Herhangi bir web uygulamasında olduğu gibi web servisleri de aldıkları girdileri kullanmadan önce doğrulamaya ihtiyaç duyarlar. XML girdisi için içerik doğrulaması altta ki maddeleri içermelidir: **-** Kusurlu XML girdilerine karşı doğrulama, **-** XML bombardıman saldırılarına karşı doğrulama, **-** Güçlü bir beyaz liste kullanarak girdilerin doğrulanması, **-**Dışarıdan girdi saldırılarına karşı doğrulama.

Çıktı Kodlaması:

Web servisleri, istemci tarafına gönderdikleri çıktı verilerinin komutlar şeklinde değil, datalar şeklinde kodlandığından emin olmak durumundadırlar. Bu, istemcinin gelen çıktı verilerini HTML sayfalarını işlemek için direkt veya dolaylı olarak AJAX nesnelerini kullanması durumunda çok daha önemli bir duruma gelmektedir.

Kural: Çıktıların kodlanmasında ki her kural için XSS önleme veri dosyasına bakılmalıdır.

Virüs Koruması:

SOAP, SOAP mesajlarına dosya ve döküman ekleme kabiliyeti verir. Buda, bilgisayar korsanlarına bu SOAP mesajlarına virüsleri ve kötü amaçlı yazılımları ekleme fırsatı verir.

Kural: Kullanılan virüs tarama teknolojisi sistem de mevcut ve sıralı şekilde sisteme entegre edilmiş olmalıdır.Bu sayede dosyalar veya eklenmiş dökümanlar diske kayıt edilmeden önce kontrolden geçirilebilir.

Kural: Kullanılan virüs tarama teknolojisinin güncel olduğundan ve her zaman en son virüs tanımlamalarını aldığından emin olunmalıdır.

Mesaj Kapasitesi:

Web Servisleri, web uygulamaları gibi otomatik gönderilen ve geniş kapasiteye sahip binlerce SOAP mesajı tarafından servis dışı bırakma saldırılarının hedefi olabilirler. Bu olay, servisi gelen isteklere cevap verme konusunda yetersiz bırakabilir veya tamamen servis dışı kalmasına neden olabilir.

Kural: SOAP mesajlarının kapasiteleri uygun bir kapasiteyle sınırlandırılmalıdır. Kapasite arttıkça veya sınırlandırılmadıkça servis dışı bırakma saldırılarının başarılı olma oranları da yükselir.

Erişilebilirlik:

İşlem hacmi, belirli bir süre içerisinde yerine getirilmiş web servis isteklerinin sayısıdır.

Kural: Yapılandırma/konfigürasyon, servis dışı bırakma durumlarını engelleyecek şekilde maksimum mesaj hacmine cevap verecek biçimde olmalıdır.

XML Servis Dışı Bırakma Koruması:

Web Servislere karşı belki de en çok bilinen ve yapılan saldırı şekli servis dışı bırakma saldırılarıdır. Bu sebeptendir ki web servisleri aşağıdaki doğrulamaları sağlamak zorundadırlar:

Kural: Yinelemeli veri taşıma yüküne karşı doğrulama,

Kural: Büyük veri yüklerine karşı doğrulama,

Kural: XML birim genişlemelerine karşı koruma,

Kural: Çok uzun element isimlendirmelerine karşı doğrulama. Eğer geliştirici, SOAP tabanlı web servisleri üzerinde çalışıyor ise, element isimleri SOAP eylemleridir.

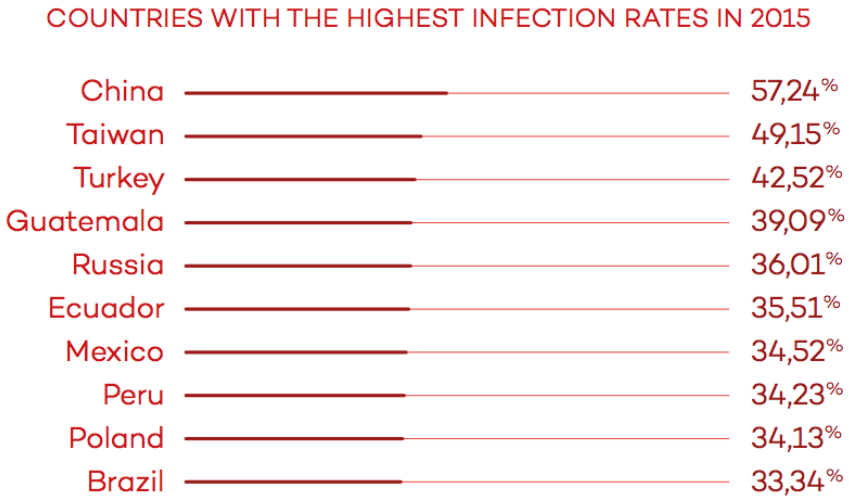
Bu koruma yöntemi, XML derleyicisi / şeması tarafından sağlanmalıdır. Doğrulamak için, derleyicinin bu tarz saldırılara karşı dayanıklı olduğuna dair testler yapılmalıdır.

6. Zararlı Yazılımlar

Zararlı Yazılım Nedir:

Zararlı yazılımlar kurumlar için, bilgi güvenliğini sağlamada en önemli tehditlerden biridir. APT (gelişmiş sürekli tehdit) saldırıları olarak bilinen ve günümüzde farkedilmesi zor ve karmaşık olan siber saldırılarda da kullanılan en önemli silahlardandır. Zararlı yazılımlar para kazanmak, sistemleri çalışmaz hale getirmek ve bilgiyi çalmaktan tutunda günümüzün en teknlojik ve en güçlü silahlarının erişemediği, imha edemediği yerlere ulaşan ve belki de tamamen kontrolü altına alan tehdittir. (Bkz: Stuxnet virüsü). Zararlı yazılımlar kurumda bulaştığı bir bilgisayar sistemi üzerinden ağ üzerindeki diğer makinelerede zarara yol açabilir. Aşağıda

verilen istatistik, bir güvenlik firması tarafından yayınlanan 2015 zararl ı yazılım raporu en çok zararlı yazılım görülen 10 ülke sıralamasını vermektedir.



