Ağ ve Bilişim Güvenliği

Öğr. Gör. Zafer SERİN

SİBER GÜVENLİK TEHDİT UNSURLARI

- Eskiden siber saldırılar sadece büyük kuruluş ve sistemlere yapılırdı. Artık kötü niyetli saldırganlar, kişi veya kuruluş ayırt etmiyor.
- Reklamlar veya masum görünen paylaşımlara kontrolsüz tıklama.
- Halka açık bir internete bağlanma hatası.
- Siber güvenlik tehdit unsurları, bilgisayar sistemleri, ağlar ve dijital varlıklar için potansiyel risk oluşturan faktörlerdir.
- İşte siber güvenlik tehdit unsurlarının bazıları:

SİBER GÜVENLİK TEHDİT UNSURLARI

- Kötü Amaçlı Yazılım(Malware)
- Virüs
- Truva Atları(Trojans)
- Casus Yazılım(Spyware)
- Botnet
- Fidye Yazılımı(Ransomware)
- Buffer Overflow
- Cross-Site Request Forgery(CSRF)
- Broken Access Control
- Zero-Day Exploits(0 Days)
- Port Configuration Hataları
- RAT(Remote Access Trojan)
- Man-in-the-Middle(MITM) Saldırısı
- Denial-of-Service(DOS) Saldırısı

ZARARLI YAZILIM NEDİR?

- Zararlı yazılımlar, sistemleri parçalamaya, bilgi sızdırmaya, sistemi ele geçirmeye yönelik olabilir.
- Özünde her zararlı yazılım bir kod parçacığıdır.
- Onları kendi içerisinde kategorize eden şey bulaştıkları sistemde nasıl davranışlar sergiledikleridir.
- Bu davranışlara göre zararlı yazılım bir Trojan, Worm, Ransomware veya virüs olarak adlandırılabilirler.

VİRÜS

- Virüs, bilgisayarlar ve diğer dijital cihazlar için zararlı yazılımlardandır.
- Virüs, genellikle zararlı bir program veya kod parçasıdır ve başka bir programın içine veya dosyasına yerleştirilmiştir.
- Bilgisayarınıza bulaştığında, zararlı kodlar çalışır ve cihazınıza zarar verebilir.
- **Nasıl Bulaşır?**
  - ✓ Virüsler, çeşitli yollarla bulaşabilirler. Bunlar arasında e-posta ekleri, kötü amaçlı web siteleri, yazılım güncellemeleri veya zararlı programların yasadışı kopyaları bulunabilir.

VİRÜS ÖRNEKLERİ

- Creeper(1971)
- Morse(1972)
- Elk Cloner(1982)
- Brain(1986)
- LoveLetter(2000)
- ILOVEYOU Virüsü(2000)
- SoBig(2003)

WORM(SOLUCAN)

- Worm(Solucan), bilgisayar ağlarında hızla yayılan ve çoğalan, zararlı bir yazılım türüdür.
- Worm, bilgisayar ağı veya cihaz içindeki diğer cihazlara kendini kopyalayabilen bir zararlı yazılımdır.
- Worm’ler kendilerini çoğaltarak hızla yayılır ve genellikle bilgisayar sistemlerine zarar verirler.

WORM(SOLUCAN)

- **Nasıl Bulaşır?**
  - ✓ Worm’ler genellikle bilgisayar ağlarında veya internet üzerindeki güvenlik açıklarını kullanarak yayılırlar.
  - ✓ İnfekte edilmiş bir cihazdan diğer cihazlara otomatik olarak kopyalanabilirler.
  - ✓ E-posta eklentileri veya indirilebilir dosyalar gibi bulaştırma yöntemleri de kullanılabilir.

WORM(SOLUCAN) ÖRNEKLERİ

- Morris(1988)
- Melissa(1999)
- Code Red(2001)
- Slammer(2003)
- MyDoom(2004)
- Storm(2007)

SPYWARE(CASUS YAZILIM)

- Spyware(Casus Yazılım), kullanıcının bilgisayarını veya diğer cihazlarını izlemek, bilgi toplamak ve genellikle izinsiz olarak kişisel bilgileri çalmak amacıyla tasarlanmış zararlı yazılımlardır.
- Spyware, kullanıcının bilgisayar aktivitelerini izleyen ve toplayan bir yazılım türüdür. Bu yazılım, genellikle kullanıcının izni olmadan veya farkında olmadan kurulur.
- Spyware, kullanıcının gezdiği web sitelerini, klavye girişlerini, e-posta adreslerini, parolaları ve diğer kişisel bilgileri kaydedebilir.

