SAKARYA ÜNİVERSİTESİ

SİBER GÜVENLİĞE GİRİŞ

SİBER GÜVENLİK TEMEL KAVRAMLARI

Prof. Dr. İbrahim ÖZÇELİK
Bilgisayar ve Bilişim Bilimleri Fakültesi

1

İÇERİK

- Siber Uzay
- Güvenlik Prensipleri (CIA, AAA)
- Siber Güvenlik ve Bilgi Güvenliği
  - Bilgi Güvenliği Zafiyet ve Tehditleri
  - Siber Güvenlik Zafiyet ve Tehditleri
- Siber Tehditler ve SoC
  - Teknoloji – İnsan – Süreç Yaklaşımı
  - SoC Kabiliyetleri

2

Siber Uzay

- Kara
- Deniz
- Hava
- Uzay
- Siber Uzay
  - İletişim halindeki tüm varlıkların oluşturduğu elektronik ortama «Siber Uzay» denir

3

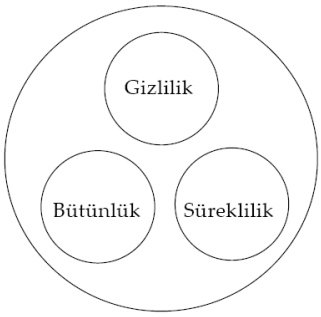
Varlıklar (Assets)

- İnsanlar (personel, müşteriler, tedarikçiler,…)
- Bilgi (kağıt ve elektronik ortam)
- Yazılım varlıkları
- Fiziksel varlıklar (bilgisayar, sunucular, ağ cihazları, PLC, IED, …)
- Hizmetler (bilişim, ısıtma, havalandırma…)
- Kurum imajı ve itibarı

4

Güvenlik Prensipleri - CIA

- **Gizlilik (Confidentiality):** Bilginin yetkisiz kişilerin eline geçmesini engellemektir. Bunu sağlamak için şifreleme yöntemleri kullanılır.
- **Bütünlük (Integrity):** Veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bunun için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar kullanılır.
- **Erişebilirlik (Availability):** Sistemleri, kurum içinden ve dışından gelebilecek tehditlere karşı korumaktır. Bunun için yedek sistemler, bakım, yedekleme, alternatif haberleşme kanalları kullanılır.



5

Güvenlik Prensipleri (Ek)

- **Kimlik Doğrulaması (Authentication):** Alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun için özetleme algoritmaları, mesaj özetleri, sayısal (elektronik) imzalar, sertifikalar kullanılır.
- **Yetkilendirme (Authorization):** Erişim kontrolü ile ilgili kaynaklara erişim haklarını / ayrıcalıklarını belirleme işlevidir.
- **İzlenebilirlik (Accountability):** Sistemde gerçekleşen olayları, daha sonra analiz etmek üzere kayıt altına almaktır.

6

Siber Güvenlik ve Bilgi Güvenliği

- Korunması gereken bilgi varlıkları aynı
- Tehdit ve zafiyet/açıklıkları farklı
- Siber Güvenlik, Bilgi Güvenliği'nde söz konusu olan tehdit ve açıklıkların bir alt kümesi ile ilgilenir.

7

Bilgi Güvenliği Zafiyet ve Tehditleri

Açıklık	Açıklığı kullanabilecek tehdit
Dokümanların kontrolsüz çoğaltılması	Hırsızlık
Yedek alınmaması	Zararlı yazılımlar, yangın
Saklama ortamlarının doğru silinmemesi ve imha edilmemesi	Yetkisiz erişim
Yazılım gereksinimlerinin yanlış veya eksik belirlenmesi	Yazılım hataları
Yazılımların yeterince test edilmemesi	Yazılım hataları, yetkisiz erişim, yazılımların yetkisiz kullanımı
Dokümantasyon eksikliği/yetersizliği	Kullanıcı hataları
Yama yönetimi eksikliği/yetersizliği	Yetkisiz erişim
İzinsiz yazılım yüklenmesi ve kullanılması	Zararlı yazılımlar, yasal gereksinimlere uyumsuzluk
Periyodik bakım eksikliği	Donanım arızaları, tozlanma, nem vb. çevresel etkiler
Voltaj değişikliklerine, ısıya, neme, toza duyarlılık	Güç dalgalanmaları, erişim güçlükleri vs.
Değişim yönetimi eksikliği	Kullanıcı hataları
Depreme dayanıksız yapılar	Deprem
Sel baskınına maruz kalabilecek bölgede konuşlanma	Sel
Korunmayan haberleşme hatları	Haberleşmenin dinlenmesi
Hat üzerinden şifrelerin açık olarak iletilmesi	Yetkisiz erişim, başkalarının kimliğine bürünme
Hassas verinin açık olarak iletilmesi	Haberleşmenin dinlenmesi
Mesaj alma/gönderme kayıtlarının bulunmaması	İnkâr etme
Personel yetersizliği	Kullanıcı hataları, işletim hataları
Eğitim ve bilinç eksikliği	Personel hataları
Bilgi güvenliği politikalarının eksikliği / yetersizliği	Yetkisiz erişim, hırsızlık, kasıtlı zarar verme

