



Siedem etapów Cyber Kill Chain

3
1. Rozpoznanie
(Reconnaissance)

3
3. Dostarczenie
(Delivery)

2
5. Instalacja
(Installation)

2
7. Działania końcowe
(Actions on Objectives)

3
2. Uzbrojenie
(Weaponization)

2
4. Eksploatacja
(Exploitation)

3
6. Kontrola i dowodzenie
(Command and Control)



Zbieranie informacji o potencjalnym celu.

Identyfikowanie słabości i infrastruktury
obronnej.

Narzędzia wykorzystywane do rozpoznania to
m.in. skanery sieci i analizy publicznych danych.

1. Rozpoznanie (Reconnaissance)



2. Uzbrojenie (Weaponization)

Tworzenie złośliwego oprogramowania, które będzie wykorzystywane w ataku.

Kompletowanie narzędzi niezbędnych do zainfekowania systemu ofiary.

W tym kroku tworzona jest tzw. „broń” – złośliwy plik lub program, który zostanie wykorzystany w dalszych krokach.



Przesłanie złośliwego oprogramowania do docelowego systemu.

Może to być realizowane poprzez e-mail (phishing), odwiedzanie zainfekowanej strony internetowej, czy też za pomocą zainfekowanego nośnika.

To moment, w którym złośliwy kod trafia bezpośrednio do ofiary.

3. Dostarczenie (Delivery)



4. Eksploatacja (Exploitation)

Wykorzystanie słabości w systemie lub aplikacji ofiary w celu aktywacji złośliwego oprogramowania.

W tym momencie kod uzyskuje kontrolę nad częścią systemu.



Zainstalowanie złośliwego oprogramowania w systemie docelowym, aby zapewnić napastnikom długoterminowy dostęp.

Może obejmować rootkity, trojany czy keyloggery, które umożliwiają utrzymanie kontroli.

5. Instalacja (Installation)



6. Kontrola i dowodzenie (Command and Control)

Nawiązanie komunikacji między atakującym a zainfekowanym systemem.

Umożliwia zdalne sterowanie systemem ofiary i dostosowywanie działań.

Wykorzystywane są tu protokoły, które często przypominają normalny ruch sieciowy, co utrudnia ich wykrycie.



Realizacja celów ataku, takich jak kradzież danych, szyfrowanie plików (ransomware), sabotaż lub usunięcie śladów.

Ostateczne działania napastnika mają na celu maksymalne wykorzystanie uzyskanego dostępu do zasobów.

7. Działania końcowe (Actions on Objectives)



Siedem etapów Cyber Kill Chain

Zbieranie informacji o potencjalnym celu.

Identyfikowanie słabości i infrastruktury obronnej.

Narzędzia wykorzystywane do rozpoznania to m.in. skanery sieci i analizy publicznych danych.

1. Rozpoznanie (Reconnaissance)

Przesłanie złośliwego oprogramowania do docelowego systemu.

Może to być realizowane poprzez e-mail (phishing), odwiedzanie zainfekowanej strony internetowej, czy też za pomocą zainfekowanego nośnika.

To moment, w którym złośliwy kod trafia bezpośrednio do ofiary.

3. Dostarczenie (Delivery)

Zainstalowanie złośliwego oprogramowania w systemie docelowym, aby zapewnić napastnikom długoterminowy dostęp.

Może obejmować rootkity, trojany czy keyloggers, które umożliwiają utrzymanie kontroli.

5. Instalacja (Installation)

Realizacja celów ataku, takich jak kradzież danych, szyfrowanie plików (ransomware), sabotaż lub usunięcie śladów.

Ostateczne działania napastnika mają na celu maksymalne wykorzystanie uzyskanego dostępu do zasobów.

7. Działania końcowe (Actions on Objectives)

Tworzenie złośliwego oprogramowania, które będzie wykorzystywane w ataku.

Kompletowanie narzędzi niezbędnych do zainfekowania systemu ofiary.

W tym kroku tworzona jest tzw. „broń” – złośliwy plik lub program, który zostanie wykorzystany w dalszych krokach.

2. Uzbrojenie (Weaponization)

Wykorzystanie słabości w systemie lub aplikacji ofiary w celu aktywacji złośliwego oprogramowania.

W tym momencie kod uzyskuje kontrolę nad częścią systemu.

4. Eksploatacja (Exploitation)

Nawiązanie komunikacji między atakującym a zainfekowanym systemem.

Umożliwia zdalne sterowanie systemem ofiary i dostosowywanie działań.

6. Kontrola i dowodzenie (Command and Control)

Wykorzystywane są tu protokoły, które często przypominają normalny ruch sieciowy, co utrudnia ich wykrycie.