Siber güvenlik

RÜVEYDA ÖZLÜ-19360859014

SUNUMA GENEL BAKIŞ

- SİBER GÜVENLİK NEDİR?
- SALDIRGAN TİPLERİ
- SALDIRI TÜRLERİ-KÖTÜ AMAÇLI YAZILIMLAR NELERDİR?
- SALDIRILARIN-KÖTÜ AMAÇLI YAZILIMLARIN OLASI BELİRTİLERİ
- BU SALDIRILARDAN NASIL KORUNABİLİRİZ?

- Siber , İngilizce ‘cyber’ kelimesinden çevrilmiş olup «Bilgisayarlara dahil olan , kullanan ve ilgili olan» anlamlarında kullanılmıştır. Bunun yanı sıra dijital verinin olduğu tüm alan siber olarak adlandırılmıştır ancak siber sadece İNTERNET DEĞİLDİR! Çünkü internet dışında çeşiti ağlar vardır ve bunlar internete bağlı değildir. Askeri ağlar , Demiryolu Hattı , Karayolu Hattı ve Metro Hattı ağları buna örnektir.
- Buradan siber güvenlik kavramına geçiş yapılacak olursa;

«Siber Güvenlik , teknolojinin ve ağ sistemlerinin oldukça gelişmiş olduğu bu dönemde , bireyi ve toplumu bu sanal ortamın zararlı etkilerinden korumayı amaçlayan bir güvenlik sistemidir.» denebilir.

PEKİ NEYİ KORUYORUZ?

Burada korumak istediğimiz en önemli şey «VERİ»lerdir.

- Veri , bilgisayar ortamında bulunan bilgilerin , programlar tarafından işlenebilmesi için derlenmiş ve formüle edilmiş şeklidir. Bunlar tıbbi kayıtlar , eğitim kayıtları , finansal belgeler şeklinde kişisel veriler olabildiği gibi kurumsal veriler de olabilir ve bunları hangi ortamda olursa olsun korumak zorundayız.
- Buna uygun bir örnek olarak KVKK verilebilir. KVKK yani Kişisel Verilerin Korunma Kanunu 7 Nisan 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bu kanun ile , kişisel verilerin sınırsız biçimde ve gelişigüzel toplanması , yetkisiz kişilerin erişimine açılması , ifşası veya kötüye kullanımı sonucu kişilik haklarının ihlal edilmesinin önüne geçilmesi amaçlanmıştır.

KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Verilerimiz ne zaman güvenli kabul edilir?

Bunun için CIA bileşenleri olarak adlandırılan 3 kritere bakılması gerekir:

- CONFIDENATIALITY(GİZLİLİK) : Verilerin sadece yetkisi olan kimseler tarafından görülmesinin sağlanmasıdır.
- INTEGRITY(BÜTÜNLÜK): Verilerin yetisiz kişiler tarafından değiştirilmesinin engellenmesidir.
- AVAILABILITY(ERİŞİLEBİLİRLİK): Kişilerin ihtiyaç duyduğunda verilerine ulaşabilmesidir.

AMA TABİ Kİ HİÇBİR ZAMAN %100 GÜVENLİK SÖZ KONUSU OLMAYACAKTIR.

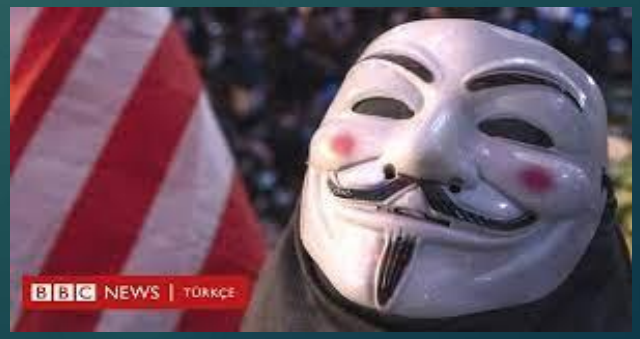
VERİLERİ KİMDEN VEYA NEYDEN KORUYORUZ?

Siber saldırganların kimi ün yapmak , kimi para kazanmak kimi de belirli motivasyonlarla saldırı gerçekleştirse de büyük çoğunluğu bu işi maddi amaçlarla yapar.

