CYBER KİLL CHAİN

İREM GÜZEL
07.02.2025

İçindekiler

Giriş

Bu raporun amacı, Cyber Kill Chain modelini detaylı bir şekilde incelemek ve modelin aşamalarında alınabilecek güvenlik önlemlerini açıklamaktır. Aynı zamanda, SOC ekiplerinin olayları tespit etme ve müdahalede bu modelin bir rehber olarak kullanılabileceğini , siber güvenlik farkındalığını artırmayı ve güvenlik olaylarının daha etkin şekilde analiz edilmesini sağlamayı hedeflemektedir.

Cyber Kill Chain Aşamaları

Reconnaissance (Keşif)

İlk aşama olan "Keşif", saldırganın hedef hakkında bilgi toplama sürecidir. Saldırgan, potansiyel zafiyetleri, hedefin güvenlik önlemlerini ve diğer kritik bilgileri belirlemek için aktif veya pasif yöntemlerle hedefi analiz eder.

- Pasif Bilgi Toplama: Hedef ile direkt olarak temasa geçilmeden bilgi toplama çeşitidir.
- Aktif Bilgi Toplama: Hedef ile direkt olarak temasa geçilen bilgi toplama çeşitidir.

Cyber Kill Chain in ilk aşamasını oluşturan bu kısımda saldırganların bilgi toplamasını zorlaştırmak için bazı önlemler alabiliriz. Örneğin; çalışanların bilinçlendirilmesi, şirket bilgilerinin gereksiz şekilde ifşa edilmemesi, IPS-IDS sistemleri kullanılarak yetkisiz taramaların engellenmesi,..

Weaponization (Silahlandırma)

"Silahlanma" aşamasında saldırgan, hedefe karşı kullanmak üzere kötü amaçlı yazılımları geliştirir ve istismarlar oluşturur. Bu aşama, saldırganın teknik yeteneklerini kullanarak etkili bir saldırı aracı oluşturduğu kritik bir noktadır. Örnek olarak

- Virüsler,
- Truva atları
- Solucanlar
- Sıfır Gün Saldırıları

gibi çeşitli kötü amaçlı yazılım türleri söylenebilir.

Delivery (Teslimat)

"Ulaştırma" aşamasında saldırganlar, oluşturdukları saldırı aracını veya kötü amaçlı yazılımı hedefe ulaştırmak için çeşitli yollar deneler. Örnek olarak,

- Phishing e-postaları
- Zararlı bağlantılar
- USB cihazları

Bunu önlemek amacıyla çalışanların bilinçlendirilmesi, spam filtrelerinin kullanılması ve e-postalardaki bağlantıların kontrol edilmesi önemlidir. Zararlı bağlantılara karşı, güncel antivirüs yazılımları ve güvenli tarayıcı ayarları kullanılmalı, bilinmeyen linkler açılmamalıdır. USB cihazlarına karşı ise bilinmeyen aygıtların kullanılmaması, antivirüs ile tarama yapılması ve hassas verilerin şifrelenmesi gibi önlemler alınmalıdır.

Exploitation (İstismar)

Oluşturulan zararlı ve belirlenen atak vektörünü kullanarak hedefin zafiyetinin sömürüldüğü aşamadır. Exploit hazırlanıp hedefe iletildikten sonra bu aşamada zararlı kod çalıştırılır. Bunu önlemek amacıyla yazılımlar ne sıklıkla güncellendiği , sistemdeki zafiyetlerin tespit edilmesi için güvenlik denetimleri yapılıp yapılmadığı kontrol edilebilir.

Installation (Kurulum)

Hedefin sömürülmesi ardından, kalıcı bir tehdit haline gelmek, güvenlik sisteminin ötesinde sistem başarılı bir şekilde kontrol edilebilmesi için hedefe asıl zararlı yazılımın indirilmesi, zararlı yazılımın sistemde kalacağı süreyi mümkün olduğunca arttırmayı hedefleyen aşamadır. Sistemde çalışan bilgisayarlarla yüklenen yazılımların denetlenmesi, kullanıcıların istedikleri yazılımları bilgisayarlara yükleyebilirlikleri, whitelisting ve blacklisting oluşturma bu aşamayı önleyebilir.

Command & Control (Komuta ve Kontrol- C2)

Komuta ve kontrol aşamasında artık hedef sistem ele geçirilmiştir. Zararlı kodlar ağa yerleştirilmiştir. Saldırgan hedef sistemde bir haberleşme kanalı açar ve her türlü erişime açık hale gelir.

Actions on Objectives (Hedefteki Eylemler)

Ve son aşamada artık saldırgan hedeflediği işlemleri sistem üzerinde gerçekleştirmeye başlar. Burada kritik verileri çalma, değiştirme, silme gibi amacı olan eylemleri gerçekleştirir.

Sonuç

Cyber Kill Chain modeli, siber saldırıları anlama ve engelleme konusunda kritik bir öneme sahiptir. Bu rapor, kurumların ve bireylerin siber güvenlik risklerini azaltmalarına ve dijital varlıklarını korumalarına yardımcı olmayı amaçlamaktadır.

Kaynakça

https://chat.openai.com/

https://myarchieve.net/the-cyber-kill-chain-stages/#teslimat-a%c5%9famas%c4%b1

https://bbsteknoloji.com/cyber-kill-chain-nedir/

https://cizgiotesi.info/bilim-teknoloji/siber-saldiri-asamalari-siber-olum-zinciri-cyber-kill-chain/

https://www.gaissecurity.com/blog/cyber-kill-chain-bir-siber-saldirinin-yasam-dongusu