SPYWARE(CASUS YAZILIM)

- **Nasıl Bulaşır?**
  - ✓ Spyware, genellikle ücretsiz yazılımların veya uygulamaların içine gizlenmiş olarak gelir. Kullanıcılar bu yazılımları indirip kurduklarında spyware de sistemlerine bulaşır.
  - ✓ Bazı web siteleri, zararlı pop-up reklamlar aracılığıyla da spyware bulaştırabilir.

SPYWARE ÖRNEKLERİ

- Adware(Reklam Destekli Yazılım)
- Keyloggers(Tuş Kaydediciler)
- Trojan Horses(Truva Atları)
- Web Browser Hijackers(Tarayıcı Kaçıranlar)
- Mobile Spyware(Mobil Casus Yazılım)

ADWARE(REKLAM YAZILIMI)

- Adware, ‘advertising-supported software’ ifadesinin kısaltmasıdır ve reklam destekli yazılım anlamına gelir.
- Temel amacı, kullanıcının internet tarayıcısına veya bilgisayarına istenmeyen reklamlar eklemek ve bu reklamlar aracılığıyla gelir elde etmektir.
- Adware genellikle ücretsiz yazılımların veya uygulamaların bir parçası olarak bilgisayara bulaşır.

ADWARE(REKLAM YAZILIMI)

- **Nasıl Bulaşır?**
  - ✓ Adware, genellikle ücretsiz yazılımların veya uygulamaların içine gizlenmiş olarak gelir. Kullanıcılar bu yazılımları indirip kurduğunda adware de sisteme bulaşır.
  - ✓ Bazı web siteleri, zararlı pop-up reklamlar aracılığıyla da adware bulaştırabilir.

ADWARE ÖRNEKLERİ

- Superfish
- MyWebSearch
- Conduit Toolbar
- Genieo

TROJAN(TRUVA ATI)

- Trojan(Truva Atı), görünüşte zararlı veya yararlı bir program veya dosya gibi davranarak, kullanıcının bilgisayarına kötü amaçlı yazılım bulaştırmak için tasarlanmış bir tür zararlı yazılımdır.
- Görünüşte zararsız bir program veya dosya gibi davranır, bu nedenle kullanıcılar tarafından kolayca kurulabilir.
- Amaçları, bilgisayara kötü amaçlı yazılım, casus yazılım veya diğer zararlı işlevleri yüklemektir.

TROJAN(TRUVA ATI)

- **Nasıl Bulaşır?**
  - ✓ Trojanlar, genellikle bilgisayar kullanıcılarına güvenilir ve çekici görünen e-posta ekleri, indirilebilir dosyalar veya uygulamalar aracılığıyla bulaştırılır.
  - ✓ Kullanıcılar, bu dosyaları veya uygulamaları indirip açtıklarında Trojan bilgisayarlarına bulaşır.

BOTNET

- Bot terimi robotun kısaltmasıdır.
- Amacı, bilgisayarınızı bir bot'a(zombi olarak ta bilinir) çevirebilen kötü amaçlı yazılımları dağıtmaktır. Böyle bir durumda bilgisayarınız, sizin haberiniz olmadan internet üzerinden otomatik görevleri gerçekleştirebilir.

BOTNET

- **Nasıl Bulaşır?**
  - ✓ Botnetler, bilgisayarlara veya cihazlara bulaşmak için genellikle kötü amaçlı e-posta ekleri, bulaşmış web siteleri, güvensiz uygulamalar veya diğer kötü niyetli yazılımlar aracılığıyla yayılırlar.
  - ✓ Kullanıcılar, bu bulaşmış dosyaları veya bağlantıları açtıklarında botnet bilgisayarlarına bulaşabilir.