Zaralı Yazılım Türleri:

Virüs:

Virüsler sistemlere bulaşmak için imaj,ses,video vb. dosyalara tutunan ve kendini çoğaltabilen zararlı yazılımlardır. Bilgisayar virüsleri, insan metabolizmasına bulaşan virüsler gibi bulaştıktan sonra diğer hücrelere,dosyalara da yayılırlar. Tutunduğu dosyanın (konak hücre) nin çalıştırılması ile sistemde aktif hale gelirler. Sistemlere sızmak için kullanıldıkları yöntemlere göre ;

- Dosya virüsleri
- Önyükleme kesimi virüsleri
- Makro virüsleri

- Komut dosyası virüsleri

Şeklinde gruplandırılır.

Solucanlar (Worm):

Solucanlar virüslere göre daha karmaşık yapıya sahip olan zararlı yazılımlardır. Bulaştıkları sistemlerde kopyalanması ve yayılması için çalıştırılmaya ihtiyaç duymazlar. Virüslerin aksine herhangi bir dosyaya tutunma ihtiyacı duymazlar ve bulundukları sistemde ki bir açık vasıtası ile bulaşırlar. Bulaşılan ağ üzerinde aşırı kaynak tüketimi yapması sebebi ile bazı işlemlerin sonlandırılmasına sebep olabilirler. Saldırganlar tarafından, bir backdoor (arka kapı) açması ve sisteminize bu şekilde erişebilmesi amacı ile kullanılırlar. Solucanlar bir sisteme sızmak için;

- E-posta eki olarak gönderilen dosyalar
- Web veya FTP kaynağı bağlantısı ile
- ICQ veya IRC mesajında gönderilen bağlantılar ile
- P2P (eşdüzeyler arası) dosya paylaşım ağları üzerinden
- Bazı solucanlar, ağ paketleri olarak yayılır. Bunlar bilgisayar belleğine doğrudan girer ve ardından solucan kodu etkinleştirilir.

yöntemlerini kullanırlar.

Truva Atı (Trojan):

Truva atı bilgisayar sistemlerine bulaşmak için zararsız gibi görülen bir programın çalıştırılması vasıtasıyla sisteme bulaşırlar. Truva atı bulaştığı sistemde virüsler gibi kendisini kopyalamaz ya da çoğaltmaz. Truva atı bilgisayarınızda oluşturduğu güvenlik açığı sebebi ile saldırganın sisteminize,dosylarınıza ve bilgilerinize erişme imkanı tanır. 7 tür truva atı vardır;

- Uzaktan Erişim
- E-posta Gönderme
- Veri yıkımı
- Proxy Truva(zararlı bulaşmış sistemi saklama)
- Ftp Truva (zararlı bilgisayardan dosya ekleme ya da kopyalama)
- Güvenlik yazılımını devre dışı bırakma
- Hizmetin reddi servis saldırıları (Dos Saldırıları)
- URL truva (zararlı bulaşmış bilgisayarı sadece pahali bir telefon hattı üzerinden internete bağlama)

Casus Yazılımlar (Spyware):

Casus yazılımlar kullanıcın izni de bilgisi de olmadan sisteme yüklenen, kullanıcıya ve sisteme ait bilgileri toplayıp saldırgana yollayan zararlı yazılımlardır.

Alınabilecek Önlemler:

- Lisanslı yazılım kullanın ve güncel tutun.
- Ağınıza izinsiz erişimleri engellemek için güvenlik duvarı kullanın.
- Kurum içinde bir güvenlik politikası oluşturun.
- İşletim sisteminizin güvenlik güncellemelerini mutlaka yapın.
- Web tarayıcılarınızın güvenli hale getirin.
- Kullanmadığınız yazılımları kaldırın.
- Personel farkındalığını arttırın.
- Mutlaka bir antivirüs programı kullanın.
- İnternet üzeriden reklam, link kısaltmları vb. gibi karşınıza çıkan ekranlara dikkat edin.
- Zararlı yazılım analizini sanal makine üzerinden yapın.
- Saldırı tespit sistemleri kullanın.

- Sisteminizi sıklıkla zararlı yazılımlara karşı tarayın.
- Usb,cd,dvd vb. gibi taşıma ortamlarının sisteminize zararlı yazılım bulaşırma ihtimalini unutmayın.
- Reklamlardaki, beklenmedik açılır pencerelerdeki veya uyarılardaki, güvenilir görünmeyen web sitelerindeki veya casus yazılımları ya da virüsleri temizlemeye yönelik tekliflerdeki **Kabul, Tamam** veya **Kabul ediyorum**şeklindeki öğeleri tıklamaktan kaçının.
- Önemli olan dosyalarınızı (veritabanı, ticari bilgiler vb.) mutlaka şifreleyin.
- E-posta eklerini açmadan önce dikkatli olun.
- Ağınızın güvenlik yapılandırmasını mutlaka yapın.
- Fiziksel olarak bilgisayarınızın güvenliğini her zaman sağlayın.

7. Ransomware Saldırıları:

Ransomware Nedir:

Ransomware(fidye yazılımları), bulaştığı sistemlerde ki bir takım verileri güçlü şifreleme algoritmaları ile kriptolayıp, bu verilerin kurtarılması karşılığında kurbandan para talep eden zararlı yazılımlardır.

