Cyber Kill Chain

The Cyber Kill Chain was developed by Lockheed Martin from a military attack model and provides a guideline for companies to defend against cyber attacks.

It describes the procedure and the attack path of a hacker in 7 steps.

1. RECONNAISSANCE: Search targets

Approach of the attacker:	Countermeasures:
Research and information collection Search for suitable targets Active data interception Social engineering	Analyze browsing behaviors and prioritize defenses

2. WEAPONIZATION: Prepare attack

Approach of the attacker:	Countermeasures:
Specific search for backdoors Preparation of "weapons" by e.g. building/buying/renting bot nets	Detect attacks early using collected metadata and appropriate tools: ExploitDB Metasploit Armitage BeEF ...

3. DELIVERY: Start execution

Approach of the attacker:	Countermeasures:
Delivery of the attack tools Mostly via usual communication channels Disguised as application documents, invoices, ...	Use artifacts of weapon systems to detect malware

4. EXPLOITATION: Exploiting security vulnerabilities

Approach of the attacker:	Countermeasures:
Browsing the attack field Exploit found vulnerabilities	Implement a patch management system and regulary check for vulnerabilities

5. INSTALLATION: Persist access

Approach of the attacker:	Countermeasures:
Malware is being installed In the case of longer-term access risk of expansion to customer and supplier networks	Monitor and analyze installation operations and data traffic

6. COMMAND AND CONTROL: Expand remote control

Approach of the attacker:	Countermeasures:
Execute targeted commands Connect to CC servers	Prevent communication to known CC servers and monitor data traffic

7. ACTIONS ON OBJECTIVES: Finish attack

Approach of the attacker:	Countermeasures:
Data is encrypted, exfiltrated or destroyed Specific extension to production processes	Use IT forensics to evaluate the attack

CC BY SA