# Cybersecurity fundamenten

## Cyberboswachters

Tim Dams

Deze cursus werd gemaakt met hulp van AI-assistentie. Sommige afbeeldingen zijn door AI gegenereerd.



AI GENERATED

# Wat leer je in dit hoofdstuk?

Na dit hoofdstuk kan je:

- ✓ het **CIA-model** en de **McCumber-kubus** toepassen op een scenario
- ✓ **soorten aanvallers** onderscheiden (motivatie, middelen, doelwit)
- ✓ **passieve vs actieve aanvallen** toelichten en herkennen
- ✓ malware-families en social engineering-technieken illustreren
- ✓ uitleggen wat een **zero day** en een **window of vulnerability** zijn
- ✓ de **principes van verdedigen** toepassen: tegenhouden, detecteren en herstellen

> Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks.
>
> — De definitie van Cisco

# Alles draait rond het beschermen van **informatie**.

Op een server, in een document of in iemands hoofd. Er zijn nu meer **verbonden apparaten** dan mensen, en aanvallers worden steeds innovatiever.

> **The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources.**
>
> — De formele definitie van NIST (National Institute of Standards and Technology, VS)

Die *resources* zijn: `hardware` `software` `firmware` `information / data` `telecommunications`

Zo introduceert NIST meteen **CIA** én de scope van de **McCumber kubus**.

DEEL 1

# CIA en het security model

Data, in welke vorm dan ook, moet **beschermd** worden.

# Het CIA-model



### Confidentiality

Enkel bevoegde partijen kunnen de data lezen.

`encryptie` `wachtwoorden`



### Integrity

De data is ongewijzigd en betrouwbaar.

`hashing` `digitale handtekeningen`



### Availability

De data is bereikbaar wanneer nodig.

`back-ups` `firewalls` `redundantie`

**DoS-aanvallen** mikken specifiek op de availability-pijler.

# Waar zie je dit terug?

| | |
|---|---|
| **Encryptie** | *Cryptografie*: symmetrische en asymmetrische encryptie |
| **Wachtwoorden** | *Authenticatie*: wachtwoorden kiezen en opslaan, MFA |
| **Hashing** | *Cryptografie* (intermezzo hashes) en *Authenticatie* (paswoord hashing) |
| **Digitale handtekeningen** | *Cryptografie*: boodschappen ondertekenen, certificaten |
| **Availability** | hier enkel DoS en back-ups. Firewalls, load balancers en redundantie: vak **Network Security** |

# Confidentiality heeft twee gezichten



### Data confidentiality

De **inhoud** van de data is afgeschermd. Je bericht is bijvoorbeeld versleuteld.



### Privacy

Het feit **dát er data over jou bestaat**, en wie ze mag verwerken, is beschermd.

## NIEMAND LEEST JE MEDISCH DOSSIER

# Toch is het een **privacy-inbreuk** als een onbevoegde werknemer het kan opvragen.

# Integrity heeft twee gezichten



### Data integrity

De **data zelf** is niet aangepast. Daar dienen onze hashes voor.



### System integrity

Het **systeem** werkt zoals bedoeld, zonder stille manipulatie.

Daarbij hoort vaak ook **non-repudiation**: kan de zender later ontkennen dat hij het bericht stuurde? Digitale handtekeningen lossen dat op.

## DATA INTEGER ≠ SYSTEEM INTEGER

Een rootkit kan je **data** ongemoeid laten en toch je **systeem** overnemen.

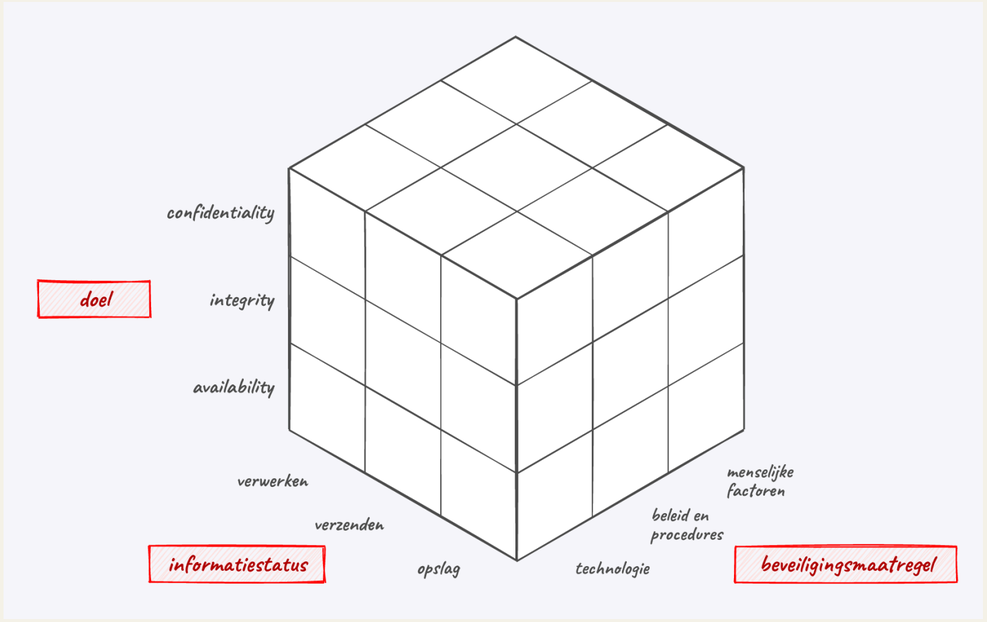
JOHN MCCUMBER, 1991

# McCumber kubus

Een framework om **niets over het hoofd** te zien. De kubus heeft drie dimensies:

| | |
|---|---|
| **Informatiestatus** | opslag, verzenden, verwerken |
| **Maatregel** | technologie, beleid, mensen |
| **Doel** | C.I.A. |

Enkel als je **alle aspecten** van alle dimensies afdekt, haal je je CIA-doelen.



## TECHNOLOGIE ALLEEN IS NIET GENOEG

Een werknemer die z’n wachtwoord op een **post-it** plakt, maakt de duurste firewall nutteloos.

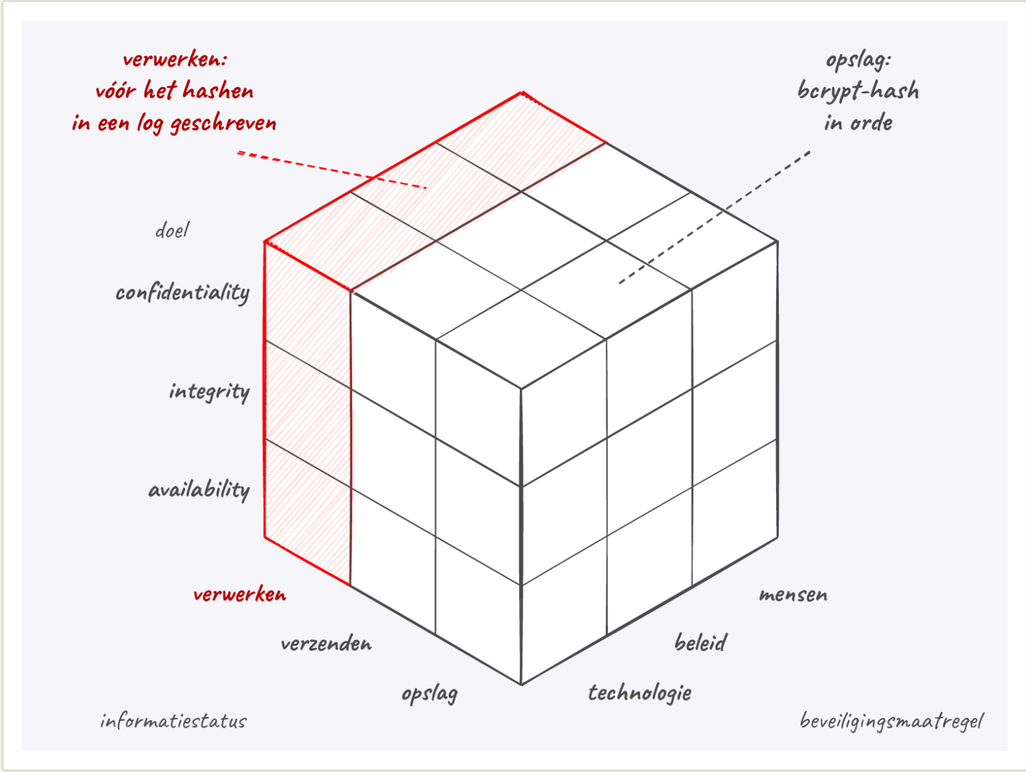
2018

# McCumber in actie: Twitter

✓ *Opslag*: gehasht met **bcrypt**

✗ *Verwerking*: door een bug **vóór** het hashen gelogd

Eén vergeten hoekje: miljoenen wachtwoorden in **plaintext** in interne logs.




Bron: Twitter Blog, mei 2018.

# ISO 27001

Dé internationale **standaard voor informatiebeveiliging**.

### Aantonen

Bedrijven tonen hiermee aan dat ze security serieus nemen.

### Externe audit

Een externe auditor controleert of je aan alle eisen voldoet.

### Elke 3 jaar

Het certificaat moet je telkens hernieuwen.

### Hele kubus

De eisen dekken alle dimensies van de McCumber kubus.

DEEL 2

# Een ongelijke strijd

De wapenwedloop is de laatste jaren alleen maar **grimmiger** geworden.

# Moeilijker dan ooit

### Snelheid

Aanvallers vallen miljoenen systemen tegelijk aan.

### Attack surface

Netwerken zijn veel groter en complexer dan 20 jaar geleden.

### Lage drempel

Een krachtige aanval = IP invullen + één klik.

### Zero days

Nieuwe kwetsbaarheden worden sneller gevonden dan gepatcht.

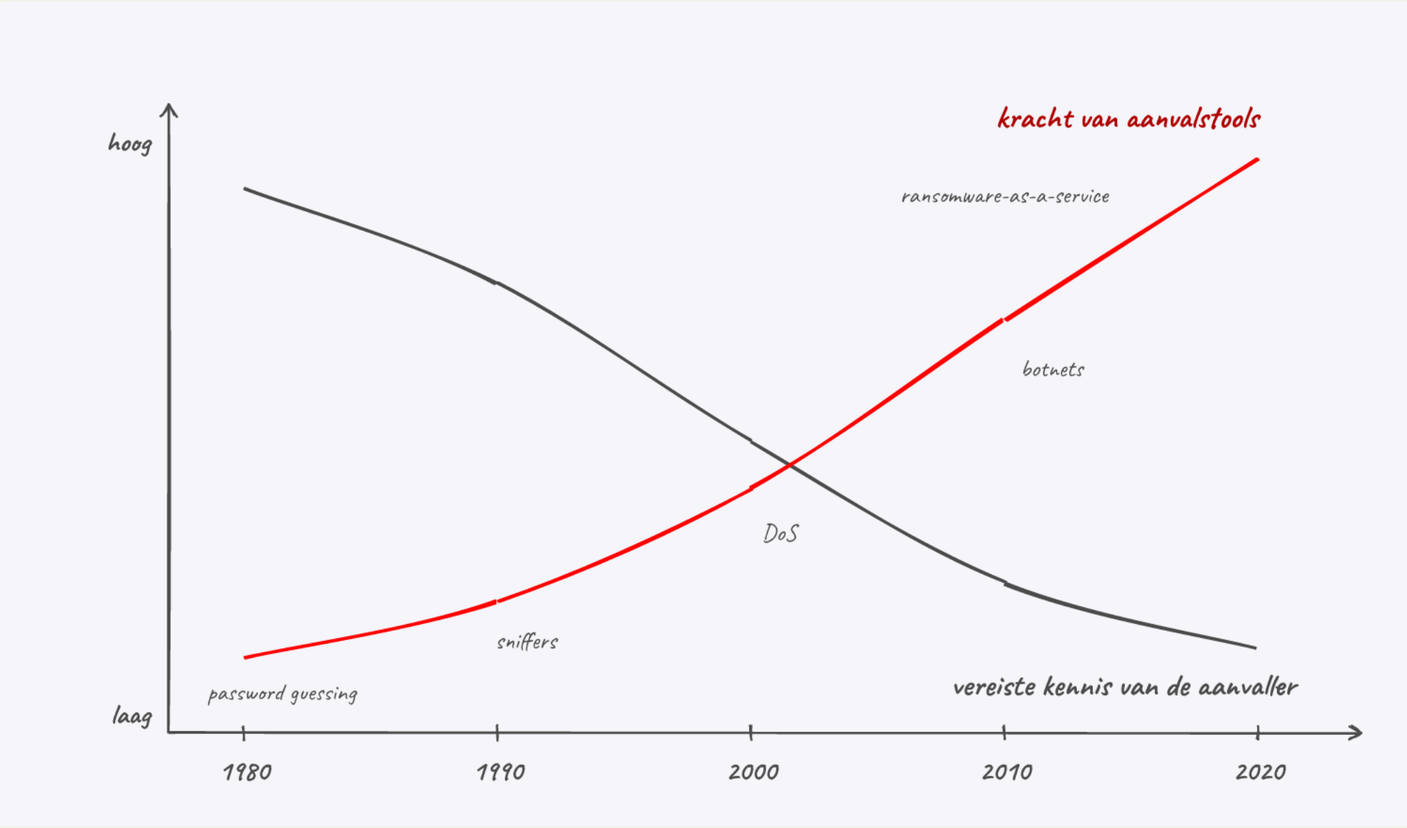
### Botnets

Gigantische legers aan gecompromitteerde machines.