Verilerin Rehin Alınması:

Siber suçlular, hedef aldıkları kişilerin veya kurumların çok önemli sayılabilecek verilerini (muhasebe kayıtları, veri tabanı, ticari bilgileler, kişisel dosyalar vb.) şifreleyerek, bu verilerin kurtarılabilmesi karşılığında para talep ederler. Bu saldırılarda siber suçlular, hedef aldıkları sistemin kullandığı FTP,telnet,smtp ve pop3 gibi protokollere brute force saldırıları düzenleyerek hedef sisteme sızabilir, hedef sistemdeki bir güvenlik açığını kullanarak uzak masaüstü bağlantısı ile sisteminize sızma işlemini gerçekleştirebilir,sahte e-posta ekleri vasıtasıyla sisteminizde bir backdoor oluşturabilir ya da bu ekler vasıtasıyla sisteminize cryptolockler vb. zararlı yazılımlar bulaştırabilirler. Hedef sisteme sızmayı başaran saldırgan verileri manuel olarak yada cryptolocker benzeri zararlı yazılım vasıtasıyla şifreledikten sonra, verilerin orjinalini silip, şifrelenmiş bir kopyasını bırakıyor. Dosyalar şifrelendikten sonra ise parayı ödemek dışında yapılabilecek

herhangi birşey kalmıyor (Parayı ödemek dosyalarınızı kurtaramayabilir!!!).

Alınabilecek Tedbiler:

- Verilerinizi düzenli olarak yedekleyin.
- Lisanslı yazılım kullanın ve güncel tutun.
- Personel farkındalığını arttırın.
- Mutlaka bir antivirüs kullanın.
- Önemli olan dosyalarınızı (veritabanı, ticari bilgiler vb.) mutlaka şifreleyin.
- E-posta eklerini açmadan önce dikkatli olun.
- Ağınızın güvenlik yapılandırmasını mutlaka yapın.
- Fiziksel olarak bilgisayarınızın güvenliğini her zaman sağlayın.
- İşletim sisteminizin güvenlik güncellemelerini düzenli olarak yapın.

Yukarıdaki önlemler dışında RDP, SSH, telnet vb. gibi uzak bağlantılarınızı mutlaka güvenli hale getirin.

8. Sosyal Mühendislik Saldırıları:

Sosyal Mühendislik Nedir:

Sosyal mühendislik, teknolojiyi kullanarak ya da teknolojiyi kullanmadan insanlardan bilgi edinme sanatıdır. İnsanları kandırarak bilgi edinme ya da menfaat sağlama düşüncesi yeni değildir. Binlerce yıldır varlığını sürdürmektedir ve insanlar var oldukça da varlığını sürdüreceklerdir. Bu tip saldırılar günümüzde pek çok alanda yaygın olarak kullanılmaktadır.

Kurumlar sistem güvenliğini sağlamak, kurum içi ağlarını ve sunucularını güvenilir ve sürekli çalışır halde tutmak için tedbir olarak en son teknolojiyle donatır. Teknolojik anlamda sistem her ne kadar sağlam duvarların arkasında çalışır olsa da, bu sistemi kullanacak olan personeller unutulmamalıdır. Kurumda çalışacak olan bireylere işe alım sürecinde hangi bilgilerin kurum içi mahrem olduğuna, şirket içi dâhili sürecin nasıl işleneceği ya da hangi personelin (kurum içi hangi bölümün) hangi bilgiye erişim yetkisi olabileceği konusunda eğitimler verilmelidir. Bu bağlamda sosyal mühendislik saldırıları, hedef olarak insanı alan, kişinin açıklıklarından faydalanarak gerekli bilgiyi toplamak üzerine yapılan saldırılardır. Bu saldırılarda hedefteki kişinin bilgisizliğinden, dikkatsizliğinden ve kişisel zaaflarından (hedefteki kişi hakkında saldırılmadan önce araştırılma yapılmışsa) faydalanılır.

Bu kişiler saldırılarda karşıdaki aktöre göre kendilerine bir rol biçerler. Genel olarak saldırganlar arkadaş canlısı davranıp iyi ilişkiler geliştirmeyi, kendini karşı cins olarak tanıtıp etkilemek(genelde bu tip saldırganların hedefleri erkektir) ya da ast üst ilişkisinden faydalanır. Bu tip saldırıların tercih

edilmesinin sebebi,sisteme doğrudan saldırı yapıp vakit kaybedileceğine kendilerine daha hızlı sonuç verecek atakları geliştirmektir. Sosyal mühendislik saldırılarında amaç; kurumun yapısı, kurumun ağ yapısı, müşteri listesi, çalışan ya da yöneticilerin kişisel bilgileri (adres, telefon, kimlik numarası, personel numarası vs.), kurum içi dâhili numaralar, şifreler ve herhangi bir saldırıda aleyhtekullanılmak üzere ne varsa elde etmektir.

Sosyal Mühendisin Hedefindeki Personeller

- **Direkt Ulaşılabilir Personeller:** Bu personeller direkt olarak müşterilerle ya da sağlayıcılarla iletişime geçen personellerdir. Teknik servis elemanları veya çağrı merkezi çalışanları bu grupta incelenir. Bu pozisyonda ki çalışanlarımız sıkı eğitimlerden geçirilmelidir.
- **Üst Düzey Personeller:** Kurumumuzda pozisyonu gereği ayrıcalıklı yetkilere sahip olan çalışanlar saldırganların en çok hedef almak istediği kişilerdir. Kurum içerisindeki görevi gereği bir takım gizli bilgilere sahip olan bu kullanıcıların, saldırgan tarafından kandırılıp çeşitli bilgiler elde edilmesi kurumumuza oldukça fazla zarar verebilir.
- **Yardım Sever Personeller:** Bu başlıktaki personellerimiz kurum içinde, müşterilerine yardım ve destek için yetkisinden çok daha fazlasını kullanır. Ama bazen işler ters gidip yardım etmek istediği müşterisi kurumumuza sızmak isteyen saldırgan olabilir. Kurumumuz içinde personellerin yetki sınırları belirlenip, bu sınırlar içerisinde görevlerini yerine getirilmesi gerektiği hatırlatılmalıdır.
- **İşe Yeni Başlayan Personeller:** Kuruma yeni başlayan personeller, sisteme erişim hakkı bulunan fakat bunun tam olarak nasıl kullanılacağını bilmeyen personeller ya da yardım masası çalışanları işe

saldırgan arasındaki farkı ayıramayacak personeller kurum için oldukça tehlikeli sonuçlar doğurabilir. İşe yeni başlayan personellere sisteme erişim yetkisi verilmeden önce sıkı eğitimlerden geçirilmeli ve bu eğitim sonunda başarıya ulaştıktan sonra sisteme erişim yetkisi verilmelidir.

