cyber security voor mediabedrijven

Handvatten voor een pragmatische aanpak

Wie is Alexander

- Architect bij KPN
- Sinds 2006 bezig met TV Media & Streaming
- Security:
  - Werk, Studie en Hobby

Wat is Cybersecurity?

- Cyberspace is een nieuwe dimensie

bron: http://www.nu.nl/gadgets/4255933

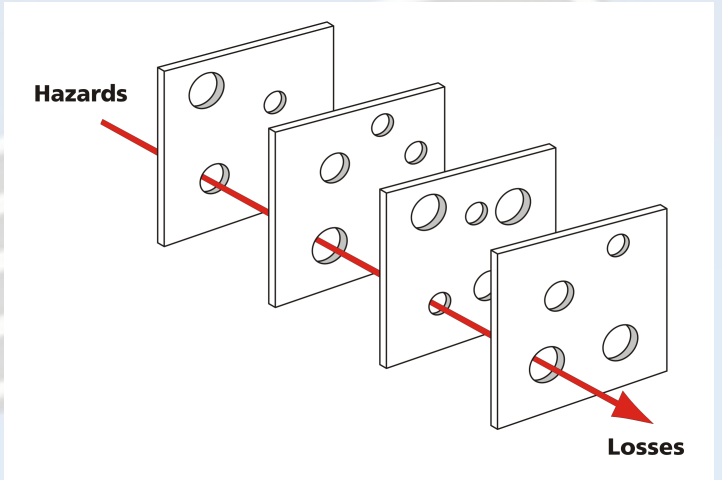
bron: https://www.security.nl/posting/470041

Doel: Beschermen van de kroonjuwelen

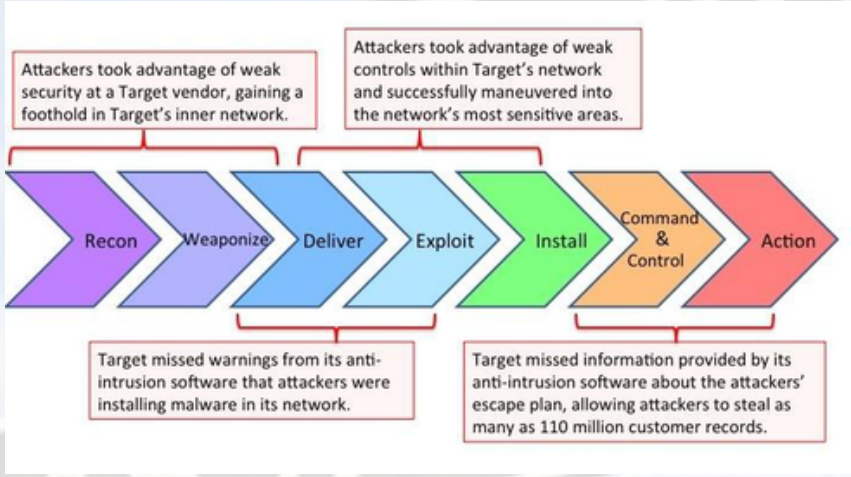
- “Tastbaar” (voor zover er sprake van is…)
  - Gegevens (wachtwoorden, softwarecode)
  - Content
- “Niet tastbaar”
  - Beschikbaarheid dienst
- C.I.A.
  - Confedential, Integrity en Availability