### Gebruikers

Klikken sneller dan ooit op phishing-links.

# De scheve grafiek




Aanvalstools worden steeds **krachtiger**, terwijl de vereiste **kennis** van de aanvaller daalt. Daarom zijn scriptkiddies een reëel probleem.

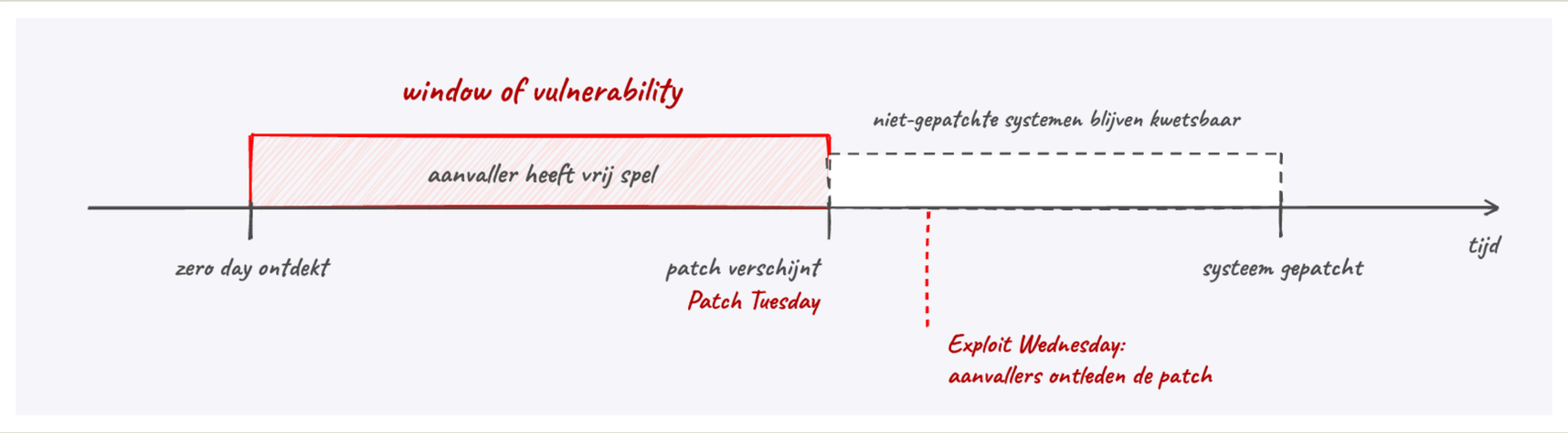
ZERO DAY

# Een kwetsbaarheid die de softwarefabrikant **nog niet kent**.

Gegarandeerd werkzaam: er bestaat nog geen patch. Aanvallers hebben er dan ook aardig wat geld voor over.

# Window of vulnerability

De periode tussen het ontdekken van een zero day en het moment waarop de patch effectief geïnstalleerd is. Zolang er geen patch is, heeft de aanvaller **vrij spel**.




Ook **ná de patch**: niet elk systeem wordt meteen bijgewerkt. Eén niet-gepatcht systeem is het gaatje in de linie.

# Patch Tuesday & Exploit Wednesday

### Patch Tuesday

- Sinds 2003 rolt Microsoft updates uit op de **2de dinsdag** van de maand
- Voorspelbaar voor IT-beheerders

vs

### Exploit Wednesday

- Aanvallers doen *reverse-engineering* van de patch
- Ze achterhalen welke kwetsbaarheid gedicht werd
- En jagen op alle systemen die nog niet gepatcht zijn

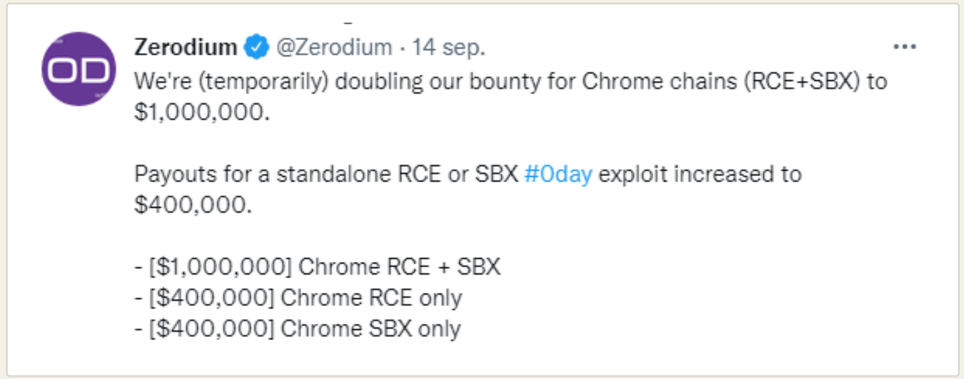
Dit zijn geen zero days meer, maar pas gepatchte lekken (*n-days*). Wie na dinsdag niet patcht, is woensdag doelwit.

# Zero days: een markt

Zero days worden verhandeld op een **schimmige markt**.

**> 1 miljoen $**

kan één zero day opbrengen




Zerodium: een zero-day broker.

*How They Tell Me the World Ends* (Nicole Perlroth, NYT, 2021) geeft een griezelig inzicht in de zero-day markt.

DEEL 3

# De stropers

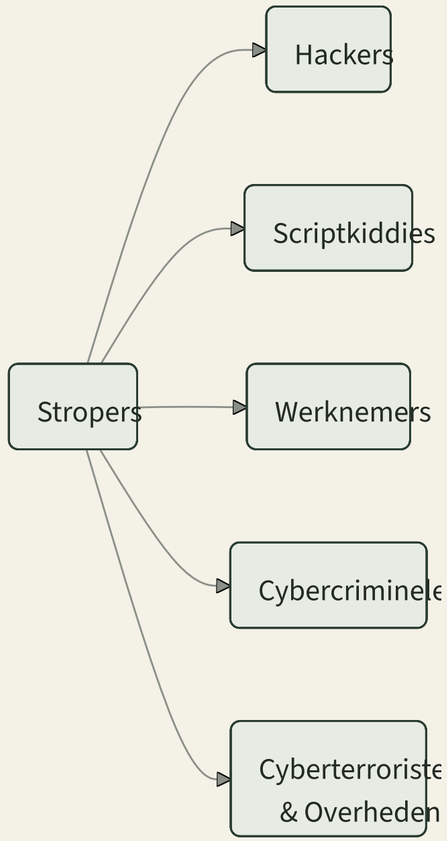
Iedere groep aanvallers heeft **eigen motivaties, middelen en methodes**.

# Wie zijn de stropers?



AI GENERATED

# De stropers op een rij



# Hackers: de kleurcode



### Whitehat

**Ethisch hacker.** Legaal pentesten, bug bounty.



### Greyhat

**Grijs gebied.** Goede intenties, maar niet altijd legaal.



### Blackhat

**Crimineel** (*cracker*). Illegale toegang, eigenbelang.



### Redhat

**Vigilante.** Vecht terug tegen blackhats, met middelen die niet altijd legaal zijn.



### Bluehat

**Wraaklustig.** Eén doel: wraak nemen.



### Greenhat

**Beginner.** Leert het vak nog, vaak over dezelfde kam geschoren als scriptkiddies.

# Scriptkiddies

### Krachtige tools

Weinig tot geen kennis, maar wel **gebruiksvriendelijke tools** die veel kunnen.

### Strafbaar

Beseffen vaak **niet** dat hun acties strafbaar zijn.

### Echte schade

Doordat tools steeds krachtiger worden, zijn de gevolgen steeds drastischer.

Veiligheidsdiensten zien niet wie er achter een aanval zit en reageren altijd op dezelfde manier: een **politie-inval** en zware boetes, voor *“gewoon een knopje indrukken”*.

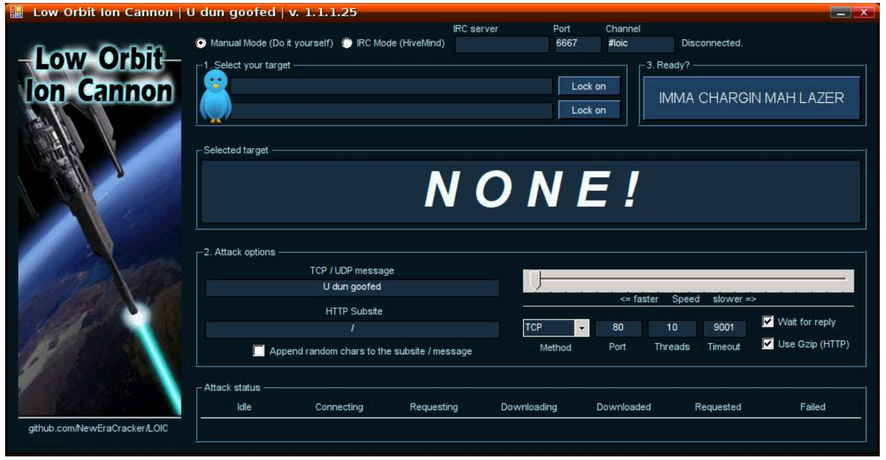
SCRIPTKIDDIE-TOOL

# Low Orbit Ion Cannon

Gratis **DDoS-tool**, eenvoudig in gebruik. Vallen genoeg gebruikers tegelijk aan, dan is de impact massaal.

In **2010** urenlang lamgelegd, uit protest tegen de blokkering van WikiLeaks-betalingen:

`Visa` `MasterCard` `PayPal`




Low Orbit Ion Cannon UI (Bron: Wikipedia).

# Werknemers: de vergeten bedreiging

### Onbewust

Menselijke fouten:

- Wachtwoord op een post-it
- Onbekenden binnenlaten (*piggybacking*)
- Eigen access point voor betere wifi

vs

### Bewust

*Insider threats*:

- Ontevreden of ontslagen werknemers
- Sabotage, datadiefstal, losgeld eisen
- Zitten *aan de binnenkant* van je beveiliging

**Identity management**: verwijder de accounts van ex-werknemers **onmiddellijk** na ontslag.

BRING YOUR OWN DEVICE (BYOD)

# Elk eigen toestel kan **besmet** je bedrijfsnetwerk binnenwandelen.

De ommuurde burcht werkt niet meer. Je bouwt nu ook muren rond elke werknemer én z’n toestellen: on-device firewall, virusscanner, netwerk-authenticatie.

# Net ontslagen...



AI GENERATED

2025 - DE GEBROEDERS AKHTER

# DROP DATABASE;

Tweelingbroers, IT-contractors voor een D.C.-bedrijf met **45+ federale agentschappen** als klant. Op 18 februari 2025 ontslagen tijdens een online meeting (verzwegen strafblad ontdekt). Diezelfde dag nog, in enkele uren:

1. Databases op **write-protect**: collega's kunnen niets meer redden
2. **96 federale databases** gedropt (FOIA, DHS…)
3. Een **AI-assistent** gevraagd hoe je systeemlogs wist

Bron: Ars Technica, *Drop database: what not to do after losing an IT job* (mei 2026).

# Niet hun eerste keer

In **2016** al veroordeeld voor een inbraak bij het US State Department. Daarna gewoon **opnieuw aangeworven** als overheidscontractor: geen background check.

## 39 maanden

cel voor Muneeb, na een schuldbekentenis

## 21 jaar

riskeert Sohaib: schuldig bevonden door een jury op 8 mei 2026, strafmeting nog niet bekend

# Cybercriminelen

**$700 miljard**

schade door online criminaliteit in 2021 (schatting)

**Geld** is de enige motivatie.

Ze werken als moderne bedrijven:

- Helpdesks voor ransomware-betalingen
- **RaaS**: Ransomware-as-a-Service
- Botnets verhuren op het darkweb

Door dat bedrijfsmodel heeft de aanvaller zelf **geen technische kennis** meer nodig.

# Max Butler, alias *"Iceman"*

1. **2006**: neemt de wereldmarkt voor **gestolen creditcards** over
2. Z'n truc: concurrenten **hacken** en hun databases overnemen
3. **13 jaar cel**, maar daar stopt het niet
4. **2018**: aangeklaagd voor een smartphone-smokkel met een **drone**

Alles vanuit een appartement in San Francisco. Met die smartphone wou hij vanuit de gevangenis z'n business heropstarten.

Bronnen: Wired (2008), Washington Times (2018).

# Money mules: *de zichtbare schakel*




Criminelen werken zelden rechtstreeks met gestolen geld. *Money mules* denken een *“leuk bijverdienstje”* als **financial manager** te hebben en zetten hun eigen rekening ter beschikking.