- **Kandırılmış ya da İkna Edilmiş Personeller:** Kurumumuzda hala aktif olarak çalışan fakat şirketimize olan bağlılığı zayıflamış, işten ayrılmayı düşünen personeller insani hırslardan ya da karşı tarafın verdiği büyük vaatlerden dolayı kurumumuza zarar verici bir eylemde bulunabilir. Kurum içerisindeki diğer çalışanlar ve insan kaynakları olumsuz davranışlar sergileyen personelleri amirlerine rapor etmelidir.

Sosyal Mühendislik Saldırılarında Kullanılan Yöntemler:

- Kurumun herhangi bir bölümünde ki çalışan gibi davranmak
- Üst düzey yetkili gibi davranmak
- Yardıma ihtiyacı olan bir personel gibi davranmak
- Kendini acındırmak
- Omuz sörfü
- Personele içinde zararlı yazılım bulunan bir usb bellek hediye etmek
- Kurbanı zararlı olan bedava bir yazılımı indirmeye ikna etmek
- Güven kazanmak için şirket içi terimler kullanmak

- Çöp karıştırmak
- Onu önceden tanıyormuş gibi yapmak
- Karşı cinsi etkilemeye çalışmak
- E-Posta ekinde keylogger ya da trojen gibi zararlı yazılımlar göndermek
- Kullanıcının yeniden parola bilgilerini girmesini sağlayan sahte pencereler açmak
- Kendini Emniyet, İstihbarat mensubu gibi tanıtmak
- Teknik destek sağlamak için aradığını ve belli başlı adımları izlemesi gerektiğine ikna etmek
- Kurumun içerisine fiziksel olarak sızmak.

Sosyal Mühendislik Saldırılarına Önlemler:

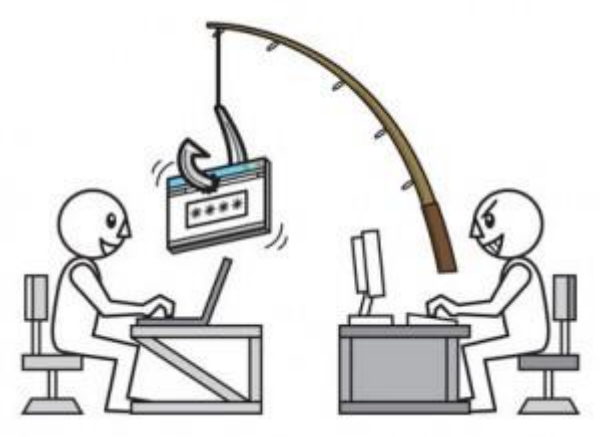
- Kurum içi uyulması zorunlu olan güvenlik protokolleri belirleyin.
- Düzenli olarak sosyal mühendislik saldırılarına karşı personel eğitimleri düzenleyin.
- Kurmunuzun fiziksel güvenlik önlemlerini alın.
- Parolanızı hiç bir zaman ikinci bir kişiyle paylaşmayınız.
- Verilerinizi sınıflandırın (Hassas,dahili,genel vb.).
- Kurum içinde personel kartı taşıma zorunluluğu getirin.
- Beklenmeyen e-posta eklerini açmayın ve tüm ekleri mutlaka virüs taramasından geçirin.
- Phishing mailler ve bu mailler vasıtası ile gelen e-posta eklerine ve düzmece sitelere karşı kurum çalışanlarınızı bilinçlendirin.

- Kurum çalışanı olarak kendini tanıtan kişilerin doğruluğunu tespit etmeden talep ettiği bilgiyi vermeyiniz ve kimlik tespiti için dahili bir süreç belirleyin.
- Kurum içine girişte elektronik kart kullanılma zorunluluğu olmalı ve kuruma ziyaretçi olarak gelen kişilerden mutlaka kimlik alınmalı.
- Bilgisayarınızın başında olmadığınız zamanlarda yetkisiz erişimleri engellemek için, cihazınızı güçlü parolalar ile koruyun.
- Parolalarınızı herhangi bir yere not etmeyin ve omuz sörfü saldırılarına karşı dikkatli olun.
- Belgelerinizi ve elektronik cihazlarınızı tamamen imha etmeden çöpe atmayınız ve şirket sınırları içinde muhafaza edin.
- Doğruluğu tespit edilmiş bilgi işlem personelleri dışında herhangi birinin talimatı ile bilgisayarlara komut girmeyin.

9. Phishing (Oltalama) Saldırıları:

Phishing Saldırısı Nedir:

Phishing İngilizce “Password” ve “Fishing” kelimelerinin birleşmesiyle oluşan ve Türkçe ‘ye oltalama saldırı olarak geçen son zamanların en popüler Sosyal Mühendislik saldırılarındandır.Saldırganlar bu saldırıda, kurbanına e-posta yollayarak saldırıyı gerçekleştirmektedir. Bu e-postalar, kurumun herhangi bir bölümünden ve ya kurbanın aktif olarak kullandığı güvenilir bit siteden geliyormuş gibi gözüken, kurbandan kişisel bilgilerini girmesini, ilgili bağlantıya gidip formu doldurmasını ve ya zararlı yazılım içeren ekteki dosyayı indirmesini ister. Kurbanın doldurduğu forum araçlığıyla ya da sistemine bulaştırdığı zararlı yazılım vasıtasıyla, bilgileri çalmayı amaçlar.



Phishing saldırıları genel kapsamlı, rastgele olarak yapılan saldırılardır. Saldırganların hedef olarak belirlediği kuruma yaptığı oltama saldırılarına “**Spear Phishing (Hedef Odaklı Oltama)**” saldırı denir. Hedef odaklı oltalama saldırısında, saldırgan hedef kurumun ticari sırları, finansal verileri ve ya bu tür bilgileri kendisine sağlayabilecek olan bir kullanıcı adı ve şifreyi ele geçirmeyi amaçlar. Klasik phishing saldırılarından farklı olarak, spear phishing saldırılarından hedef kurum ve personellerini araştırırlar. Kurum içerisinde kullanılan sistemleri araştırabilecekleri gibi, hedef seçtikleri personellerin çeşitli sosyal medya hesaplarını inceleyip, onların hobileri ve ya ilgisini çekebilecek olan bilgileri toplar. Elde ettikleri bilgiler ışığında hedefe özel, phishing mail ve ya açılabilir pencere oluştururlar.