RANSOMWARE(FİDYE YAZILIMI)

- Ransomware, kötü amaçlı bir yazılım türüdür ve adını rehine verileri fidye karşılığında serbest bırakma eyleminden alır.
- Ransomware, dosyaları veya bilgisayarın tamamını şifreleyerek kullanıcının erişimini engeller.
- **Nasıl Bulaşır?**
  - ✓ Ransomware, genellikle sahte e-posta ekleri, kötü amaçlı web siteleri, güvensiz indirme kaynakları veya açıkları kullanarak bilgisayarlar bulaşır.
  - ✓ Kullanıcılar, kötü amaçlı dosyaları veya bağlantıları açtıklarında ransomware bulaşabilir.

RANSOMWARE ÖRNEKLERİ

- WannaCry
- Locky
- CryptoLocker
- Ryuk
- NotPetya(Petya/ExPetr)

BUFFER OVERFLOW

- Bir programın bellek alanının sınırlarının dışına çıkılarak kötü amaçlı kodların çalıştırılmasına izin veren bir güvenlik açığıdır. Zararlı yazılım türü değil saldırı türlerine bir örnektir.
- Örnek: Morris Worm, buffer overflow açığı kullanarak ilk büyük çaplı internet saldırısını gerçekleştirmiştir.

CROSS-SITE REQUEST FORGERY(CSRF)

- Saldırganların kullanıcıların hesaplarını izinsiz olarak farklı bir web sitesi üzerinden işlem yapmaya zorladığı bir saldırı türü
- Örnek: Bir saldırgan, kullanıcının banka hesabından para transferi yapmasını isteyen sahte bir web sayfası oluşturabilir.

CROSS-SITE SSCRIPTING(XSS)

- Saldırganların web sitelerine zararlı kodlar ekleyerek kullanıcıların tarayıcılarında çalışmasını sağladığı bir saldırı türü.
- Örnek: Bir saldırgan, kullanıcılara zararlı bir JavaScript kodu içeren sahte bir e-posta gönderebilir.

BROKEN ACCESS CONTROL

- Kullanıcıların izin verilmeyen kaynaklara veya işlevlere erişim sağlamasına izin veren bir güvenlik açığıdır.
- Örnek: Bir kullanıcının hesap ayarlarını değiştirmesi gereken bir işlevin, yetkisiz erişime açık olması.

ZERO-DAY EXPLOITS(0 DAYS)

- Yazılım veya sistem güvenlik açıklarının keşfedildiği ve henüz üretici tarafından düzeltilmediği durumlar.
- Örnek: Saldırganlar, henüz açığı kapatılmamış bir yazılım veya işletim sistemi güvenlik açığından faydalanabilirler.

PORT CONFIGURATION HATALARI

- Ağ cihazlarının yanlış yapılandırılması sonucu ağ güvenliğinin tehlikeye girmesi.
- Örnek: Açık bir ağ bağlantısı, yetkisiz erişimlere yol açabilir.

RAT(REMOTE ACCESS TROJAN)

- Saldırganların bir bilgisayar sistemine uzaktan erişim sağlamak amacıyla kullanılan truva atları.
- Örnek: Poison Ivy RAT, uzaktan bilgisayar kontrolü sağlayan bir RAT örneğidir.

MAN-IN-THE-MIDDLE(MITM) SALDIRILARI

- Saldırganların iki iletişim halinde ki tarafın arasına girerek iletileri izlemesine veya manipüle etmesine olanak tanıyan saldırı türü.
- Örnek: Bir kişi, halka açık bir Wi-Fi ağı üzerinden verileri izleyebilir veya değiştirebilir.

DENIAL OF SERVICE(DOS) SALDIRILARI

- Hedeflenen sistem veya ağa yoğun talep gönderilerek hizmetin kesilmesine neden olan saldırılar.
- Örnek: SYN Flood saldırısı, bir sunucunun hizmet veremeyecek kadar çok bağlantı istediği aldığı bir tür DOS saldırısıdır.

ÖNEMLİ PORT NUMARALARI

- 21: FTP(File Transfer Protocol)
- 22: SSH(Secure Shell)
- 23: TELNET
- 25: SMTP(Simple Mail Transfer Protocol)
- 53: DNS
- 80: HTTP
- 110: POP3
- 115: SFTP
- 139: NetBIOS

ÖNEMLİ PORT NUMARALARI

- 389: LDAP
- 443: SSL
- 444: SNPP
- 1194: OpenVPN
- 1433: SQL
- 1521: Oracle
- 27017: MongoDB
- 3306: MySQL
- 5432: PostgreSQL