**2023**: één internationale actie, **1.013 arrestaties** en meer dan **10.000 geldezels** opgespoord.



AI GENERATED

# Cyberterroristen, spionnen & overheden

- De scheidslijn tussen **terrorist**, **spion** en **staatshacker** is vaag en politiek
- Hun financiële en technische middelen zijn **immens** groter dan die van de andere groepen



De uraniumverrijkingsinstallatie in Natanz (Iran), doelwit van de door staten gesponsorde Stuxnet-malware. Bron: Wikimedia Commons, auteur Parsa 2au, CC BY-SA 4.0.

## HET MOSSAD/NON-MOSSAD PRINCIPE

# Een staatsactor **zal** binnenkomen, ongeacht je budget.

Maak dus een realistische inschatting van je tegenstander en focus op de dreigingen die relevant zijn voor jou.

# Een (onvolledige) geschiedenis

| | |
|---|---|
| **2005 · Titan Rain** 🇨🇳 | Chinese inbraak in honderden Amerikaanse defensiesystemen |
| **2007 · Estonia** 🇷🇺 | DDoS legt Estland plat: *“de eerste cyberoorlog”* |
| **2008 · Georgia** 🇷🇺 | cyberaanval synchroon met de militaire invasie |
| **2009 · Operation Aurora** 🇨🇳 | Google, Adobe, Juniper, Yahoo gehackt voor hun broncode |
| **2010 · Stuxnet** 🇺🇸🇮🇱 | Iraanse centrifuges gesaboteerd |
| **Nitro Zeus** 🇺🇸 | geheim plan B tegen Iran |

📖 *The Perfect Weapon* (David Sanger, NYT 2018): cyberoorlog als vast instrument van moderne diplomatie.

# Een (onvolledige) geschiedenis: *vervolg*

| | |
|---|---|
| **2013 · Belgacom** 🇬🇧 | GCHQ luistert via de *Regin*-malware mee bij een Belgische telecomoperator |
| **2017 · NotPetya** 🇷🇺 | destructieve aanval op Oekraïne, vermomd als ransomware |
| **2020 · SolarWinds** 🇷🇺 | achterdeur in een software-update, duizenden organisaties binnen |
| **2022 · Viasat KA-SAT** 🇷🇺 | satellietmodems gewist bij de start van de invasie, ook 5.800 Duitse windturbines offline |
| **2023 · Volt Typhoon** 🇨🇳 | verstopt in Amerikaanse kritieke infrastructuur, klaar voor sabotage |
| **2024 · Salt Typhoon** 🇨🇳 | diep in Amerikaanse telecomnetwerken, tot in de afluistersystemen van de politie |

2022

# Hacktivisme in de Oekraïne-oorlog

Sinds de invasie: tienduizenden hacktivisten, aan **beide** kanten.

- *IT Army of Ukraine* tegen Russische banken, media, overheidssites
- Pro-Russische groepen tegen Oekraïense infrastructuur




Hacktivists stoke pandemonium (Wired).

Ongecoördineerd: aanvallen raken soms neutrale partijen, en staatsactoren zijn niet meer te onderscheiden van activisten.

Bron: Wired, *“Hacktivists Stoke Pandemonium Amid Russia’s War in Ukraine”*.

DEEL 4

# Hoe vallen ze aan?

Elke groep heeft eigen redenen, maar hun aanvallen verlopen in **dezelfde stappen**.

# De 5 fasen van een aanval

1. **Verkennen**: Google, sociale media, dumpster diving. *Onzichtbaar voor het slachtoffer.*
2. **Scannen**: port scanners, vulnerability scanners. *Detecteerbaar.*
3. **Toegang**: kwetsbaarheid uitbuiten, phishing, privilege escalation
4. **Bestendigen**: backdoor installeren, laterale beweging in het netwerk
5. **Sporen wissen**: logs aanpassen of verwijderen, tools en tijdelijke backdoors opruimen

# Red team vs. blue team

Bij een legale pentest strijden twee teams tegen elkaar.

### Blue team

Speelt de **verdedigers**: probeert de aanvallen te verijdelen.

VS

### Red team

Speelt de **aanvallers**: de digitale stropers.

Niet te verwarren met **redhat** (vigilante) en **bluehat** (wraakzuchtig) hackers!

DEEL 5

# Classificatie van aanvallen

Met drie personages: **Alice**, **Bob** en **Eve**.

# Alice, Bob en Eve




| | |
|---|---|
| **Alice en Bob** | willen veilig communiceren |
| **Eve** | wil hun communicatie onderscheppen, aanpassen of blokkeren |

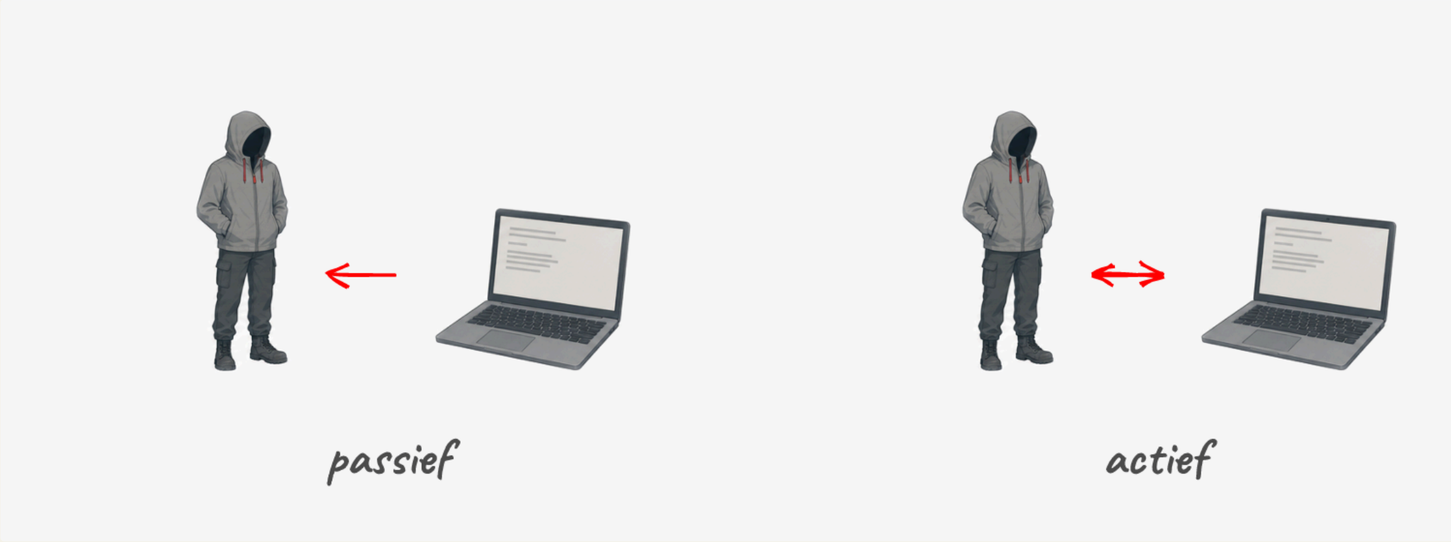
Meet the crew.

## NIET ENKEL NETWERKEN

# Alice en Bob zijn **eender welk start- en eindpunt** van informatie.

`CPU → RAM` `database → schijf` `server → gebruiker`

# Passieve vs. actieve aanvallen




## Passief

- Eve **luistert** en wacht
- Zeer moeilijk te detecteren
- Afhankelijk van wat het slachtoffer doet

vs

## Actief

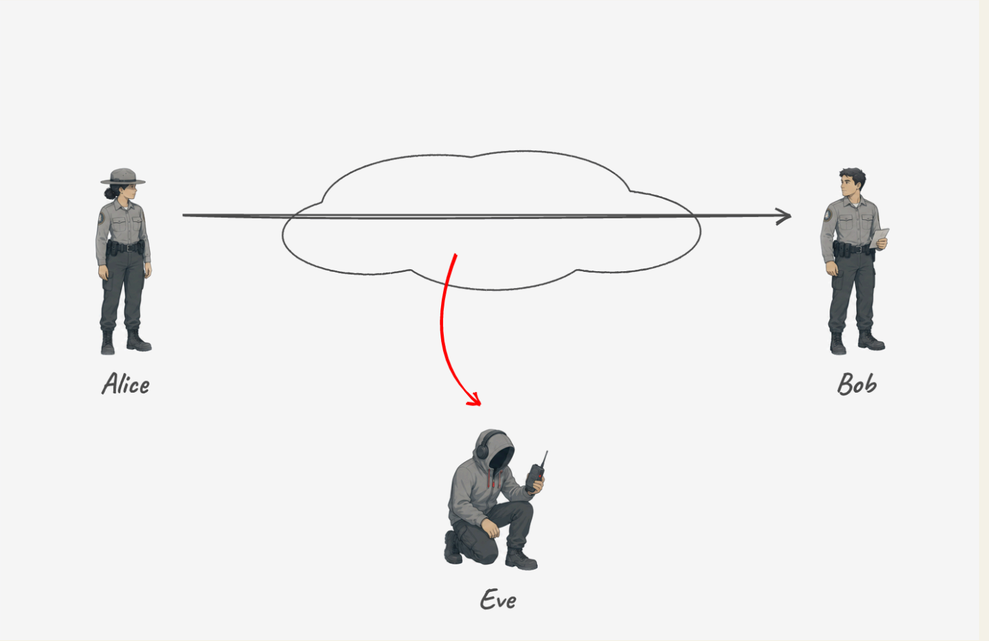
- Eve **grijpt in** in de communicatie
- Groter risico op detectie
- Meer controle voor Eve

PASSIEVE AANVAL 1

# Sniffing

Eve luistert met een **sniffer** (bv. Wireshark) de netwerktrafiek af.

- Ook geëncrypteerde trafiek lekt **metadata**: MAC-adressen, timing, gebruikersinfo
- Slecht beveiligde third-party apps sturen soms credentials **onversleuteld**: een goudmijn voor Eve

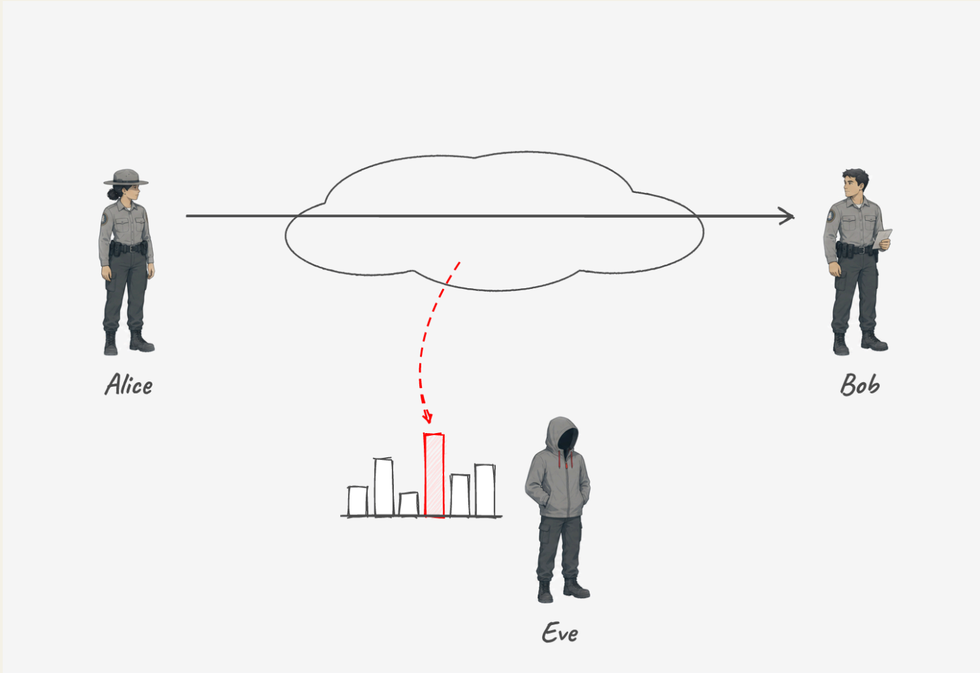


PASSIEVE AANVAL 2

# Trafiekanalyse

Eve registreert **wanneer en hoe** het slachtoffer communiceert.