Phishing Saldırısının Amaçları Nelerdir:

- Kimlik bilgilerinin çalınması
- Fikri mülkiyetin elde edilmesi

- Ticari sırların çalınması
- Kurum içi mahrem bilgilerin elde edilmesi
- Finansal verilerin çalınması
- Kullanıcı adı ve Şifrenin çalınması
- Kullanıcı hesap numaralarının çalınması
- İnternet bankacılığı şifrelerinin çalınması
- Kurumun sistemine zararlı yazılım bulaştırılması

Alınması Gereken Önlemler:

- E-postanın kimden geldiğinden emin olunmadan dikkate alınmaması konusunda kurum çalışanları bilinçlendirilmeli, hiçbir kuruluş e-posta yoluyla kişisel bilgileri talep etmez.
- Güvenli olmadığı düşünülen ve halka açık olan internet ağlarından elektronik işlem gerçekleştirmemeleri konusunda kurum çalışanlarını bilinçlendirilmeli.
- İnternet adresi olarak ip değeri barındıran sayısal değerler ile karşılaşıldığında mutlaka dikkat edilmelidir.
- Gelen e-postalarda maili gönderen ve yönlendirdiği internet adresi gibi bilgilere mutlaka bakılmalı.
- Bilgisayarını güncelleştirmeleri ve güvenlik yamaları her zaman kontrol edilmeli ve mutlaka bir anti virüs programı kullanılmalı.
- Şüpheli görülen e-posta ve linkleri ile ilgi mutlaka kurum içi ilgi personeli bilgilendirin.

- E-postalarda ki kısaltılmış URL (bit.ly,goo.gl ve tinyurl.com) adreslerine kesinlikle tıklamamalı.
- Şüpheli ve ya bilinmeyen web sitelere kişisel bilgiler kesinlikle verilmemeli.
- SSL sertifikası güvenli ve kullanıcı ile sunucu arasındaki veriyi 128 bit ile şifrelenmiş bir web sitede işlem yapldığını gösterir. Elektronik işlemler yapılan sayfalarda SSL sertifikasının bulunup bulunulmadığına mutlaka kontrol edilmeli.

10. Kurumsal Sosyal Medya Hesabı Güvenliği

Sosyal medya işlerimizi tanıtmak için kullandığımız önemli bir iletişim aracıdır. Saldırganlar ise kurumsal itibarımıza zarar vermek, müşterilerimize yönelik sosyal mühendislik saldırılarında veya sırf kendi isimlerini duyurup reklam yapmak için bu hesaplarımızı hedef almaktadırlar. Sosyal medya hesaplarımızda yaşanacak bir güvenlik ihlali kurumsal itibarımızı zedeleyecek sonuçlar doğurabilir.

Alınması Gereken Önlemler:

Kurumsal sosyal medya hesaplarının da en nihayetinde bireysel kullanıcıların elinde olduğunu düşünürsek sadece teknik önlemler almak yeterli olmayacaktır. Bu hesapları yöneten personelin de dikkatli olması gerekir.

Politikalarınızı belirleyin

Kurumsal sosyal medya hesaplarına kimlerin erişebileceği, nasıl paylaşımlarda bulunacağı açıkça belli olmalıdır.

Kurumsal sosyal medya hesabı kullanım politikası aşağıdaki başlıkları düzenlemelidir:

- Paylaşılmaması gereken bilgileri belirler
- Sorumlu personelin olumsuz davranışlarının sonuçlarını belirler
- Şirketinize soruların soruları yanıtlayacak kişiyi belirler
- Sosyal medya "tonunu" belli eder (sen mi diyeceğiz? Siz mi? Vb.)
- Şirket kültürüne uygundur
- İlgili personele yol gösterir niteliktedir
- Şirket çalışanlarının kişisel hesaplarında şirket ismini/logosunu kullanabilmesini ve işleri hakkında görüş bildirme özgürlüğü (veya yasağı) gibi konular da bu politika dahilinde belirlenebilir.

Sahipleri belirleyin

Kurumsal sosyal medya ağlarının kim veya kimler tarafından yönetileceğinin net bir şekilde belirlenmesi çok önemlidir. Kullanıcı bilgileri mümkün olduğunca üçüncü taraflarla paylaşılmamalı, paylaşılması gerekiyorsa (halkla ilişkiler firması, vb) bunun çok sıkı bir şekilde denetlendiğinden emin olun.

Kullanıcılarınızı eğitin

Sosyal medya hesaplarıyla ilgilenecek personelin sosyal medya üzerinden gelebilecek tehlikelere karşı eğitilmesi önemlidir. Sosyal mühendislik saldırılarına karşı ekstra tedbirli olmaları gerekir. Bu saldırılar DM (direkt mesaj) yoluyla yapılabileceği gibi, herkese açık şekilde "@sirketinizin_kullanıcı_adı bu iddia doğru mu?" veya "@sirketinizin_kullanıcı_adı sizi çok seviyorum!" gibi merak uyandıracak bir mesajın devamında kısaltılmış bir URL (t.co, bit.ly veya goo.gl gibi bir hizmet kullanılarak adresin tamamını yazmak yerine, gerçek adresi saklayacak kısaltılmış bir adres) ile yapıldığını görüyoruz.

Sürekli izleyin

Hesaplarınızı gerçek zamanlı ve sürekli olarak izleyin. İzinsiz veya politikaların izin verdiğinin dışında yapılacak

paylaşımlardan ne kadar hızlı haberdar olursanız o kadar kısa sürede müdahale edebilirsiniz.

