CYBER KILL CHAIN

HAZIRLAYAN: MURAT GÜRSOY
TARİH: 29/01/2025

İçindekiler

Giriş

Siber güvenlik dünyasında saldırganların sistemlere sızma süreçlerini anlamak, savunma stratejileri geliştirmek için kritik bir gerekliliktir. Lockheed Martin tarafından geliştirilen **Cyber Kill Chain** modeli, siber saldırıların belirli aşamalardan oluştuğunu gösteren bir yapıdır. Bu model, saldırganların gerçekleştirdiği adımları analiz ederek, siber güvenlik uzmanlarının erken müdahale etmesini sağlar.

Cyber Kill Chain Nedir?

Cyber Kill Chain, siber saldırı süreçlerini adım adım analiz eden ve her aşamaya uygun savunma önlemleri belirlemeye yardımcı olan bir çerçevedir. Bu model, **saldırganların yöntemlerini ve stratejilerini belirleyerek savunma mekanizmalarının güçlendirilmesini sağlar**. Bu sayede organizasyonlar, saldırıları daha erken tespit edebilir ve etkisini en aza indirebilir.

Cyber Kill Chain Aşamaları

Cyber Kill Chain modeli yedi ana aşamadan oluşur:

1. Keşif (Reconnaissance)

Bu aşamada saldırganlar, hedef sistem veya kuruluş hakkında bilgi toplar. Açık kaynak araştırmaları (**OSINT**), phishing saldırıları ve sosyal mühendislik teknikleri kullanılarak sistemdeki zafiyetler belirlenmeye çalışılır.

- **Saldırı Yöntemleri:**
    - Sosyal medya ve açık kaynaklardan bilgi toplama (**OSINT**).
    - E-posta veya sahte web siteleri ile **phishing** saldırıları düzenleme.
    - Ağ taramaları ve güvenlik açıklarını keşfetme.
- **Savunma Stratejileri:**
    - Ağ trafiği izleme ve anomali tespiti.
    - Çalışanların siber güvenlik farkındalığını artırma.
    - Hassas bilgilerin açık kaynaklardan kaldırılması.

2. Silahlandırma (Weaponization)

Saldırgan, topladığı bilgilere dayanarak zararlı yazılımlar veya kötü amaçlı komut dosyaları hazırlar.

- **Saldırı Yöntemleri:**
    - **Zero-day açıklarını** kullanarak özel zararlı yazılım geliştirme.
    - Kimlik avı saldırıları için özel olarak hazırlanmış kötü amaçlı ekler oluşturma.
- **Savunma Stratejileri:**
    - **Tehdit istihbaratı** analizi.

- Güvenli yazılım geliştirme.
- Zararlı yazılım analiz araçlarının kullanımı.

3. Teslimat (Delivery)

Saldırgan, zararlı yazılımı hedefe ulaştırır.

- **Saldırı Yöntemleri:**
  - **Phishing** e-postaları ve kötü amaçlı ekler gönderme.
  - USB bellekler üzerinden zararlı yazılım yayma.
  - Web sitelerine zararlı kod yerleştirme (**Drive-by Download**).
- **Savunma Stratejileri:**
  - E-posta filtreleme ve phishing tespiti.
  - USB ve harici cihaz kullanım kısıtlamaları.

4. Sömürme (Exploitation)

Saldırgan, hedef sistemdeki bir güvenlik açığını kullanarak zararlı yazılımı çalıştırır.

- **Saldırı Yöntemleri:**
  - İşletim sistemlerindeki veya yazılımlardaki güvenlik açıklarını kullanma.
- **Savunma Stratejileri:**
  - Güncel **yama ve güvenlik güncellemelerinin** uygulanması.
  - Güvenlik duvarı ve antivirüs sistemlerinin aktif kullanımı.

5. Kurulum (Installation)

Saldırgan, zararlı yazılımı sisteme yerleştirerek saldırının devamlılığını sağlar.

- **Saldırı Yöntemleri:**
  - **Rootkit** veya **Trojan** yükleyerek sistem üzerinde kalıcılık sağlama.
- **Savunma Stratejileri:**
  - Davranışsal analiz tabanlı güvenlik sistemleri kullanma.

6. Komuta ve Kontrol (C2 - Command & Control)

Saldırgan, ele geçirilen sisteme uzaktan erişim sağlar.

- **Saldırı Yöntemleri:**
  - Zararlı yazılımın saldırganın kontrol sunucusuna bağlanmasını sağlama.
- **Savunma Stratejileri:**
  - Ağ trafiği analizi ve şüpheli bağlantıların engellenmesi.

7. Hedefe Yönelik Eylem (Actions on Objectives)

Bu aşamada saldırgan, sistemi kullanarak nihai hedefini gerçekleştirir.

- **Saldırı Yöntemleri:**
    - Hassas verileri çalarak ticari veya finansal avantaj sağlama.
    - Fidye yazılımları (**Ransomware**) kullanarak dosyaları şifreleme.
- **Savunma Stratejileri:**
    - **Veri şifreleme** ve **yedekleme sistemlerinin** düzenli test edilmesi.

Cyber Kill Chain Modelinin Önemi

Cyber Kill Chain modeli, saldırıların **önceden tespit edilmesini ve durdurulmasını** sağlar. Güvenlik ekipleri, bu model sayesinde saldırının hangi aşamada olduğunu anlayarak, savunma mekanizmalarını etkin hale getirebilir.

Sonuç

Siber saldırılar giderek daha sofistike hale gelmektedir. Cyber Kill Chain modeli, güvenlik uzmanlarının **saldırı zincirini kırmasına** yardımcı olur. Gelecekte, **yapay zekâ ve otomatikleştirilmiş güvenlik sistemleri** bu süreci daha da güçlendirecektir.

Kaynakça

1. https://www.defenceturk.net/gelismis-siber-saldirinin-7-evresi-siber-olum-zinciri-cyber-kill-chain
2. https://ozdenercin.com/2019/08/16/endustriyel-kontrol-sistemlerinde-siber-olum-zinciri-cyber-kill-chain/
3. https://www.nist.gov/cyberframework