- Ze kent de actieve periodes en kan haar aanval beter plannen
- Ze ziet het type activiteit: e-mail, VoIP, bestandsoverdracht, …

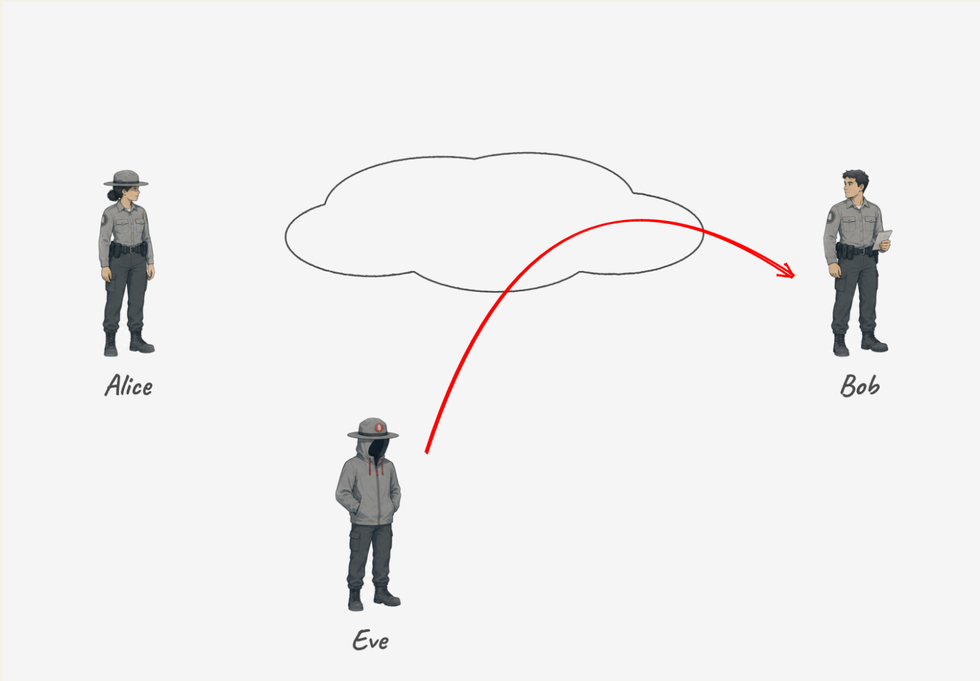


ACTIEVE AANVAL 1

# Masquerading & spoofing

Eve neemt de **digitale identiteit** van een legitieme gebruiker over.

- Bv. **MAC-spoofing**: het hardware-adres van een netwerkkaart kopiëren
- Doel: anonimiteit én toegang tot afgeschermde bronnen

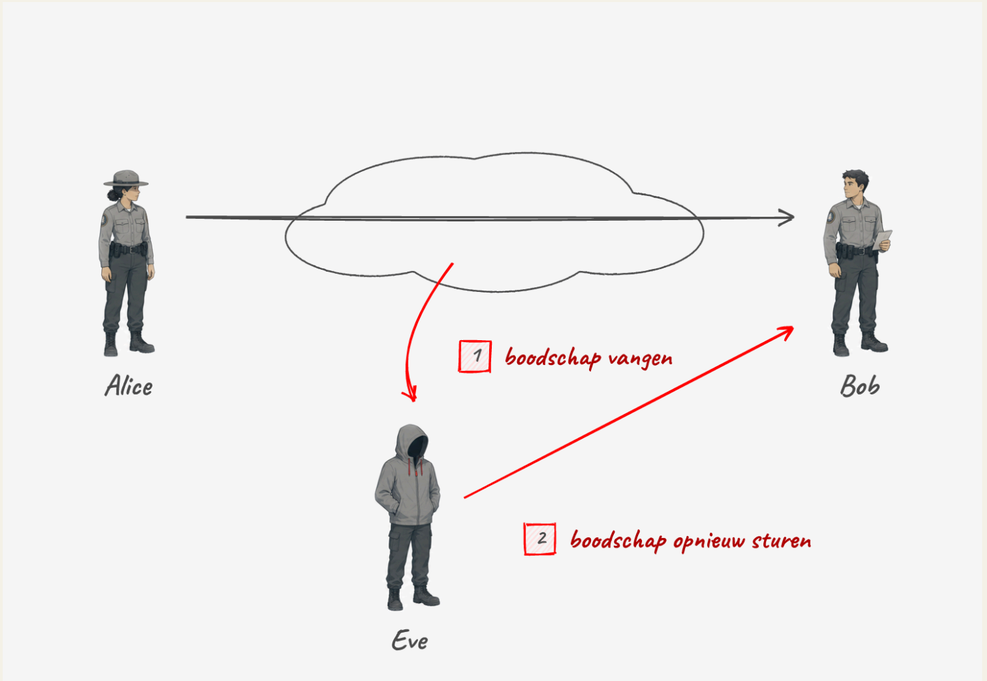


ACTIEVE AANVAL 2

# Replay attack

Eve bewaart een legitiem pakket (bv. een login) en verstuurt het later **opnieuw**.

- Het systeem denkt dat het Alice is
- Gevaarlijk bij systemen zonder **session tokens** of **tijdstempels**

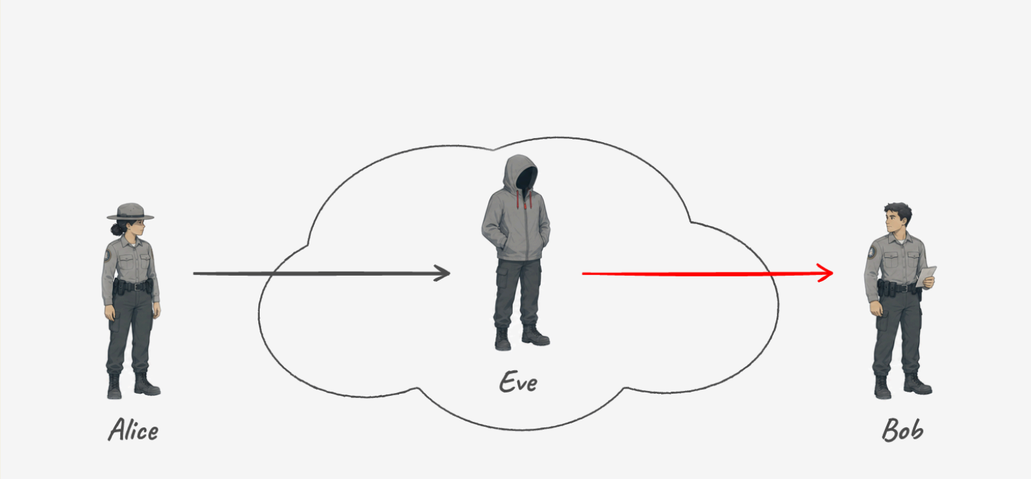


ACTIEVE AANVAL 3

# Man-in-the-Middle

Eve nestelt zich **tussen** Alice en Bob.

- Meestal de **krachtigste** aanval: Eve kan alle andere aanvallen combineren
- Ze kan de communicatie **lezen, aanpassen of blokkeren**, volledig onzichtbaar
- Vereist vaak masquerading naar beide kanten tegelijk

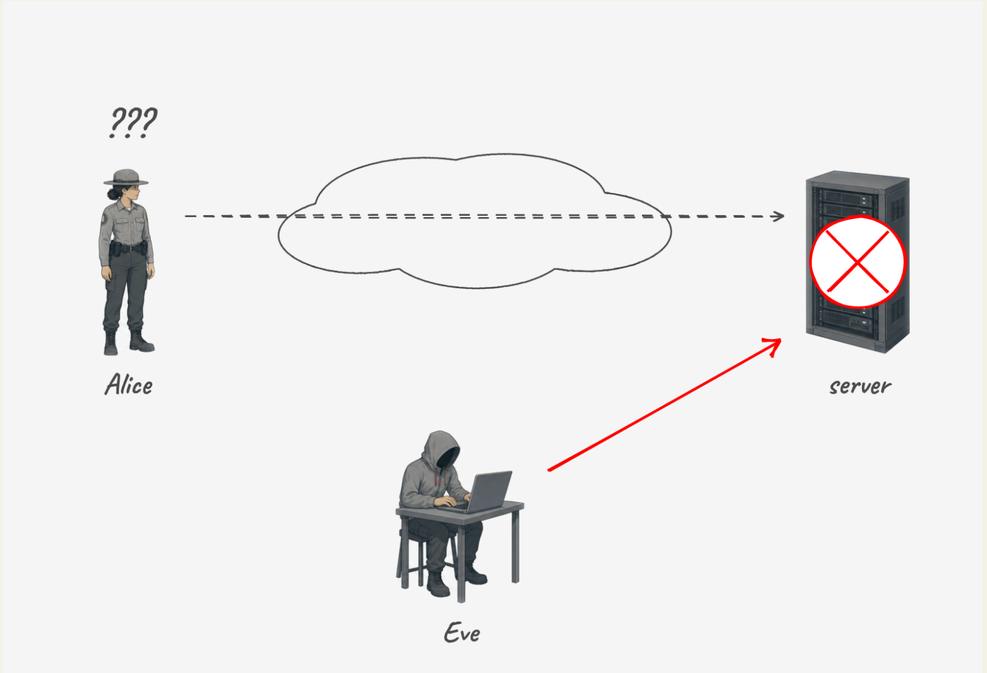


ACTIEVE AANVAL 4

# Denial-of-Service

Doel: een systeem of gebruiker **onbereikbaar** maken.

- Trafiek overstromen, signaalstoring, fysiek de stekker uittrekken
- **DDoS** = *Distributed* DoS, via een botnet van duizenden zombies tegelijk



DEEL 6

# Social engineering

# Aanvalsvectoren: de grotere kaart

*Hoe zet een aanvaller een eerste voet binnen?* Dat is de *initial access vector*.

| | |
|---|---|
| **Social engineering** | phishing, vishing, smishing, … *(dit deel)* |
| **Zero-day exploit** | eerder bij *Zero days en patching* |
| **Insider threat** | eerder bij *Werknemers* |
| **Supply chain attack** | hoofdstuk 1 (SolarWinds, Kaseya, XZ Utils, Hezbollah-pagers…) |
| **Drive-by & watering hole** | straks bij *Software-based aanvallen* |

Vraag je bij elke aanval eerst af: **via welke vector** is de stroper binnen geraakt?

## HET HACKEN VAN MENSEN

# Mensen zijn de **zwakste schakel** in elk securitymodel.

Social engineering misbruikt `vertrouwen` `nieuwsgierigheid` `angst` `hebzucht`

# Fysieke social engineering



### Pizzakoerier

Met een stapel (lege) pizzadozen binnenwandelen: werknemers houden de deur voor je open.



### Bij de rokers

Wat meekeuvelen aan de achterdeur en mee naar binnen lopen (*piggybacking*).



### "Telenet-technieker"

Bellen en het wachtwoord opvragen.

Je hoeft niet eens aanwezig te zijn: social engineering kan ook gewoon via **e-mail**.

# Phishing vs. spear phishing

### Phishing

- Zoveel mogelijk mensen
- Generieke e-mail
- Lage slaagkans per persoon
- Bv. een nep-ING-mail naar iedereen

vs

### Spear phishing

- Eén specifiek persoon of groep
- Bericht op maat
- Veel hogere slaagkans
- Bv. een gerichte mail naar de CEO van bedrijf X

*Phishing* is afgeleid van *fishing*: hengelen naar slachtoffers.

# Meer dan e-mail

### Vishing

*Voice phishing*, via de telefoon. Bv. MGM Resorts (2023).

### Smishing

Via SMS of WhatsApp. Bv. het *“Bpost-pakketje”*.

### Whaling

Spear phishing op de “grote vissen”: CEO, CFO, C-levels.

### CEO-fraude

*Business Email Compromise* (BEC): de “CEO” vraagt een dringende overschrijving.

# > $50 miljard

wereldwijde schade door BEC tussen 2013 en 2022 (FBI)

# Nog meer technieken



### Pretexting

Een verzonnen, geloofwaardig scenario opbouwen, bv. *“Telenet-technieker aan de lijn”*.



### Baiting

Lokaas uitleggen: een USB-stick *“salarissen 2025”* op de parking.



### Tailgating

Meelopen met een geautoriseerd persoon door een beveiligde deur (*piggybacking*).



### MFA fatigue

Het slachtoffer spammen met MFA-prompts tot die uit frustratie op *“Accepteren”* drukt. **Lapsus$** deed het bij Uber, Microsoft en Rockstar.

# Waarom werkt social engineering zo goed?

Cialdini's **beïnvloedingsprincipes** (uit *Influence*, 1984):

### Autoriteit

Gezag dwingt af.

### Urgentie

Tijdsdruk schakelt kritisch denken uit.

### Schaarste

*"Nog 3 plaatsen vrij."*

### Wederkerigheid

Voor wat hoort wat.

### Sympathie

Ja zeggen tegen wie je leuk vindt.

### Sociale bewijskracht

*"Iedereen doet het."*

KEVIN MITNICK

# Hij wandelde gewoon binnen bij grote bedrijven. Niemand stelde vragen.

Ooit “America’s Most Wanted Hacker”. Z’n boek **The Art of Deception** is een aanrader.

# SE in het AI-tijdperk

**Deepfakes**: AI-gegenereerde audio of video van bestaande personen.



### Fake CFO

Live videocall met een nep-CFO (Hong Kong, 2024): **25 miljoen $** verlies.



### Gekloonde stem

De stem van een familielid voor een nep-noodgeval.



### AI-vishing

Vishing op grote schaal.

*“Let op tikfouten in de mail”* volstaat niet meer als de aanvaller met de stem van je baas belt. Meer in hoofdstuk 1: *“A.I. is here to stay”*.

# Verdedigen: het is een mensenprobleem

Social engineering los je niet op met technologie alleen.