Maksimum güvenlikle kullanın

Bir çok önemli sosyal medya platformu SMS ile tek kullanımlık şifre gönderimi (2 factor authentication) gibi ek güvenlik özellikleri sunmaktadır. Bunlar mutlaka kullanılmalıdır.

Uygulamalara dikkat edin

Sosyal medya hesabınıza yükleyebileceğiniz üçüncü taraf uygulamaların (doğum günü hatırlatıcısı, oyun, vb.) birer saldırı vektörü olabileceğini unutmayın. Kurumsal hesaplara gerekmedikçe uygulama yüklenmemesinde fayda vardır.

Güvenli ağlardan giriş yapın

Kurumsal sosyal medya hesabına ortak kablosuz ağ veya bilmediğiniz/güvenmediğiniz ağlar üzerinden giriş yapmayın. Bu tür durumlarda güvenli olduğunu bildiğiniz bir ağa VPN tünel (SSL veya IPsec) oluşturup onun üzerinden bağlanın.

Parola

En kritik konulardan birisi de kırılması/tahmin edilmesi zor bir parola kullanılması, bunun düzenli aralıklarla değiştirilmesi ve bu parolanın dağıtımının kontrollü bir şekilde yapılmasıdır.

Farklı bir tarayıcı kullanın

Kişisel güvenliğiniz için bankacılık işlemlerinizi günlük olarak internette kullandığınızdan farklı bir tarayıcı kullanmanızda fayda vardır. Benzer şekilde kurumsal sosyal medya hesaplarına erişim için personelin günlük olarak

kullandığından farklı bir tarayıcı kullanmasında fayda var. Saldırganlar bir tarayıcıyı kolayca ele geçirip üzerinde saklanan parolaları görebilirler. Bu tür bir saldırıya kurban gitmemek için sosyal mühendislik saldırılarına hedef olabilecek tarayıcıyı ayrı tutmak lazım.

Sosyal medya hesaplarının kullanıldığı bir şirkette saldırganların akıllarına gelen bütün saldırı vektörlerini kullanacaklarını göz önünde bulunduracak şekilde bir risk analizi ve testleri yapılmalıdır.

11. Parola Güvenliği

Gerçekleşen saldırılarında, belki de en çok elde edilmek istenen bilgi kurumun kullandığı sunucuya,sisteme ya da OWA gibi kurumsal e-posta adreslerine erişimini mümkün kılacak parolaları ele geçirmektir. Sosyal mühendislik başlığında da bahsettiğimiz gibi sistemi kırmak ya da Brute Force atakları yaparak şifre elde etmek daha çok zaman alacak eylemler olduğu için ilk olarak sosyal mühendislik yolları ile elde etmeye çalışacaktır. Siber saldırganlar sosyal mühendislik saldırlarında başarıyı ulaşamaz ise bir sonraki adımları olan şifrenizi kırma aşamasına geçecektir.

Özellikle kurum sistemelerine yapılan şifre deneme saldırılarında sistemlerin default olarak bırakılmış parolar (https://cirt.net/passwords adresinden ulaşabilirsiniz) ya da basit parolalar kulanılması siber suçluların sisteminize girmesine ve ağır hasarlar yol açmasına sebep olabilir. . Bu saldırılarda ki başarılar inanılmaz derecede iyidir örnek vermek gerekirse; 15 Temmuz 2015 de hacklenen **Ashley Madison** adlı arkadaşlık sitesine ait parolalar yayınlandı ve çalınan 11 milyon parola üzerinde yapılan incelemelerde en sık kullanılan ilk 3 parola şu şekildedir;

1. 120 bin kişi ile “123456”
2. 48 bin kişi ile “12345”
3. 39 bin kişi ile “password”

Yukarıda listelenen şifrelere baktığımızda Brute Force saldırısında kullanıcılara sadece bu 3 şifre ile deneme yapsak 207 bin kişinin hesabını ele geçirmiş oluyoruz. İnsanlar bazen parola oluşturma gibi konuda bu kadar özensiz davranıyor, bu tarz parolalar oluşturmak hırsızlara karşı kapısı ve penceresi açık bırakılmış bir ev kadar güvenlidir. Kurumlar içersin de

personeller ve kullanılan sistemler için bir şifre politikası belirlenip, güvenli şifre oluşturmak zorunlu bir görev olmalıdır.

Parola Güvenliği İçin Tavsiyeler:

- En az 8 karakterden oluşturulmalıdır.
- Harfler ve özel karakterlerin (“^, +, %, &, /, (, $,], *, ?, _, -”) kullanılması zorunlu olmalıdır.
- Parolalarda büyük ve küçük harf kullanımı zorunlu olmalıdır.
- Parolalarımızda kişisel bilgiler (eşimizin adı, çocuğumuzun adı, doğum tarihi vb.) bilgiler bulunmamalı
- Parolalarımızda ünlü isimler, film adları ve karakter isimleri (frodo, batman, messi) bulundurulmamalıdır

- Bütün fabrika çıkışlı parolaları değiştirin
- Kullanıcılarınızın parolalarını yönetmelerini kolaylaştırın. Parola yönetimi yazılımı kullanmak farklı sistemler için farklı parola kullanmalarını kolaylaştıracaktır
- Kullanıcılar tarafından belirlenen parolaların zayıf olabileceğini kabul edin. Parola politikalarını belirlemez ve bunların uygulanması için gerekli teknik önlemleri almazsanız kullanıcılar her zaman basit parola kullanmayı tercih edecektir.