Amatörler

Hackerlar

Organize Gruplar



SALDIRGAN TÜRLERİ

- AMATÖRLER(SCRİPT KIDDIES): Network , kodlama , işletim sistemi gibi konularda becerisi az olan veya hiç olmayan ve saldırılar için internetten buldukları hazır araçları kullanan bir gruptur. Her ne kadar hazır araçları kullansalar da bu saldırılar zarar verici sonuçlar doğurabilir.
- HACKERLAR: Bu grup beyaz , gri , siyah şapkalı olarak üçe ayrılır. Network , kodlama , işletim sistemi gibi konularda yeterli bilgiye sahiptirler. Elde ettikleri verileri iyi niyetle ve sistemlerin zafiyetlerini tespit etmek için kullanıyorlarsa beyaz şapkalı, kötü niyetle kullanıyorlarsa siyah şapkalı , girdikleri sistemde buldukları açıkları sisteme zarar vermeden ve bilgileri çalmadan sistem yöneticilerine haber veriyorlarsa gri şapkalı olarak adlandırılırlar.
- ORGANİZE GRUPLAR: Bu grupta siber suçlular , hacktivistler , teröristler ve devlet destekli bilgisayar korsanları bulunur. Siber suçlular genellikle güç ve zenginlik odaklı profesyonel suçlu gruplardır. Hacktivistler kendileri için önemli olan konularda farkındalık yaratmak için politik açıklamalar yaparken , devlet destekli saldırganlar ise hükümet adına istihbarat toplar yada sabotaj yaparlar.

En yaygın zararlı yazılım türleri:

- CASUS YAZILIM(SPYWARE): Kullanıcıyı izlemek için tasarlanmıştır. Genellikle etkinlik izleyicileri , tuş vuruşu toplama ve veri yakalama içerir.
- FİDYE YAZILIMI(RANSOMWARE): Bir bilgisayar sistemini veya içerdiği verileri bir ödeme yapılıncaya kadar esir tutmak için tasarlanmıştır. Genellikle veriler kullanıcı tarafından bilinmeyen bir anahtarla şifrelenir.
- VİRÜS(VIRUS): Kendini diğer dosyaların içerisine gizleyerek kullanıcının izni yada bilgisi dahilinde olmadan bilgisayarın çalışma şeklini değiştiren bir tür bilgisayar programıdır. Çoğu virüs USB , Optik diskler , ağ paylaşımları ve e-posta ile yayılır.
- TRUVA ATI(TROJAN): İstenen bir işlem kisvesi altında kötü amaçlı işlemler yapan yazılımlardır. Onu çalıştıran kullanıcının ayrıcalıklarından yararlanır. Truva atları diğer zararlı yazılımlar gibi kendi başlarına işlem yapamazlar. Kendilerini kopyalayıp dağıtsalar bile her kurbanın programı(Truvayı) çalıştırması gerekir

- SOLUCAN(WARM): Ağdaki güvenlik açıklarından yararlanarak kendilerini çoğaltan yazılımlardır. Genellikle ağları yavaşlatır. İlk enfeksiyondan sonra artık kullanıcı katılımına ihtiyaç duymazlar. Bir host enfekte olduktan sonra , solucan üzerinden çok hızlı bir şekilde yayılır
- ORTADAKİ ADAM(MAN-IN-THE-MIDDLE): Saldırganın kullanıcının bilgisi olmadan bir cihaz üzerindeki kontrolü ele geçirmesini sağlar. Bu erişim düzeyi ile saldırgan , kullanıcı bilgileri istenen hedefe gönderilmeden önce araya girebilir ve bu bilgileri yakalayabilir. Finansal bilgileri çalmak için yaygın olarak kullanılmaktadır
- OLTALAMA(PHISHING): Genellikle kullanıcı isimleri, parolalar, kredi kartı bilgileri, ağ kimlik bilgileri gibi hassas ve gizli bilgilere ulaşmak amacıyla yapılan saldırılardır. Siber saldırganlar, telefon veya e-posta yoluyla normal bir birey veya kurum gibi görünerek mağdurları belirli eylemleri - zararlı bir bağlantıya veya eke tıklamak gibi - gerçekleştirmeleri veya isteyerek gizli bilgileri açıklamaları için manipüle etmek üzere sosyal mühendisliği kullanırlar.

SOSYAL MÜHENDİSLİK

Sosyal mühendislik, saldırganın istediği şekilde davranmanızı sağlayan psikolojik bir saldırı türüdür. Teknoloji kullanımından çok insanların hile ile kandırılarak bilgi elde edilmesidir. Kötüye kullanılan unsur ise sistem zafiyetleri değil insan zafiyetleridir.