8

Siber Güvenlik Zafiyet ve Tehditleri

Açıklık/Zafiyet Kaynakları: Varlıklardaki kusurlar

- Yazılım veya donanımsal üretim hatalarından kaynaklı
- Topoloji kaynaklı
- Zayıf güvenlik politikalarından kaynaklı
- Olası tehditlerin yetersiz bilgilendirmesinden kaynaklı
- Protokol zayıflıklarından kaynaklı
- Portların zayıflıklarından kaynaklı
- Yazılım yapılandırması kaynaklı

Siber Tehditler/Saldırılar: Zarar veren etkenler

- DDoS-Servis dışı bırakma saldırıları
- Malware-Zararlı yazılım saldırıları
- Botnets-Zombi makinalar
- Ransomware-Fidye zararlıları
- Spyware-Casus yazılımlar
- Phishing-Oltalama
- Worms-Solucanlar
- Backdoors-Arka kapı
- APT-Hedef odaklı saldırılar

9

Siber Tehdit Özellikleri

- Siber Uzayda herhangi coğrafi konumdan herhangi bir saatte saldırı şansı
- Saldırı için düşük maliyet (Bilgisayar + İnternet)
- Taşeron kullanma şansı (Kiralık Botnet, Birkaç 10 USD/Onlarca bot)

10

Siber Tehditlerin Hedefleri

- Bilgi Sistemleri ve Kritik Ulusal Altyapılar
  - Finans
  - Ulaştırma
  - Telekomünikasyon
  - Enerji
  - Su Yönetimi
- Sık sık güncellenmeyen sistemler
- Değer ifade eden sektörler
- Ülkenin kritik sektörlerine ait know-how (Savunma Sanayi)
- Ulusal güvenliğe ait kritik bilgiler (Sağlık verileri, kritik ekonomik veriler)
- Mobil Uygulamalar ve Gömülü Sistemler
- …

11

Varlık, Zafiyet, Tehdit, Risk

Varlıklar (Sahibi, Değeri ve Konumu)
- İnsanlar (personel, müşteriler, tedarikçiler,..)
- Bilgi (kağıt ve elektronik ortamdaki)
- Yazılım varlıkları
- Fiziksel varlıklar (bilgisayar, sunucular, ağ cihazla
- Hizmetler (bilişim, ısıtma, havalandırma..)
- Kurum imajı ve itibarı

Açıklık/Zafiyet Kaynakları: Varlıklardaki kusurlar
- Yazılım veya donanımsal üretim hatalarından kaynak
- Topoloji kaynaklı
- Zayıf güvenlik politikalarından kaynaklı
- Olası tehditlerin yetersiz bilgilendirmesinden kaynakl
- Protokol zayıflıklarından kaynaklı
- Portların zayıflıklarından kaynaklı
- Yazılım yapılandırması kaynaklı

Siber Tehditler/Saldırılar: Zarar veren etkenler
- DDoS-Servis dışı bırakma saldırıları
- Malware-Zararlı yazılım saldırıları
  - Botnets-Zombi makinalar
  - Ransomware-Fidye zararlıları
  - Spyware-Casus yazılımlar
    - Phishing-Oltalama
    - Worms-Solucanlar
    - Backdoors-Arka kapı
  - APT-Hedef odaklı saldırılar

Risk: Varlık üzerindeki bir açıklığın bir tehdit tarafından kullanılmasına bağlı zarar beklentisidir

Risk = f (Varlık, Açıklık, Tehdit)