- Otomatik olarak atanan parolaların da sorunlu olabileceğini kabul edin. Bilgisayar tarafından oluşturulan süper karmaşık bir parola güzeldir tabii ki ama hatırlaması zor olacağından kullanıcıların bunu bir yere not edebileceğini düşünmemiz gerekir. Bu nedenle otomatik olarak oluşturulan parolaların daha kolay hatırlanabilmesini sağlayacak bazı kurallar belirlemekte fayda olabilir

- Kullanıcı ve yetkili hesapları farklı yönetin. Kullanıcıların güçlü parola kullanması yeterli olabilir belki ama yetkili hesaplara girişin iki kademeli bir doğrulama ile yapılması uygun olacaktır
- Hesapları kilitleyin. Belli bir sayıda yanlış parola denemesi yapıldığında hesabın kilitlenmesini sağlayın. Bunun dışında giriş denemeleri ve benzeri saldırgan davranışları da izleyecek bir sistem kurulmalıdır
- Parolaları düz metin olarak tutmayın. Her hesap için tekil olan bir girdi (salt) ile birlikte hash değerlerini tutun
- Sosyal mühendislik ve phishing başlıkları altında verilen önlemler dizisine dikkat edin.

Linux/Windows Dosyaları ve Komutları:

Linux:

- ls -> Dosyaları listeler
- cd dir -> Belirtilen dizine girer
- cd -> Ana dizine geçiş yapar
- pwd -> Bulunduğunuz dizini gösterir
- rm dosya -> Dosya siler
- rm -r dizin -> Belirtilen dizini siler
- rm -f dosya -> Belirtilen dosyayı silmeye zorlar
- cat > dosya -> Dosyaya girdi yönlendirir
- more dosya -> Dosyanın çıktısını sayfalayarak gösterir
- head dosya -> Dosyanın ilk 10 satırını gösterir
- tail dosya -> Dosyanın son 10 satırını gösterir
- tail -f dosya -> Dosyanın son 10 satırını eşzamanlı olarak gösterir
- date -> Şuan ki tarihi verir
- cal -> Takvimi gösterir

- w -> Sistemle ilgili özet bilgileri verir
- whoami -> Giriş yapan kullanıcıyı gösterir
- finger kullanıcı -> kullanıcı hakkında bilgi verir
- uname -a -> çekirdek bilgisini gösterir cat
- /proc/cpuinfo -> işlemci bilgisini gösterir
- cat /proc/meminfo -> RAM bilgisini gösterir
- man komut -> Girilen komutun kullanımını gösterir
- df -> disk kullanımını gösterir
- free -> kullanılan RAM bilgisini gösterir
- ps -> aktif süreçleri gösterir.
- top -> tüm süreçleri gösterir
- kill pid -> belirtilen süreçi sonlandırır
- killall proc -> belirtilen tüm süreçleri sonlandırır
- chmod -> Bir dosyanın izin haklarını değiştirir
- history -> Kullanıcının o zamana kadar kullandığı komutları gösterir.
- Hostname -> Sistemin host adını gösterir.
- Last -> Sistem de en son oturum açan kullanıcıları listelersiniz.
- Lsmod -> Yüklenmiş modülleri gösterir.
- Netstat -> Ağ bağlantılarını görüntüler
- Nslookup -> DNS sorgusu
- Passwd -> Şifre değiştirir
- Traceroute -> Router takibi
- Ping hedef -> Hedef ip ye ping atar
- Whois domain -> Belirtilen alan adının kayıt bilgilerini gösterir.
- Dig domain -> Belirtilen alan adının DNS bilgilerini gösterir.
- Arp -> Host ve IP numarasini göster.4123

Iptables:

Linux da varsayılan güvenlik duvarı olan ip tables, servislerin çalıştığı portlardan geçen trafiği engelleyebilir veya başka bir porta yönlendirebilir.

-N	Yeni işlem ekleneceğini belirtir.
-X	Boş bir zinciri siler.
-L	Listeleme işlemi yapar.
-F	Tüm kuralların silineceğini belirtir.
-D	Belirtilen kuralı siler.
-A	Yeni bir kural oluşturur.
-R	Belirlenen yerdeki kuralı yeni kural ile değiştirir.
-I	Kural eklemek için kullanılır
-s	Kaynak adresi belirtmek için kullanılır
-d	Varış adresini belirtmek için kullanılır
-p	Kuralda kullanılacak protokolü belirtir
-j	Uygulanacak kuralı belirtir. (DROP paketi kabul etmez ve gönderilen kişi paketin engellendiğinden haberi olmaz, ACCEPT paketi kabul eder, REJECT paketi kabul etmez ama gönderen kişi bilgilendirilir.)

Linux Dosyaları ve Kullanım Amaçları:

.bash_history: Kullanıcıların çalıştırdıkları son komutlar bulumaktadır.

/etc/login.defs: Kullanıcıların sisteme giriş ve parolaların düzenlenmeleri ile ilgili bazı bilgiler bulundurur.

/etc/resolv.conf: DNS ayarları için kullanılan dosyadır.

/etc/services: Sistemde bulunan servislerin kullandıkları port numaralarını barındırır.

/etc/hosts: Makine isimleri ve ip adresleri gibi bilgileri barındırır.

/var/log/message : Genel olarak logların yazıldığı dosya, sistem ile ilgili loglar
/var/log/cron.log : Cron işlemi logları (cron job)
/var/log/boot.log : System boot logları
/var/log/utmp : Login kayıt logları
/var/log/wtmp : Login kayıt logları
/var/log/yum.log : Paket yükleme uygulaması logları Centos
/var/log/apt.log : Paket yükleme uygulaması logları Debian
/var/log/auth.log : Kullanıcı tanıma logları
/var/log/kern.log : Çekirdek Logları
/var/log/maillog : Mail server logları
/var/log/mysqld.log : MySQL database server log dosyası
/var/log/secure : Authentication log
/var/log/faillog : Kullanıcı başarısız giriş logları
/var/log/dpkg.log : Tüm binary paket logları, yükleme ve diğer bilgileri içerir.
/var/log/fsck/ : fsck komutunun logları
/var/log/apport.log : Uygulamaların hatalarının işlendiği log dosyası
/var/log/daemon.log : NTPD gibi çalışan servislerin loglarının tutulduğu dosya
/var/log/debug : Hata ayıklama için kullanılan log dosyasıdır
/var/log/syslog : Sistem mesaj servisinin log dosyasıdır
/var/log/proftpd : FTP servisinin log dosyasıdır (Proftp)
/var/log/syslog : Sistem mesaj servisinin log dosyasıdır