Swiss cheese en de kill chain

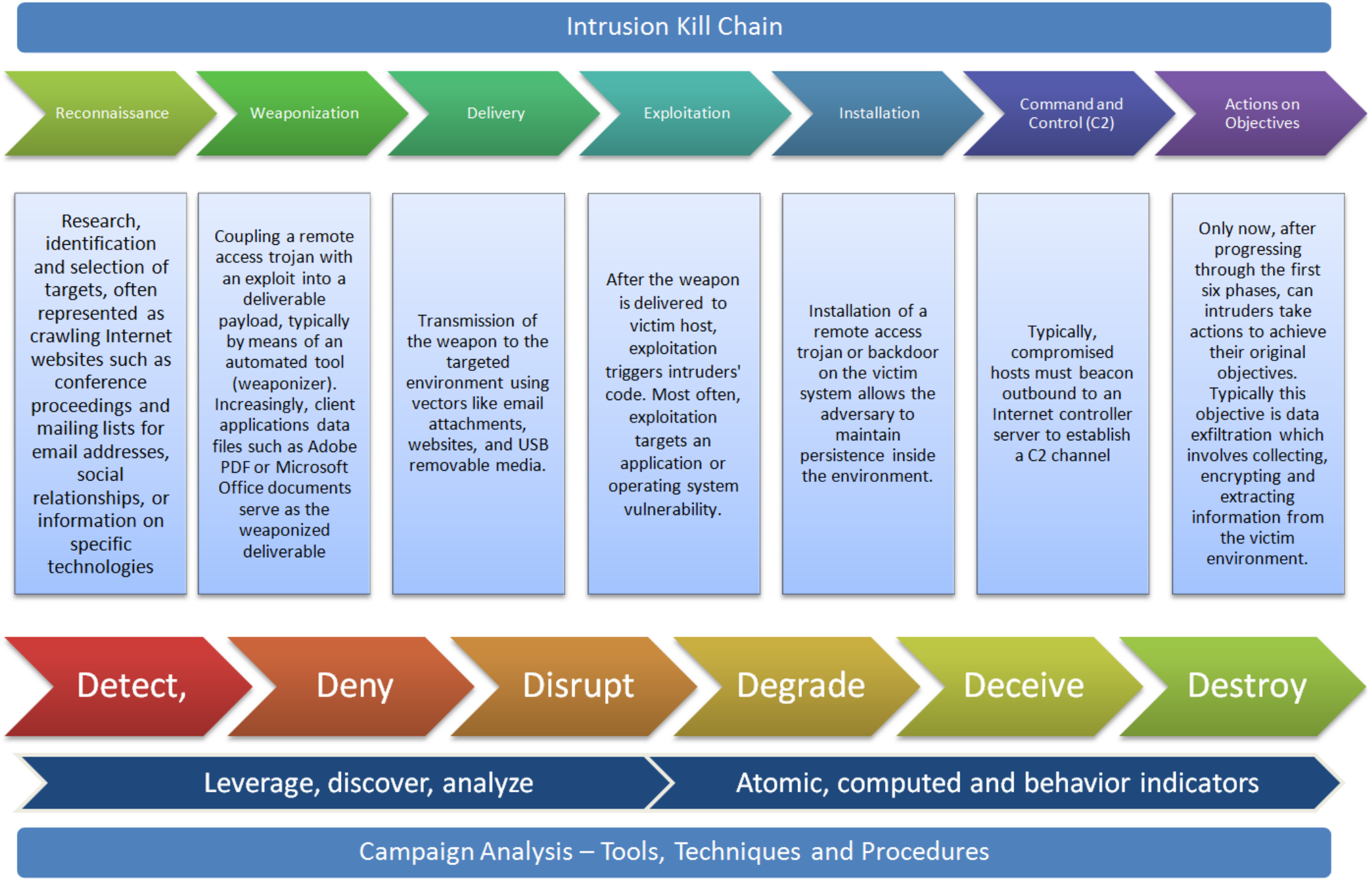
- Iedere laag beschermen.
- Niet vertrouwen op die ene perfecte firewall.
- Swiss cheese-model
- Weerstand tegen de Cyber Kill Chain