12

Siber Tehditler ve SOC

- Siber saldırıların/tehditlerin tespit edilmesinin zorlaşması
  - Siber saldırıların / tehditlerin gün geçtikçe karmaşıklaşması,
  - Hedef odaklı yapılan siber saldırıların, özellikle Gelişmiş Israrcı Tehdit (Advanced Persistent Threat, APT)'lerin teknik ve taktiklerin sürekli değişmesi,
  - Yeni teknik ve taktiklerin ortaya çıkması
  - Saldırganların sisteme ilk sızma anı ile sızıntının tespit anı arasında geçen ortalama sürenin 146 gün olması [Fireeye araştırma raporu]
- Global tehditlerin vakaya dönüşme oranı
  - Zararlı yazılım bulaşma oranı
  - Hedef odaklı atakların oranı
- Güvenlik Ürünü Yetersizliği
  - Her firmada aynı kapsayıcılıkta ya da yeterlilikte güvenlik ürünü bulunmamakta,
- Yetişmiş İnsan Gücüne Olan İhtiyaç
  - Güvenlik ürünlerine tekil bir şekilde bakmak ya da incelemek yeterli gelmemekte
  - Teknolojilerin hem bir süreçle hem de yetişmiş insan profiliyle birlikte değerlendirilmesi gerekmekte

13

Siber Güvenlik Operasyon Merkezi, SOC

- Bütüncül ve tamamlayıcı teknoloji yaklaşımı ile
- Tanımlı ve etkin süreçlerle ve
- Siber saldırganlar gibi birikime sahip konusunda uzmanlaşmış kişilerle
- Yukarıdaki riskleri minimize etme ya da herhangi bir saldırı durumunda hızlı bir şekilde geri dönüşü yapabilme

14

Teknoloji – İnsan – Süreç Yaklaşımı

- Teknoloji:
  - Ağ, sunucu ve istemci güvenliğinin sağlanması, Güvenlik Bilgi ve Olay Yönetimi (SIEM), tehdit istihbaratı, saldırı tespit/önleme sistemi, gelecek nesil güvenlik duvarları, vb.
- İnsan:
  - Siber operasyonlar özel yetenekler gerektirmektedir.
  - İnsan bu operasyonlarda genellikle en zayıf halka durumunda kalır.
  - Bu eksikliği ortadan kaldırmak için insana teknoloji kadar önem gösterilmesi ve yatırım yapılması gerekir.
  - SGOM analist ve operatörlerin (SGOM takımının) iyi eğitimli ve yetenekli olması tercih edilir
  - Sürekli eğitim, kurs, sertifika, üyelikler, vb. araçlarla yatırım yapılır.
  - SGOM içerisinde insan sayısı, niteliği, verimi ve vardiyası ile alakalı çalışmaların ve planlamaların yapılması gerekmektedir.
- Süreç:
  - Planlı çalışmaların yapılması gerekmekte ve bu çalışmaların da başarılı olabilmesi için **bir süreç** içerisinde değerlendirilmesi gerekmektedir.
  - Zafiyet yönetimi, vaka yönetimi, risk yönetimi, standartlara ve regülasyonlara uyumluluk gibi konular SGOM içerisinde yürütülmesi gereken süreçlere örnek olarak verilebilir.

15

Teknoloji – İnsan – Süreç Yaklaşımı

Süreçler

- Servis Yönetimi Süreçleri
- Zafiyet Yönetim Süreçleri
- Risk Yönetimi Süreçleri
- Güvenli İzleme Süreçleri
- Vaka Araştırması ve Cevap Verme Süreçleri
- Log Yönetimi Süreçleri
- Analiz ve Raporlama Süreçleri
- İhlal Keşfi ve İyileştirme Süreçleri

İnsan

- Güvenlik Analistleri
- Güvenlik Araştırmacıları
- Güvenlik Yöneticileri
- …..

Teknolojiler

- Log Yönetimi ve SIEM
- Zafiyet Değerlendirme
- Tehdit İstihbaratı
- Uç Nokta Tehdit Algılama ve Yanıt
- Güvenlik Orkestrasyon ve Yanıt
- Güvenlik Analitiği
- ….

16

SOC Kabiliyetleri

- Gartner Adaptif Güvenlik Mimari modeline göre SGOM dört farklı yeteneği:
  - Tahmin (Predict):
    - Güncel tehditlerin farkında olma,
    - Bu tehditleri kullanabilecek atakları öngörme
    - Proaktif maruz kalma analizleri yapabilme.
  - Koruma (Prevent): Siber saldırılardan korunmak amacıyla;
    - Sistemleri izole etme,
    - Sıkılaştırma (hardening),
    - Saldırganları yönlendirme ve vakaları önleme.
  - Tespit (Detect): Sisteme girmeyi başaran bir saldırganın
    - Varlığını tespit etme,
    - Risklerini belirleme,
    - Önceliklendirme yapabilme.
  - Müdahale (Respond):
    - Siber saldırıyı tespit sonrası vakaya doğru ve zamanında müdahale edebilme,
    - Sistemleri güvenli hale getirecek değişiklikleri yaparak geri dönüşü sağlama

17