/var/log/dmesg : Sisteminiz boot ederken olusan hatalari dmesg programi ile gözlemliyebilirsiniz. Özelikle ag kartiniz yada sürücülerle ilgili sorunlari gözlemlemek icin faydalı olabiliyor
/var/log/proftpd.log : Proftp FTP servisinin loglarının tutulduğu dosyadır.
/var/log/kern.log : Çekirdekte meydana gelen olayların loglarının tutulduğu dosyadır.Kernel yani çekirdek, sunucunuzun en önemli bileşenidir. Normal kullanımında, log dosyasını çok dolu olarak görmezsiniz, fakat herhangi bir disk ya da farklı bir donanım sorununda, bu log dosyası bu sorunlarla ilgili önemli bilgileri size sunar.
/var/log/auth.log : Kullanıcıların ne zaman giriş yapmaya çalıştığı ile ilgili bilgileri tutar. Önemli giriş bilgilerini /var/log/secure (yetkilendirme logları) dosyası aracılığıyla da kontrol edebilirsiniz.
/var/log/maillog : Herhangi bir spam sorunu var ise; spam yaratanı bu loglardan bulabilirsiniz. Aynı zamanda herhangi bir "brute force" yani; saldırı durumu olup olmadığını da kontrol edebilirsiniz.
/var/log/httpd ya da /var/log/apache2 : Apache web sunucuları için; access, error gibi logları barındırır.
/var/log/mysqld.log : Mysql Logların tutulduğu dosyadır.

Windows Komutları:

- **assoc**: Dosya uzantılarını ve bunların ilişkilendirmesini gösterir ya da değiştirir.
- **attrib:** Dosya özniteliklerini görüntüler ve ya değiştirir.
- **cacls:** Dosyanin erişim denetim listelerini görüntüler ve ya değiştirir.

- **cd:** Geçerli dizini değiştirir ya da görüntüler.
- **date**: Sistem tarihini görüntülemek ve ya değiştirmek için kullanılır.
- **del**: Dosya silmek için kullanılır.
- **dir**: Bir dizinde ki dosya ve alt dizinleri gösterir.
- **time**: Sistem saatini görüntüler.
- **ver:** Kullanılan işletim sistemi versiyonunu gösterir.
- **vol**: Diskin etiket numarasını ve seri numarasını gösterir.
- **md:** Dosya oluşturmak için kullanılır.
- **rd:** Klasör silmek için kullanılır.
- **copy:** Dosya kopyalamak için kullanılır.
- **format**: Diski biçimlendirir.
- **control admintools**: Yönetimsel araçları açar.
- **ipconfig**: İp yöneticisi
- **ipconfig/all**: İp adresini ve yapılandırma bilgilerini gösterir.
- **ipconfig /displaydns** : DNS cache
- **ipconfig /flushdns** : DNS cache temizleme
- **logoff**: Geçerli oturumu kapatır.
- **perfmon**: Performans izleyicisi
- **systeminfo**: Sistem özelliklerini ve bilgilerini gösterir.
- **ping:** Hedef ip ye ping atar.
- **tasklist**: Çalışan programları listeler.
- **taskkill**: Çalışan programları kapatmak.
- **sc query**: Çalışan servisleri listeler.
- **wmic bios get name,serialnumber,version**: Bios modelini ve seri numarasını öğrenmek için kullanılır.
- **wmic csproduct get name,identifyingnumber,uuid:** Anakart modelini ve seri numarasını öğrenmek için kullanılır.

- **wmic cpu get name,CurrentClockSpeed,MaxClockSpeed** : İşlemci modelini ve seri numarasını öğrenmek için kullanılır.
- **tracert**: Paketlerinizi bilgisayarınızdan hedefe göndermede kullanılan IP yönlendiricileri serisini ve her atlamada bunun için geçen süreyi görüntüler.
- **syskey**: Kayıtlı bulunan şifrelerin veritabanına ulaşır.
- **chkdsk**: Harddisk hataları düzeltme aracı.
- **sfc /scannow:**Korumalı sistem dosyalarının bütünlüğünü kontrol eder.
- **regedt32**: Windows kayıt defterini açar.
- **wscui.cpl** : Windows güvenlik merkezini erişim sağlar.
- **netplwiz**: Kullanıcı hesapları ve denetimini açar.
- **pathping:** Hedefe gönderilen paketlerin durumunu öğrenmemizi sağlar.
- **%systemroot%** : İşletim sisteminin kurulduğu klasör.
- **%username%:** Logon olan kullanıcının ismidir.
- **arp:** Adres çözümleme protokolü önbelleğini görüntüler.
- **net share:** Bilgisayardaki paylaşılmış klasörleri ve sürücüleri görüntüler.
- **mmc:** Windows yönetim panelini açar.
- **driverquery:** Yüklü olan tüm sürücülerin listesini görüntüler.
- **netstat:** Ağ bağlantılarını, yönlendirme tablolarını ve ağ ara yüzlerini gösterir.

Kaynakçalar:

1. http://alperbasaran.com/ag-guvenligi-kontrol-listesi/
2. http://www.slideshare.net/AlperBasaran
3. https://www.us-cert.gov/security-publications
4. http://www.udhb.gov.tr/doc/siberg/Kurumsal_SOME_Reh_V1.pdf
5. http://www.webguvenligi.org/docs/web_uygulama_guvenligi_kontrol_listesi_2010.pdf
6. http://www.webguvenligi.org/belgeler
7. http://www.slideshare.net/AlperBasaran/sosyal-muhendislik-saldrlar
8. http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/a%C4%9F-cihazlar%C4%B1n%C4%B1n-g%C3%BCvenli%C4%9Fini-sa%C4%9Flama-y%C3%B6ntemleri
9. https://docs.google.com/document/d/1zoSvVk0hSLIgCyPnz2K-bXVTWvi5LXBU4bYkBMrlzYw/edit?pref=2&pli=1
10. https://eventualis.org/wp-content/uploads/2011/06/cheatsheet-tr.pdf
11. http://www.mimforeva.com/linux-log-dosyalari/