Karşılıklı etkileşim açısından sosyal mühendislik türlerini iki başlık altında toplayabiliriz.

- İnsan Tabanlı Sosyal Mühendislik Teknikleri: Burada insanlarla doğrudan iletişime veya etkileşime geçilmesi söz konusudur. Amaç istenen bilginin doğrudan elde edilebilmesidir. Bu noktada başkasının kimliğine bürünme , üçüncü taraf gibi davranma , yardım ve destek hizmetlerini kullanma gibi durumlar karşımıza gelmektedir.

- Bilgisayar Tabanlı Sosyal Mühendislik Teknikleri: Sosyal mühendislik süreçlerinde insanlarla doğrudan etkileşime geçilebildiği gibi bilgisayar tabanlı teknikler de kullanılmaktadır. Bu teknikte ‘OLTALAMA-PHİSHİNG’ vazgeçilmez bir unsurdur. Aynı şekilde telefonla dolandırıcılık , sahte siteler , trojan ve benzeri türdeki zararlı kodların kullanımı da yaygındır.

Sosyal mühendislik süreçlerinde kurbandan alınabilecek bilgi karşılığında yardım , para , hediye ve benzeri ilgi çekici birçok yöntem kullanılabilir. Hassas bilgiye ulaşmak için kişinin zafiyetlerini kullanmaya yönelik karşımıza gelen bu siber saldırı türü saldırganın kârlı çıkacağı bir senaryoya ikna edilmeye çalışılır.

İnternet Şubemize Giriş Yapan
Müşterilerimiz ;
-90 İPhone X
-900 Samsung Galaxy Tab 3 LİTE
-9000 Kişiye 200 TL Bonus Puan . Detaylar
İnternet Şubemizde http://vakiftank.com/

Olası Saldırılardan Korunma Yöntemleri

- İşletim sisteminizi ve yazılımlarınızı güncel tutun

Çok duyduğumuz bir öneri olsa bile aslında ciddi önem arz etmektedir. Bunun en büyük somut örneği 'WANNACRY' saldırısıdır. Mayıs 2017 de gerçekleşen bu saldırı küresel bir fidye yazılım salgınıydı ve hedefi Microsoft Windows işletim sistemleriydi. Kullanıcının dosyaları rehin tutuldu ve bunların iadesi için Bitcoin cinsinden fidye istendi. Çağın gerisinde kalmış bilgisayar sistemlerinin kullanılmaya devam edilmesi ve yazılım güncellemesi konusunda gerekli bilince sahip olunmaması saldırının başarılı olmasına sebep oldu. Microsoft , WannaCry fidye yazılımı saldırısı başlamadan yaklaşık iki ay önce kullanıcıların sistemlerini saldırganların kullandığı güvenlik açığına karşı koruyan bir güvenlik yaması yayınladı. Ne yazık ki , birçok kişi ve kuruluş işletim sistemlerini düzenli olarak güncellemediğinden saldırıya karşı savunmasız kaldı. Yani güncellemeyi saldırıdan önce yüklememiş olanlar yamadan yararlanamadı ve güvenlik açığına karşı savunmasız kaldı. Bu saldırıya maruz kalan kişilere üç gün içinde fidyeyi ödemezlerse dosyaların kalıcı olarak silineceği söylendi. Verilerin iadesinin herhangi bir garantisi olmadığından bu fidyenin ödenmemesi gerekir. Zaten bu saldırıda da kurbanların dosyalarını geri alıp alamadığı da hala kesinleşmemiştir , bazı araştırmacılar bir kişinin bile dosyalarını geri alamadığını iddia etti. Bu gibi durumlar için dikkat etmemiz gereken bir diğer unsurda diğer maddede belirteceğimiz gibi verilerinizi yedeklemeniz.

- Verilerinizi yedekleyin:
- Güvenlik duvarı kullanın: Güvenlik duvarı , Network üzerinden gelecek ataklara karşı savunma yapar. Zararlı yazılım , bir makineye bulaştıktan sonra Network üzerinden diğer cihazlara bulaşmaya çalışır , güvenlik duvarı bu teşebbüsü engeller.
- Maillerdeki linklere ve USB belleklere dikkat edin.
- Bilmediğiniz yazılımları çalıştırmayın.
- Antivirüs yazılımı kullanın.
- Güçlü parolalar kullanın ve kişisel bilgilerinizi gerekli olmadıkça paylaşmayın.

BENİ DİNLEDİĞİNİZ İÇİN TEŞEKKÜR EDERİM ☺