bron: https://en.wikipedia.org/wiki/Swiss_cheese_model

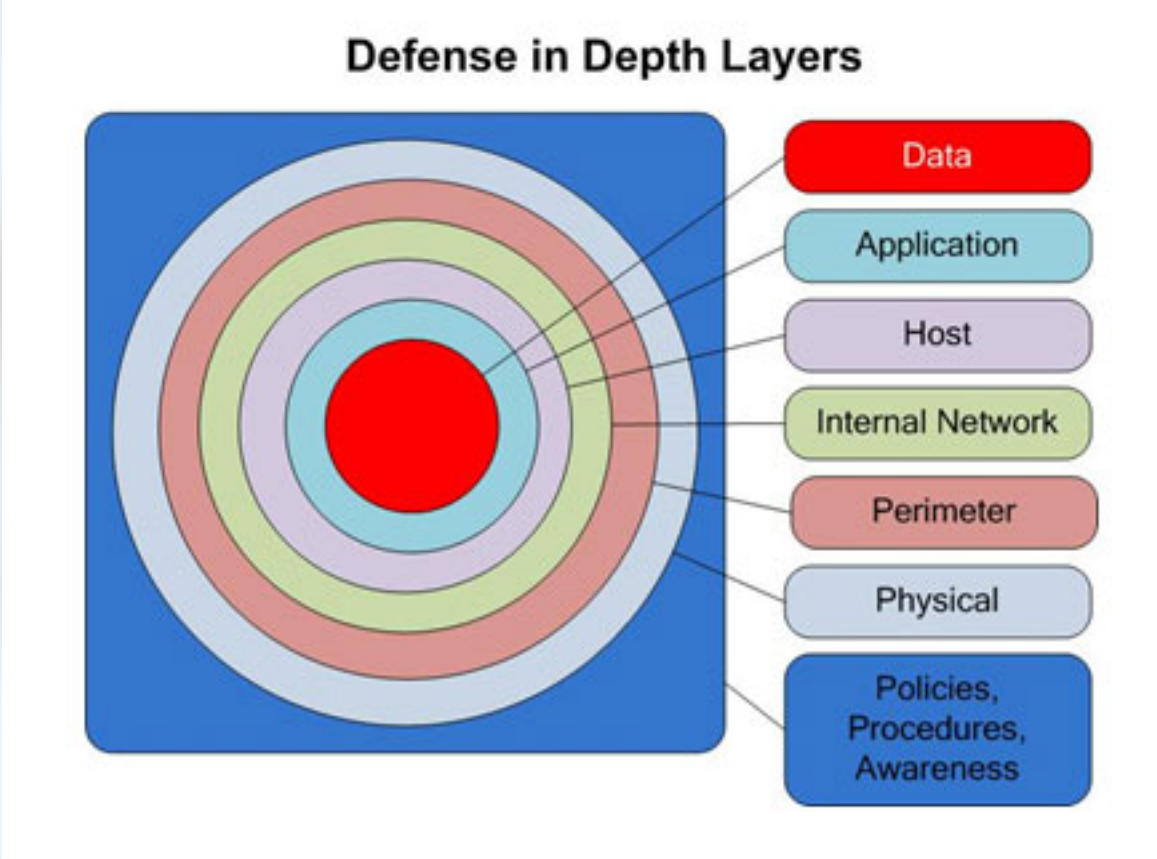


bron: "A 'Kill Chain' Analysis of the 2013 Target Data Breach," March 26, 2014; US Senate Committee on Commerce, Science, and Transportation


Intrusion Kill Chain
Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command and Control (C2)
Actions on Objectives
Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies
Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool (weaponizer). Increasingly, client applications data files such as Adobe PDF or Microsoft Office documents serve as the weaponized deliverable
Transmission of the weapon to the targeted environment using vectors like email attachments, websites, and USB removable media.
After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability.
Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.
Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel
Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment.
Detect,
Deny
Disrupt
Degrade
Deceive
Destroy
Leverage, discover, analyze
Atomic, computed and behavior indicators
Campaign Analysis – Tools, Techniques and Procedures

Defence in depth

- Policies, Procedures & Awareness
- Fysiek
- Perimeter
- Intern Netwerk
- Host
- Applicatie
- Data