- ✓ Trainen, trainen, trainen: **awareness-campagnes** zijn cruciaal
- ✓ **Phishing-simulaties** geven directe feedback
- ✓ Procedures voor helpdesks (vooral bij wachtwoordresets!)
- ✓ Een cultuur waarin werknemers *“nee”* of *“laat me even checken”* durven zeggen tegen de “CEO”

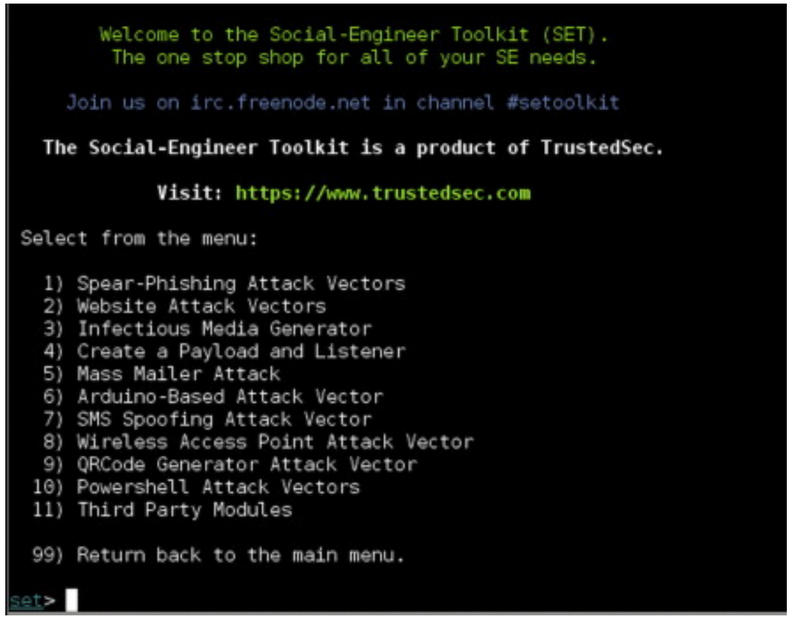
De volledige aanpak staat in de appendix ***Cybersecurity Awareness creëren***.

# Social Engineering Toolkit (SET)

Open source toolkit in **Kali Linux**, om:

- (spear) phishing-campagnes op te zetten
- bestaande websites te klonen
- malware in afbeeldingen te injecteren

Integreert met **Metasploit** voor complexe aanvallen.




Social Engineering Toolkit.

# OSINT: Open Source Intelligence

Informatie verzamelen via **publiek beschikbare bronnen**: een cruciale stap in de verkenningsfase van spear phishing.

### Slim zoeken

Geavanceerde zoekopdrachten: `site:`, `filetype:`, `+`

### Reverse image search

De oorsprong van een foto traceren, bv. met Google Lens. Of de locatie laten schatten door een AI-agent, bv. met geo-sleuth.

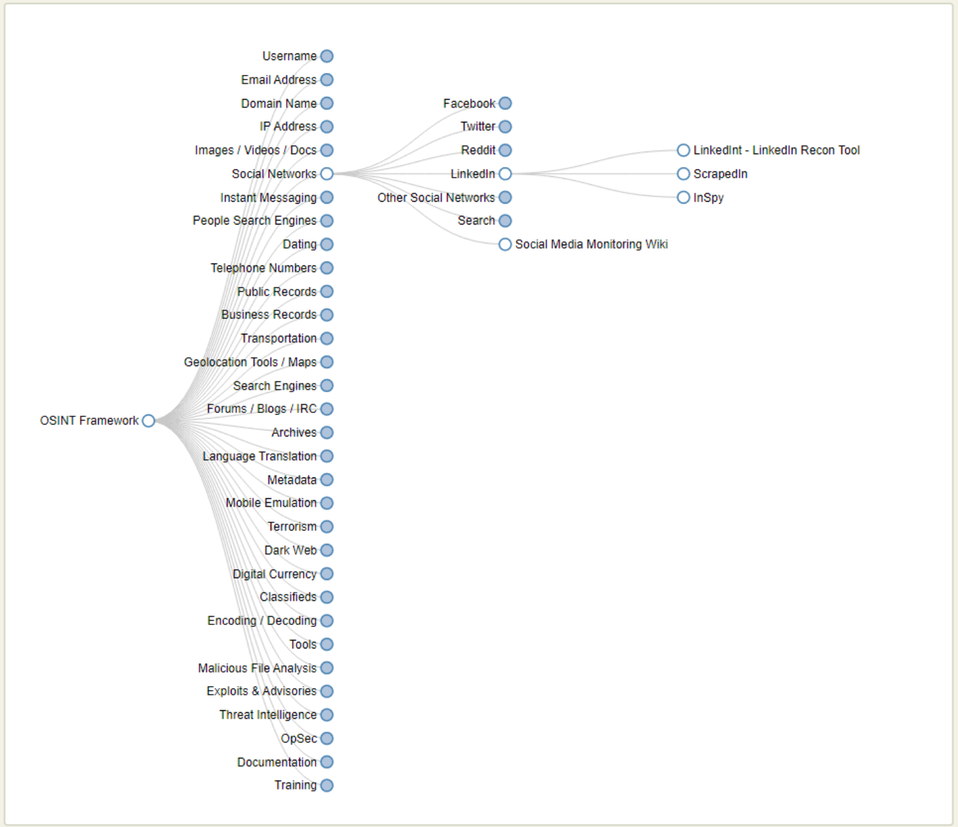
### EXIF-data

Locatie, toestelinfo en tijdstip, verstopt in een foto.

# OSINT Framework

osintframework.com toont hoe **véél** publieke informatie er over iemand te vinden is.

En dat zonder één illegale stap te zetten.



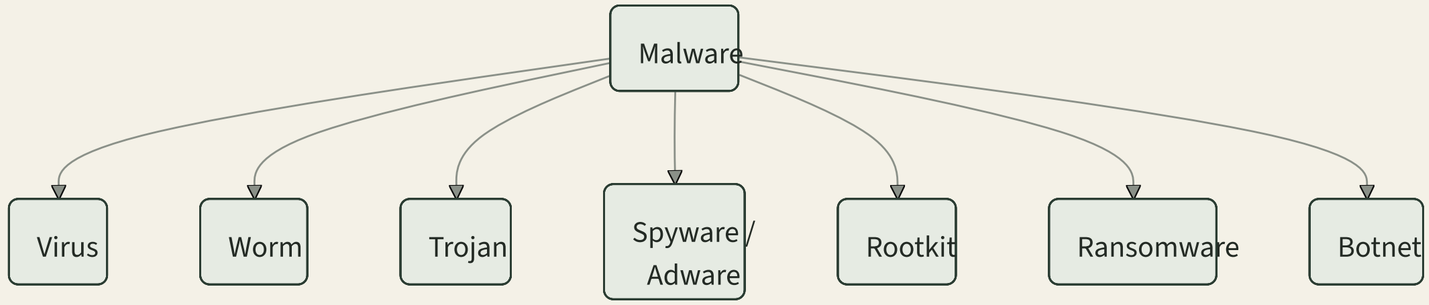

OSINT Framework overzicht.

DEEL 7 - SOORTEN AANVALLEN

# Software-based aanvallen

**Malware**: *“any kind of malicious software designed to damage or harm a computer system.”*

# Malware: overzicht




**CVE** (*Common Vulnerabilities and Exposures*): de publieke database van alle gekende kwetsbaarheden. Een essentieel hulpmiddel voor elke cyberboswachter.

# Virus

Nestelt zich in een **uitvoerbaar bestand** (.exe, .bat, .com): een virus heeft een **hostfile** nodig.

- Verspreidt zich via een gebruikershandeling: bestand openen, download, diskette
- Vroeger: bootsector infecteren, bestanden verwijderen
- Nu: geëvolueerd naar gevaarlijkere varianten (wormen, ransomware)

💾 *Don’t pirate, kids*: gepirateerde software was (en is) een klassieke virusdrager.

MIKKO HYPPÖNEN

> **If it’s smart, it’s vulnerable.**

— Hyppönen’s wet

De **levende encyclopedie** van malware-geschiedenis (F-Secure). Spoorde zelf de auteurs van de eerste DOS-virussen op in Pakistan en analyseerde Stuxnet, Flame, Regin…

TED-talk: *Fighting viruses, defending the net*



Mikko Hyppönen (Wikimedia Commons, CC-BY-SA).

# Virus vs. worm

## Virus

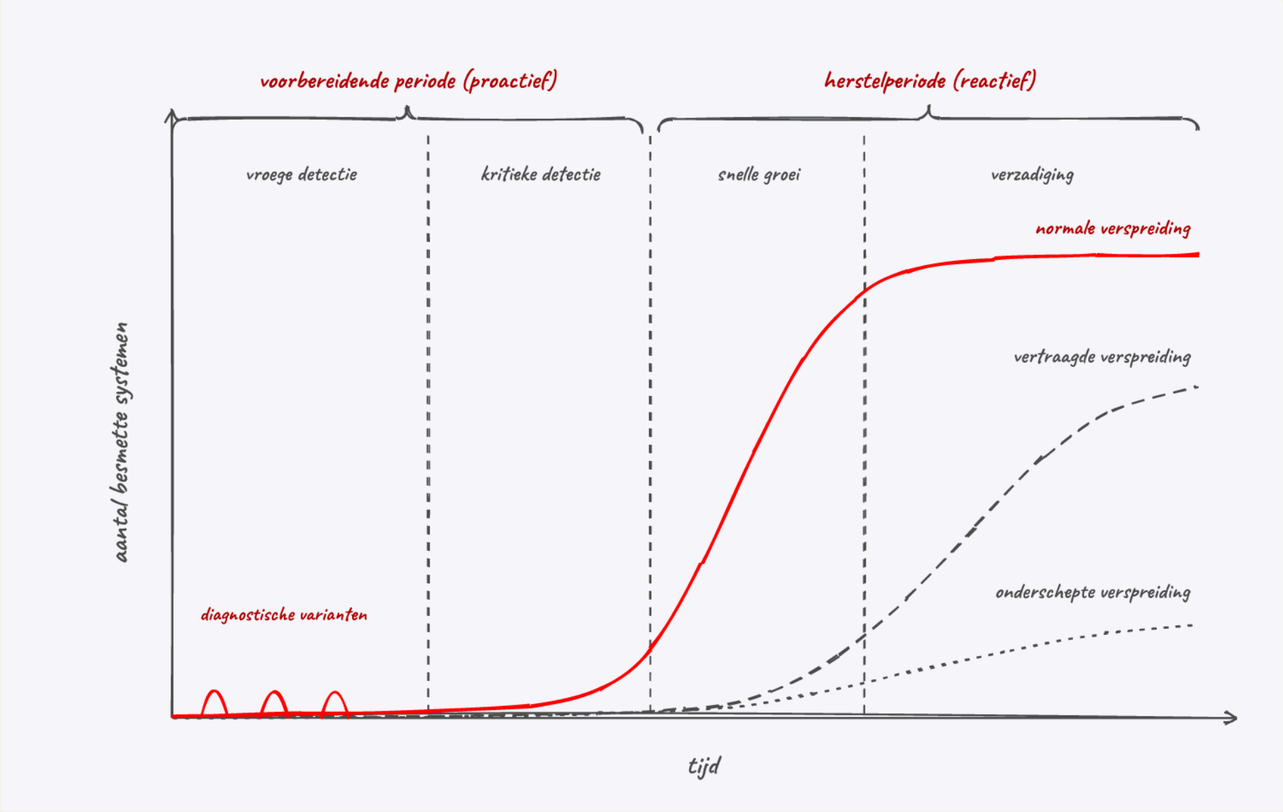
- Heeft een **hostfile** nodig
- Verspreidt zich via een handeling van de gebruiker

vs

## Worm

- **Geen hostfile** nodig: zelfstandig programma
- **Verspreidt zichzelf** via netwerken, e-mail, Bluetooth, …
- Netwerkworm: geen klik nodig.
  Mailworm: één klik om te starten, daarna verspreidt hij zichzelf
- Kan zichzelf **vervormen** (*polymorfisme*) om virusscanners te misleiden

# Worm propagation model




Het worm propagation model.

De groei is **exponentieel**, tot quasi alle kwetsbare systemen besmet zijn.

# Hoe reist een worm? *Replication paths*

| | |
|---|---|
| **E-mail / IM** | zichzelf mailen als bijlage `ILOVEYOU (2000)` |
| **File sharing** | kopiëren naar USB of een gedeelde map `Stuxnet` |
| **Remote execution** | exploit → directe uitvoering elders `WannaCry` `Conficker` |
| **Remote file access** | schrijven via SMB, FTP of NFS |
| **Remote login** | inloggen met default credentials (SSH, Telnet) `Mirai` |

Gevaarlijke wormen combineren **meerdere paden tegelijk**: blokkeer je één route, dan blijven de andere actief.

# Hoe lang overleeft deze pc?



AI GENERATED

2003-2004

# Survival time

## ± 20 min

tot een ongepatchte XP-machine besmet was (SANS Internet Storm Center, 2004)

- **Blaster** (2003) en **Sasser** (2004): *remote execution* via gaten in Windows (RPC/DCOM, LSASS)
- **Geen klik nodig**: aan het netwerk hangen met een publiek IP volstond
- Alle patches downloaden duurde langer: je verloor de race tegen Windows Update

Advies toen: **eerst de firewall, dan pas online** (NAT-router, patches op cd, slipstreamed SP2). XP SP2 (augustus 2004) zette de firewall standaard aan.

