CYBER KILL CHAIN

07 ŞUBAT 2025

HAZIRLAYAN: ALİ BERK CENGİZ

İçindekiler

GİRİŞ

Siber güvenlik tarafında, organizasyonların karşılaştığı tehditler her geçen gün daha karmaşık hale gelmektedir. Bu tehditlerin karşısında etkin bir savunma oluşturmak için, saldırıların nasıl ve hangi aşamalarda gerçekleştirildiğini anlamak çok büyük öneme sahiptir. İşte bu noktada, Cyber Kill Chain modeli devreye girer. 2011 yılında Lockheed Martin tarafından geliştirilen bu model, bir siber saldırının aşamalarını sistematik bir şekilde tanımlar ve bu aşamaların her birinde savunma stratejileri geliştirilmesine yardımcı olur.

CYBER KILL CHAIN

Cyber Kill Chain, siber saldırganların hedefe ulaşmadan önce geçtikleri çeşitli aşamaları tanımlar. Bu aşamalar, saldırının önlenmesi veya tespit edilmesi için kritik noktalar sağlar.

1. Reconnaissance: Saldırganın hedefi belirlemek ve zayıf noktaları tespit etmek için bilgi topladığı ilk aşamadır. Hedefin ağ yapısı, yazılımlar ve kullanıcı davranışları hakkında veri toplanır.
2. Weaponization: Saldırgan, keşif aşamasında elde ettiği zayıf noktaları kullanarak, hedefi etkisiz hale getirecek araçlar ve teknikler geliştirir. Bu genellikle malware ve exploit kullanımıyla yapılır.
3. Delivery: Saldırgan, oluşturduğu zararlı yazılımı hedefe iletmek için çeşitli yollar kullanır.
4. Exploitation Sömürme: Teslim edilen zararlı yazılım hedefin zayıf noktalarını kullanarak devreye girer. Bu aşama, sistemin kontrolünü ele geçirmek için kritik bir adımdır.
5. Installation: Zararlı yazılım, hedef sistemde kalıcı hale gelir ve saldırganın geri erişim sağlamak için kullanacağı arka kapıları yerleştirir.
6. Command and Control: Saldırgan, hedef sistemle iletişim kurarak uzaktan kontrol sağlamak amacıyla komutlar gönderir. Bu aşamada, saldırgan hedefteki sistem üzerinde tam kontrol sağlar.
7. Actions on Objectives: Saldırgan, hedef sistem üzerinde belirlediği nihai amaca ulaşır. Bu aşama, verilerin çalınması, sistemin bozulması veya hizmetlerin engellenmesi gibi sonuçlara yol açabilir.

Savunma Yöntemleri

Cyber Kill Chain modeli, her bir aşama için savunma stratejileri geliştirilmesini önerir. Bu stratejiler, saldırganların her adımda yakalanmasını veya engellenmesini sağlamayı hedefler.

- Keşif aşaması: Ağ izleme ve davranışsal analizler ile saldırganların hedef tespiti yapmalarına engel olunabilir.
- Silahlandırma ve teslimat aşamaları: E-posta filtreleme, zararlı yazılım tespiti ve güvenlik duvarı kullanımı saldırıların önlenmesinde etkilidir.
- Sömürme ve kurulum aşamaları: Yazılım güncellemeleri, yamalar ve güvenlik protokolleri ile sistemin savunması artırılabilir.
- Komut ve kontrol aşaması: Trafik analizleri ve ağ güvenliği çözümleri, saldırganın uzaktan kontrol sağlamasını engelleyebilir.

SONUÇ

Cyber Kill Chain, siber saldırıların karmaşık yapısını anlamak ve bu saldırılara karşı etkili savunma mekanizmaları geliştirmek için önemlidir. Kurumlar, bu modeli kullanarak saldırıların her aşamasında uygulanabilecek savunma stratejileri geliştirebilir ve siber güvenlik postürlerini güçlendirebilir. Siber tehditlerin sürekli evrim geçirdiği dünyada, Cyber Kill Chain gibi modeller, siber güvenlik uzmanları için vazgeçilmez bir araç haline gelmiştir.

Kaynakça

1. Lockheed Martin. (2011). "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains."
2. Symantec. (2020). "Understanding the Cyber Kill Chain."
3. MITRE ATT&CK Framework. (2023). "Tactics, Techniques, and Procedures (TTPs)."