bron: https://technet.microsoft.com/en-us/library/cc512681.aspx

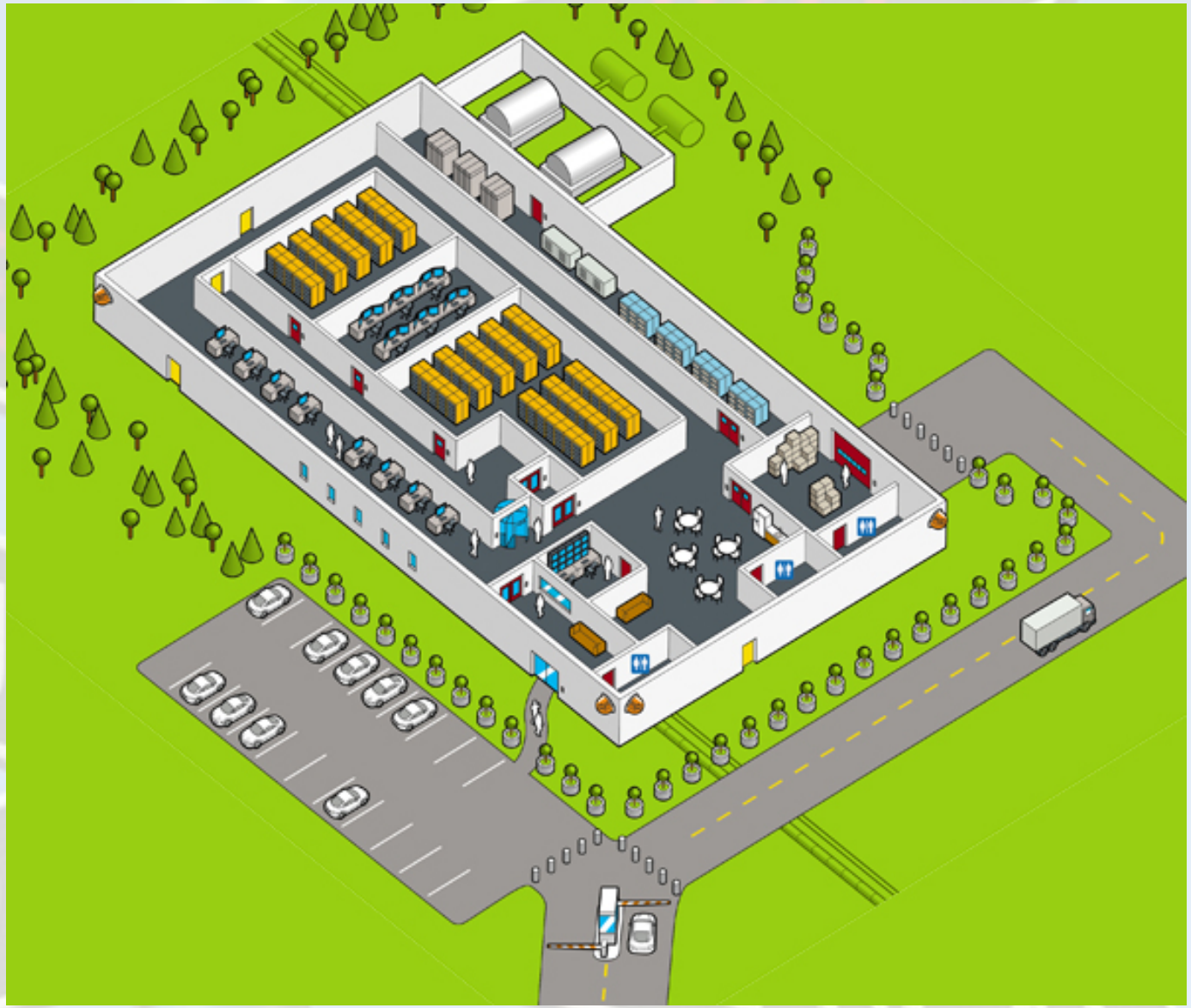
Policies, Procedures & Awareness

- Data clasificatie (de kroonjuwelen)
- Wachtwoord beleid
- Grootste uitdaging is het overbrengen van het beleid
  - Ook naar leveranciers

bron: https://nl.wikipedia.org/wiki/Tien_geboden

Fysiek

- Hekken
- Muren
- Bewaking
- Sloten en sleutels
- Badges
- Etc…



bron: http://www.csoonline.com/article/2112402

Perimeter

- Firewalls, Nat, Anti-ddos, Verkeer validatie, IDS
- Beveiliging op de transportlaag. (Encryptie, SSL, Identificatie)
  - https://www.ssllabs.com/
- Zorg dat alarmen bij een centrale plek komen, bijvoorbeeld een Security Operations Center (SOC)
- Netwerk zonering en segmentering
  - http://www.clico.pl/services/Network_Securite_Architecture.pdf

Intern Netwerk

- De toolset is vergelijkbaar met de perimeter, echter de instellingen kunnen afwijken. Neem hier dienst specifieke maatregelen.

Host

- Platform O/S
- Vulnerability Mgmt (patches)
- Anti Malware
- Anti Virus
- Links:
  - https://benchmarks.cisecurity.org/ (ook voor diverse appliances)
  - http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf
  - http://www.serverhardening.com/
- Tip: Appliances hebben veel overeenkomsten. Doe eerst ervaring op met generieke Hard- en software

Applicatie

- Authenticatie
- Authorisatie
- OWASP
  - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Bekende applicatie servers hebben ook hardening guidelines

Data

- Database security
- Backups
- Content Security
- Message Level Security (integrity, syntax checking)
  - https://msdn.microsoft.com/en-us/library/ff650794.aspx

Review en Pen-testen

- Code-Review
- Penetratie testen (intern/extern)
- Responsible Disclosure
  - https://www.ncsc.nl