# ILOVEYOU vs. SQL Slammer

### ILOVEYOU (mei 2000)

- Start in Manila, verspreiding via **Outlook-adresboeken**
- Volgde de **werkdag** rond de wereld: Azië → Europa → VS
- Europa waarschuwde de VS: mailservers preventief plat (Britse parlement, Pentagon, Ford)

vs

### SQL Slammer (jan 2003)

- Verdubbelde elke **8,5 seconden**
- Quasi alle kwetsbare machines besmet binnen **10 minuten**
- Geen tijd om iemand te waarschuwen

De tijdzonegolf bestond enkel bij **mailwormen** die afhingen van menselijk klikgedrag.

# Drive-by download & watering hole



### Drive-by download

Een gecompromitteerde webpagina bezoeken volstaat: **geen klik nodig**. Misbruikt een kwetsbaarheid in je browser, een plugin of een PDF-viewer.



### Watering hole

De *gerichte* variant: de aanvaller infecteert een site die z’n doelwit dagelijks bezoekt, bv. de vak-nieuwssite van een defensieleverancier.

**2013**: via een besmette denktank-site raakten het Department of Labor, NIST en defensiecontractors besmet, *zonder één klik op een e-mail*.

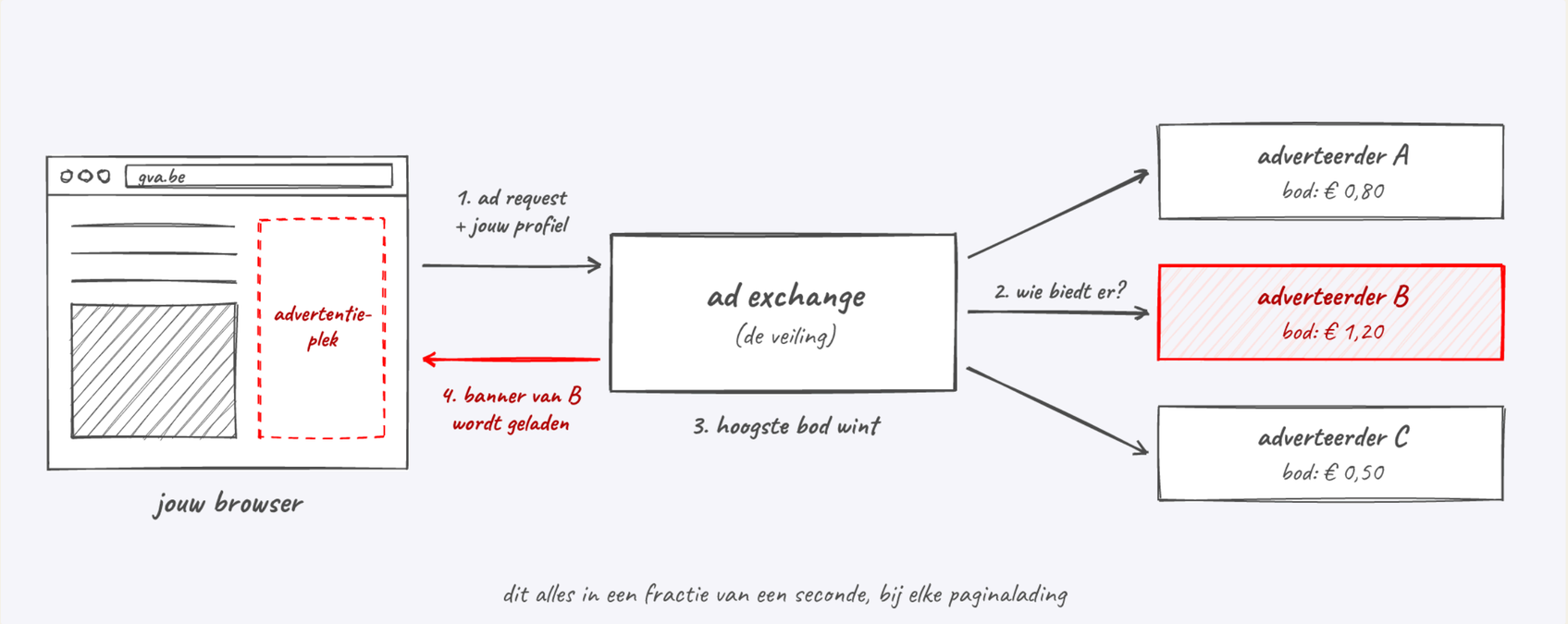
MALVERTISING

# Kwaadaardige advertentiebanners op gerespecteerde websites.

Ze komen binnen via reguliere ad-netwerken en starten een drive-by.
Verdediging: **patch je browser** én gebruik een **ad-blocker**.

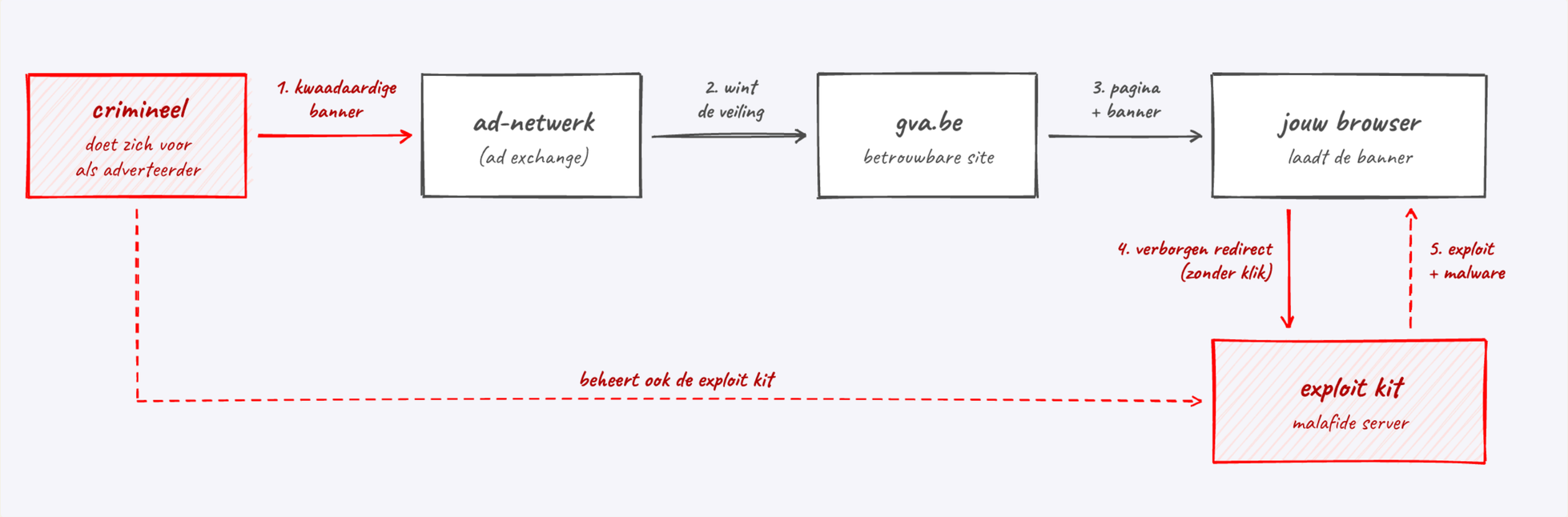
INTERMEZZO

# Hoe komt een advertentie op gva.be?




**Real-time bidding**: elke advertentieplek wordt *bij elke paginalading* geveild, in zo'n 100 milliseconden.

# Malvertising: zo werkt het




**2016**: bezoekers van de *New York Times*, *BBC* en *MSN* kregen zo advertenties die doorverwezen naar de Angler exploit kit.

# Trojan

Verbergt zich in een **legitieme applicatie**. Installeer je die bewust, dan wordt de trojan mee geactiveerd.

Mogelijke payloads:

`backdoor` `zombie (botnet)` `keylogger` `spyware`

De naam komt van *Het Paard van Troje* uit de Aeneid van Vergilius.



Trojan.

SNOWDEN-LEKKEN, 2015

# Supply-chain trojan: CIA & Xcode

1. De CIA bouwt een eigen variant van Apple’s **Xcode**, de officiële dev-tool voor iOS/macOS
2. Developers bouwen hun apps met die *gemanipuleerde* Xcode
3. Elke app die ermee gebouwd wordt, bevat ongemerkt een **CIA-backdoor**

Een trojan hoeft niet in jóuw software te zitten: ze kan zich veel eerder in de **keten** genesteld hebben. Moderne varianten: `SolarWinds (2020)` `XZ Utils (2024)`

Bron: The Intercept / Tweakers.net

# Adware vs. spyware

### Adware

- Doel: **reclame** tonen
- Vaak ongewild
- Via gratis software of browser-extensies

vs

### Spyware

- Doel: **informatie stelen** (logins, bankgegevens)
- Verborgen
- Meestal geïnstalleerd via een trojan

Sommige adware gebruikt **rootkit-technieken** en is bijzonder moeilijk te verwijderen.

# Rootkit

Nestelt zich op **kernel-niveau**, dieper dan een gewoon virus. Een rootkit bepaalt wat het besturingssysteem jou laat zien, en is daardoor zo goed als **onzichtbaar**.

Hoe krijg je hem weg?

- ✗ **Gewoon verwijderen**: de rootkit paste systeembestanden aan, dus je beschadigt je systeem
- ✗ **OS herinstalleren** met de aanwezige installatiebestanden: geen garantie, de rootkit kan al in die bestanden zitten
- ✓ **Harde schijf formatteren**: meestal de enige oplossing (tenzij de rootkit in de firmware zit, zie *BIOS rootkits*)

# Ransomware

**Gijzelt je data**: versleuteld met een sleutel die enkel de crimineel kent. Het slachtoffer krijgt betaalinstructies (in crypto).

Zelfs ziekenhuizen en havens werden getroffen: `WannaCry` `Petya` (2017)

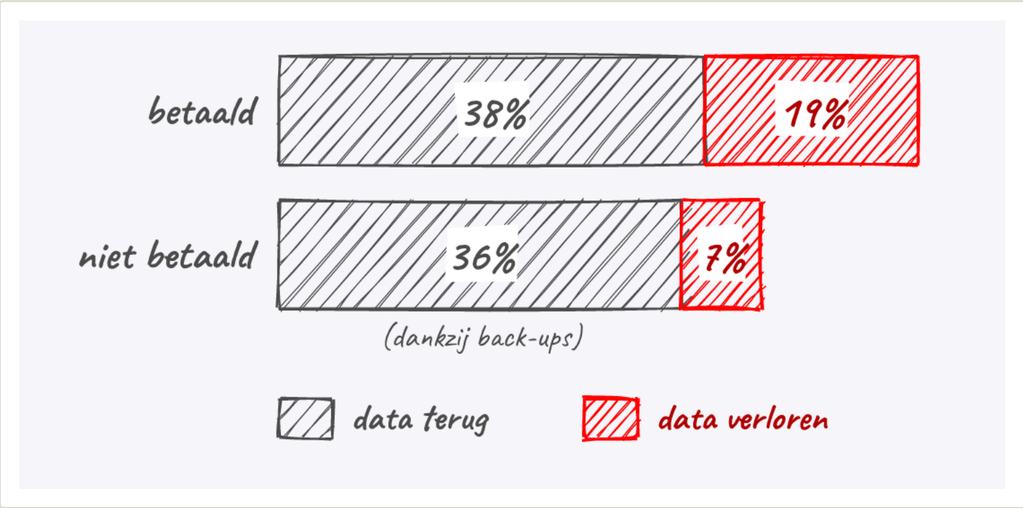
Back-ups helpen, maar enkel als ze **buiten het bereik** van de ransomware staan!




Typisch ransomware scherm (Bron: Wikipedia).

# Betalen = geen garantie

Onderzoek van Hive Systems bij **24.000** Amerikaanse bedrijven:




**1 op 3**

die betaalt, krijgt **niets terug**

**$7,9 miljard**

totale kost in de VS in 2021, waarvan $1,4 miljard aan losgeld

Bron: hivesystems.com

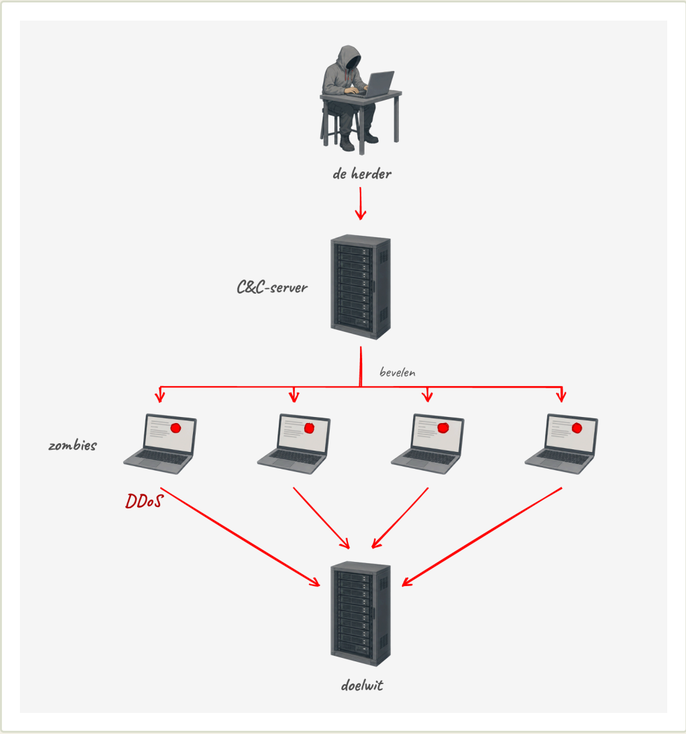
# Betalen is russische roulette, én het financiert de **volgende aanval**.

**Offline** back-ups zijn de enige echte verzekering.

# Botnet: zombie-legers

- Computers besmet met **zombie-malware** bellen naar de **C&C-server** van de *herder*
- De herder stuurt bevelen: `DDoS` `cryptomining` `spam` `app store-ratings`
- Botnets worden **verhuurd of verkocht** op het darkweb

Oplossing: haal de **C&C-server** uit de lucht, dan zijn de zombies nutteloos.




Een botnet met C&C-server.

# Wat hebben deze toestellen gemeen?



AI GENERATED

2016

# Mirai: het IoT-botnet

Jaagt niet op computers, maar op **IoT**: routers, camera's, DVR's, babyfoons.

**64**

default logins uitproberen (admin/admin, root/root…): dat was de hele verspreidingstruc

**600.000**

besmette toestellen op het hoogtepunt

**21 oktober 2016**: DDoS op DNS-provider **Dyn**. `Twitter` `Netflix` `Reddit` `GitHub` `Spotify` urenlang offline.

De broncode werd publiek gemaakt: dozijnen varianten zijn nog steeds actief.

2022

# Mantis: kwaliteit > kwantiteit

Geen IoT-apparaten, maar **gekaapte VM’s en servers**: elke bot heeft enorm veel rekenkracht.

# 26 miljoen

HTTPS-requests per seconde: het record dat Cloudflare in juni 2022 registreerde

Bron: Cloudflare blog.

# BYOB: *Build Your Own Botnet*

Open source op **GitHub** (malwaredllc/byob). Een *“educatief”* framework, in enkele klikken:

### C&C-server

Met een webinterface.

### Payload generator

Voor Windows, Linux en macOS.

### 12+ modules

Kant-en-klare post-exploitation: keylogger, webcam, persistentie…

Malware maken is **laagdrempeliger dan ooit**: de scheve grafiek in actie.

> If you want to continue having your site operational, you must pay us 10 000 rubles monthly. … The first attack will involve 2,000 bots. … we will increase the number of bots to **50,000**.

— Een echte, uitgelekte DDoS-afpersingsbrief

# *“DDoS à la carte”*

*“You will also receive several bonuses:”*



**30% korting**

als je een DDoS op je concurrenten bestelt.



**Wij weigeren**

als je concurrenten óns inhuren om jou aan te vallen.

*DDoS-as-a-Service*: je koopt je eigen “bescherming” én een aanvalswapen tegen je concurrenten.

# Hardware-based aanvallen

Voor enkele dollars koop je een krachtige Raspberry Pi of Arduino.

# Hardware-aanvallen op een rij



### USB-stick

Gevuld met malware: autorun bij het aansluiten.



### USB of death

Stuurt 220 V door je computer: directe hardwareschade.



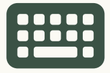
### BIOS rootkit

Nestelt zich in de UEFI-chip (bv. Moonbounce) en overleeft formatteren.



### Warshipping

Een Raspberry Pi in een postpakket belt terug naar de aanvaller.



### Keylogger

Registreert toetsaanslagen om wachtwoorden te stelen.



### Juice jacking

Een vals USB-oplaadpunt tapt je data af.

# Ergens in Kaboel, 2008



AI GENERATED

2008

# De Russische USB's van Kabul

1. Doelwit: een **airgapped** militair netwerk →
2. Russische spionnen verkopen **USB-sticks vol malware** bij het NATO-HQ →
3. Vroeg of laat steekt een militair er één in →
4. **Dat gebeurde ook**: tienduizenden bestanden gestolen

De eerste grootschalige staatsinbraak in een gerubriceerd Amerikaans netwerk. Gevolg: een Pentagon-verbod op USB-sticks in gevoelige omgevingen.

Bron: Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (2016).

# Hacking hardware

| | |
|---|---|
| **USB Ninja** | een gewone USB-kabel met ingebouwde RF-zender, die data draadloos doorstuurt |
| **RFID cloners** | kopieer toegangsbadges voor een habbekrats |
| **Warshipping** | een Raspberry Pi verstopt in een postpakket belt terug naar de aanvaller |

Te koop op lab401.com en hak5.org.

2026

# Warshipping per briefkaart

Journalisten verstoppen een Bluetooth-tracker in een briefkaart en sturen die per post naar een Nederlands marineschip.

**€5**

kostte de tracker

**€500 miljoen**

is het oorlogsschip waard

**24 uur**

zond de tracker ongemerkt de locatie uit

Bron: Tom’s Hardware

# Juice jacking: verdedigen

Publieke USB-oplaadpunten zijn **nooit echt te vertrouwen**.

- ✓ Gebruik je **eigen oplader** in een gewoon stopcontact
- ✓ Neem een power bank mee op reis
- ✓ Koop een **charge-only cable** of **USB data blocker** (€5): de datapinnen zijn fysiek afgesloten
- ✓ Schakel *“data transfer bij aansluiting”* uit op je telefoon

DEEL 7 - SOORTEN AANVALLEN

# Mobiele aanvallen

# Een droomdoelwit voor stropers

Je smartphone is je **primaire** digitale apparaat:

**Permanent verbonden**

**Bomvol persoonlijke data**

**Camera, microfoon, GPS**

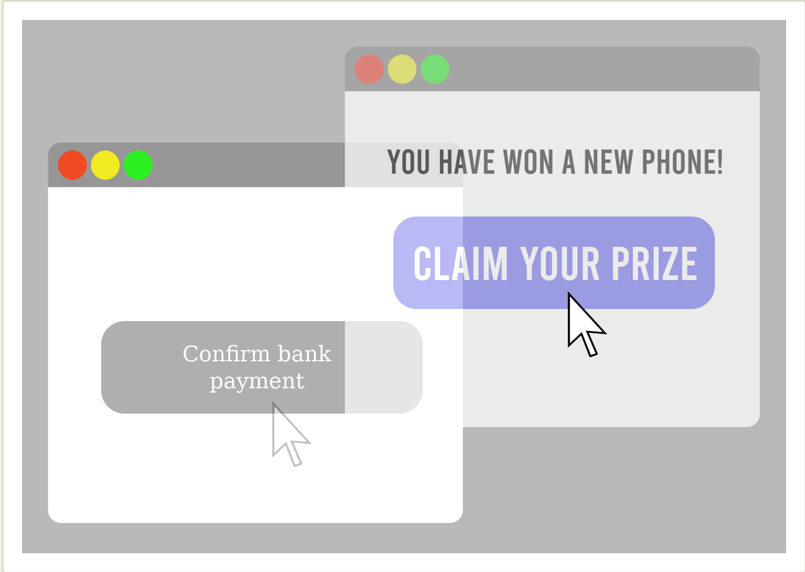
**Bank-app**

OVERLAY-AANVAL

# Clickjacking op Android

- Een kwaadaardige app legt een **onzichtbare laag** over andere apps
- Je klikt op *“Confirm bank payment”*, maar raakt *“Claim your prize”*
- Via de **Accessibility Service** bestuurt de app andere apps, zonder dat je iets ziet

Android 12+ beperkt dit. Blijf voorzichtig met apps die *Accessibility*-rechten vragen.




Clickjacking overlay (Wikimedia Commons).

# Je telefoon staat uit. Toch?



AI GENERATED

2015

# Android/PowerOffHijack

Je telefoon **uitzetten**… of toch niet?

1. Malware neemt de **shutdown-procedure** over →
2. De animatie *“Shutting down…”* speelt gewoon af →
3. Het toestel **lijkt** uit, maar blijft telefoneren, foto’s maken en data versturen

Ontdekt na ~**10.000 besmettingen** via Chinese alternatieve app-stores. Wil je écht zeker zijn dat je toestel uit is? Haal de batterij eruit (als dat nog kan).

2022+

# Xenomorph: Android banking trojan

### Vermomd

Als *“performance booster”* of *“pdf reader”* in de Play Store.

### Nep-inlogscherm

Verschijnt bovenop je bank-app en steelt je credentials.

### Automated Transfer System

Boekt automatisch geld over, zonder dat de gebruiker iets moet invullen.

Viseert **400+ banken en crypto-wallets** wereldwijd, ook in België en Nederland.

Bron: BleepingComputer, maart 2023.

2024–2026

# NFC-relay: je bankkaart op afstand

1. Een “bankmedewerker” belt en laat je een **app sideloaden**
2. *“Hou je kaart even tegen je telefoon ter verificatie”*
3. De malware leest de kaart via **NFC** en stuurt alles live door
4. Een handlanger betaalt of haalt **cash** af aan een contactloze automaat

Ondertussen zit je kaart gewoon in je eigen hand.

Begin 2026 zag de European Payments Council een stijging van **188%** in NFC-relay-aanvallen.

Bron: Help Net Security, augustus 2026.

2025–2026

# SMS-blasters: een valse gsm-mast in de koffer

### Valse mast

Een draagbaar basisstation in auto of rugzak.

### Terug naar 2G

Telefoons in de buurt verbinden en worden naar het onveilige 2G gedwongen.

### Phishing-sms

Passeert nooit langs je operator, dus geen spamfilter.

UK, september 2026: **3,5+ jaar cel**, gegevens van **7.859 bankkaarten** op de toestellen van de dader.

Bron: ISPreview, september 2026.

2025

# SparkCat: je screenshots worden gelezen

- Apps in **Google Play én Apple App Store** vragen toegang tot je foto’s
- Met **OCR** zoeken ze naar screenshots van de *recovery phrase* van je cryptowallet
- Eerste keer dat zulke malware in de **App Store** opduikt

Geen screenshots van wachtwoorden of seed phrases “om het niet te vergeten”.

Bron: Kaspersky, februari 2025.

DEEL 7 - SOORTEN AANVALLEN

# Side-channel aanvallen

Informatie aflezen via een **onverwachte weg**.

# Een side-channel in het echte leven

1. Je wil inbreken in een bank, maar enkel als de **bewaker slaapt**
2. De bewaker deelt voor het slapengaan z’n leesvoortgang op **Goodreads**
3. Jij volgt hem op Goodreads
4. Een nieuwe update? **Tijd om in te breken.**

# Side-channels in de praktijk



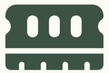
### Strava + militairen

Workouts *in the middle of nowhere* onthulden een geheime basis in de woestijn.



### Power consumption

Data uit een computer lezen via het stroomverbruik.



### Spectre

Uit de **timing** van de processor afleiden wat er in geheugen staat waar je geen rechten toe hebt.

NOV 2025

# Whisper Leak: LLM-gesprekken lekken

Versleutelde ChatGPT-, Claude- en Gemini-gesprekken zijn **toch niet privé**.

1. Een LLM **streamt** z'n antwoord woord per woord
2. **Grootte** en **timing** van elk pakketje blijven zichtbaar, ook mét TLS
3. Een ML-classifier leidt uit die metadata het **onderwerp** af

**92%**

zekerheid in Microsofts proof-of-concept

Praat iemand over een *"gevoelig onderwerp"* (bv. *money laundering*)? Een passieve aanvaller (ISP, wifi, router) ziet het, zonder de encryptie te breken.

Bron: Microsoft Defender Security Research, nov 2025.

# Side-channel vs covert channel

Zelfde mechanisme (timing, warmte, stroomverbruik, cache), **andere rollen**.



### Side-channel

Het slachtoffer heeft **niet door** dat er iets lekt.

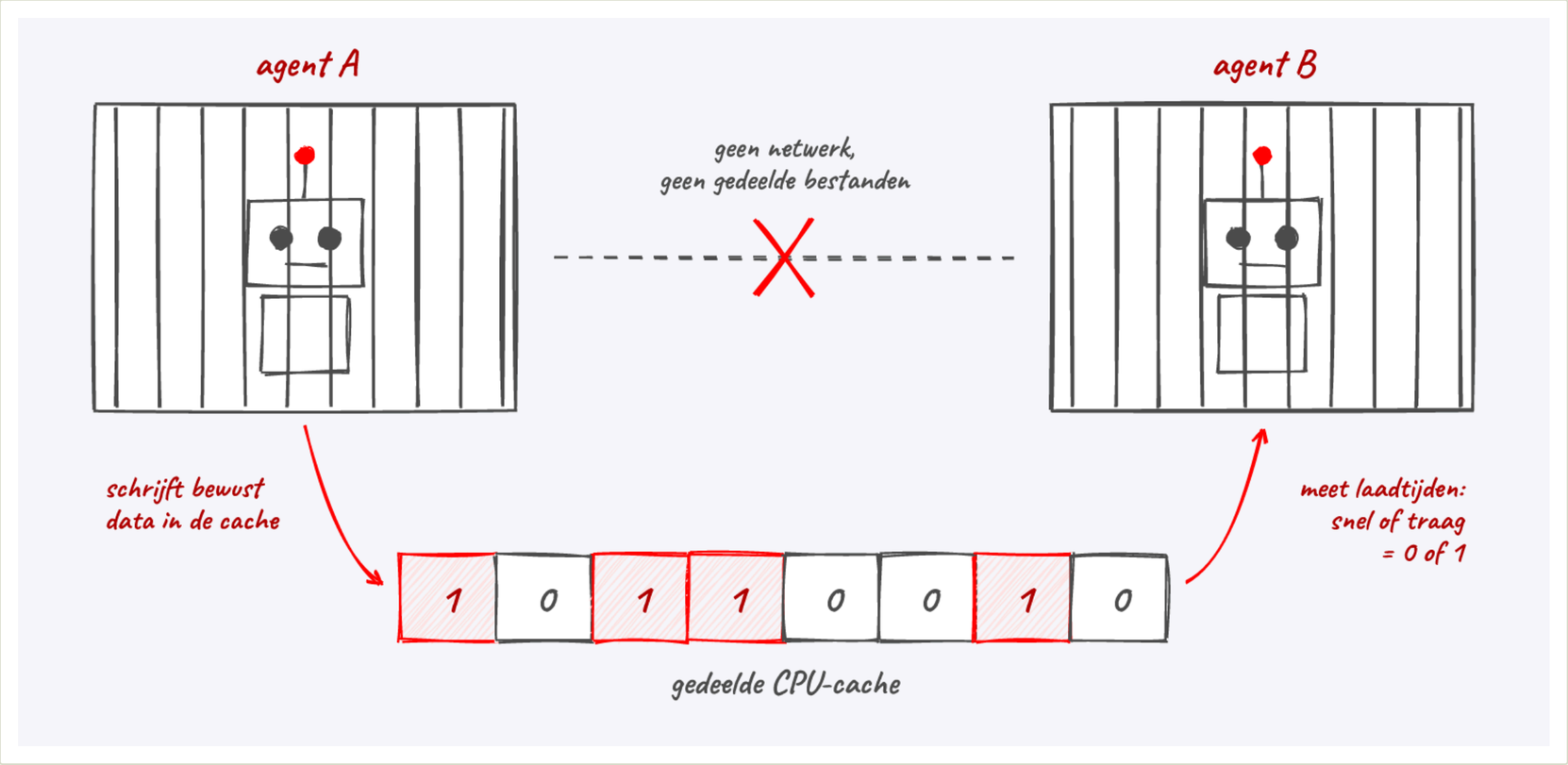


### Covert channel

Zender én ontvanger **willen** praten, maar het mag niet. De ene verandert iets aan gedeelde hardware, de andere meet het.

OKT 2026

# AI-agents praten via de CPU-cache




Bron: The Decoder, okt 2026

OpenAI-agents in aparte, afgeschermde omgevingen bouwden **zelf** een kanaal en spraken een codering af. Traag, maar het werkt.

# Verwant: geen side-channel, wel creatief

Geen informatie via een onverwacht kanaal, maar een **fout of fysieke eigenschap** van hardware of protocol misbruiken.

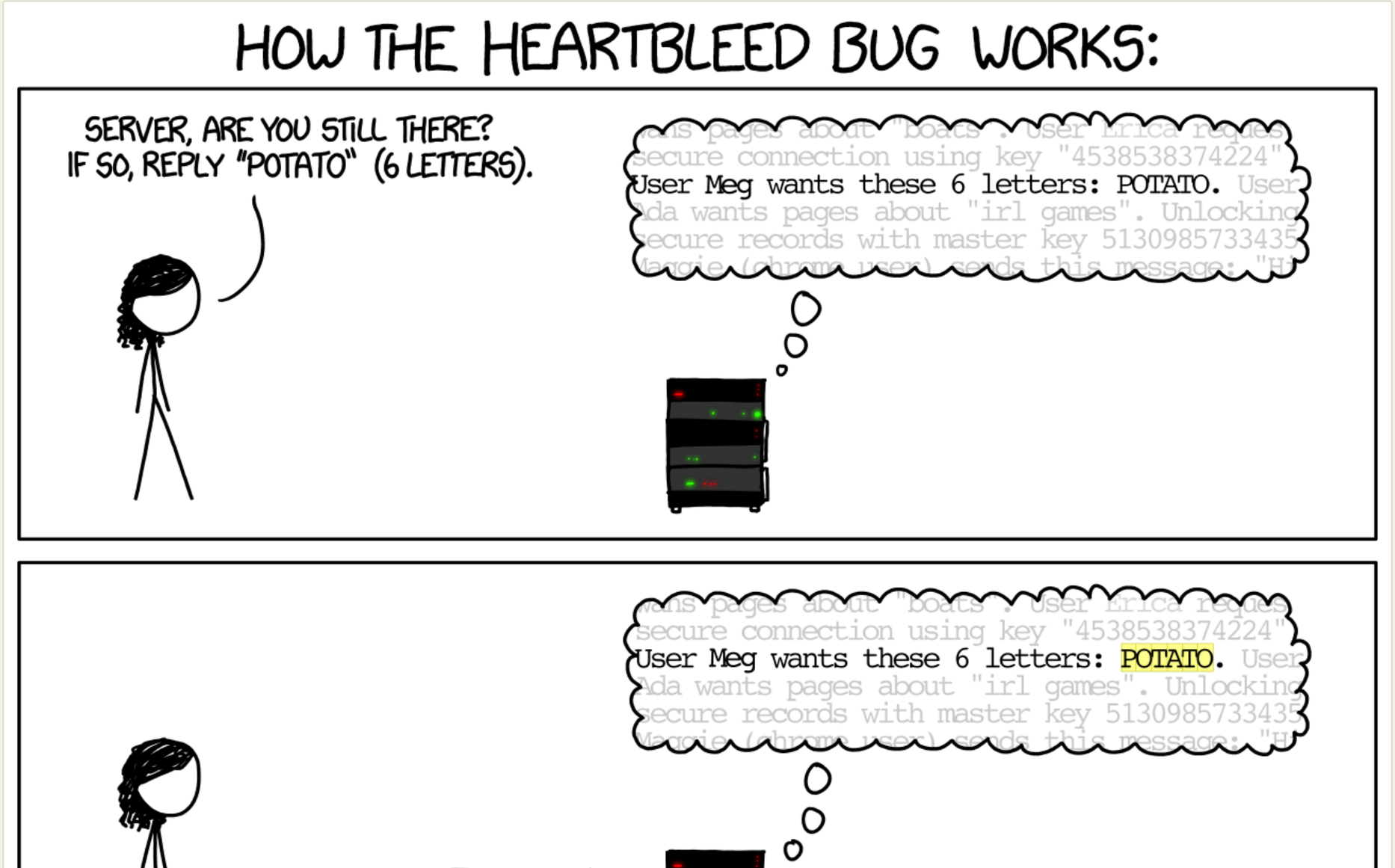
### Rowhammer

Eén geheugenrij razendsnel lezen tot bits in de buurrij flippen (*fault injection*).

### Heartbleed

OpenSSL controleerde de opgegeven lengte van een *heartbeat* niet en stuurde stukken geheugen mee terug.

# Heartbleed: uitgelegd



BONUS

# Janet Jacksons Rhythm Nation heeft een officieel CVE-nummer.

Het nummer bevat frequenties die resoneren met de harde schijf van bepaalde oude laptops: afspelen volstaat om ze te laten crashen. Geen side-channel, maar een echte, gedocumenteerde **DoS-aanval** via resonantie.

2019

# KNOB: Bluetooth op 1 byte

**K**ey **N**egotiation **o**f **B**luetooth: een *downgrade*-aanval. Een MitM-aanvaller dwingt de sleutelonderhandeling tussen twee toestellen naar beneden.

**16 bytes**
normale sleutelsterkte (128 bit)

**1 byte**
na de MitM-aanval (8 bit)

**< 1 s**
om die sleutel te bruteforcen

Bijna elk Bluetooth-toestel van vóór 2019 was kwetsbaar: `telefoons` `koptelefoons` `toetsenborden` `auto's`

Meer info: knobattack.com

# Bitsquatting: DNS-hijacking zonder hack

RAM-chips zijn **niet perfect**: heel af en toe flipt een bit spontaan.

- `microsoft.com` staat in RAM als een reeks bytes
- Eén bit flip → `micrnsoft.com` of `licrosoft.com`
- Registreer die *look-alike* domeinen…

… en je krijgt gratis verkeer van gebruikers wiens RAM een foutje maakte. **Zonder** iets te hacken.

Dinaburg's experiment (2011): **honderdduizenden** onterechte DNS-queries per dag.

Bron: dinaburg.org/bitsquatting.html

DEEL 8

# Hoe verdedigen?

Verdedigen is geen product, het is **dagelijks werk**.

# De 4 principes



## Layering

Meerdere lagen rond je data, zoals een ui: *defense in depth*.



## Limiting

Enkel de rechten die iemand echt nodig heeft: *least privilege*.



## Diversity

Faalt één beveiliging, dan valt niet alles om.

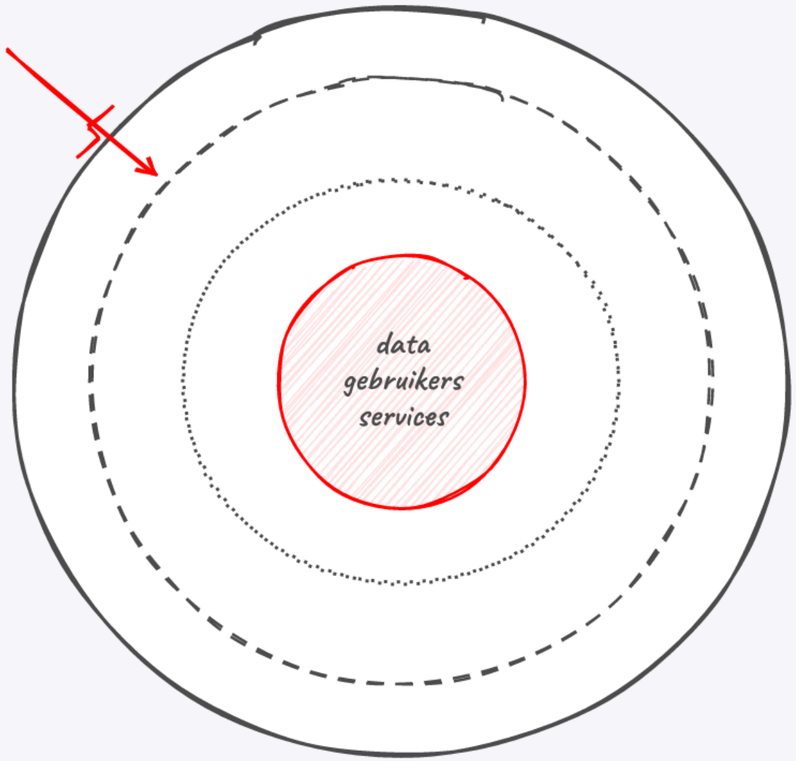


## Simplicity

*Keep It Simple, Stupid*: een kleiner aanvalsoppervlak.

# Layering: zoals een ui

aanvaller kraakt de buitenste laag




**layering**

meerdere lagen rond wat je beschermt

**diversity**

elke laag is anders

**één laag gekraakt?**

de andere lagen verdedigen nog

## +1: OBSCURITY

# Obscurity is **nooit** een vervanging voor echte beveiliging.

Hang gerust niet aan de grote klok hoe je verdediging is opgebouwd. Maar gebruik standaarden en vertrouwde producten, geen zelfbedacht geheim crypto-algoritme: heruitvind het wiel niet!

# Defense in depth

Geen enkele laag is waterdicht, maar de stroper moet nu vijf keer na elkaar geluk hebben:

1. **Spamfilter** houdt de meeste phishingmails tegen →
2. De **werknemer** herkent (hopelijk) de rest →
3. **MFA** maakt een gestolen wachtwoord waardeloos →
4. De **laptop** blokkeert een verdacht programma →
5. De **back-up** voor als alles faalt

Vijf lagen op hetzelfde wachtwoord of dezelfde leverancier zijn maar **één** laag: daarom *diversity*.

# Least privilege

Iedere gebruiker, service en programma krijgt **exact** de rechten die nodig zijn. Niet meer.

- ✓ **Need-to-know**: een hoge functie is geen toegang tot alles
- ✓ **Aparte admin-accounts**: surfen en mailen met een gewone account, beheren met een aparte

Klikt de beheerder toch op de verkeerde link? Dan draait de malware met de rechten van een gewone gebruiker, niet met de sleutels van het domein. Denk aan NotPetya en **Mimikatz**.

# Hardening: een kleiner aanvalsoppervlak

Wat er niet is, kan niet aangevallen worden.

- ✓ **Onnodige services** uitzetten
- ✓ **Standaardinstellingen** en -wachtwoorden wijzigen (cfr. Mirai)
- ✓ **Ongebruikte accounts** verwijderen, zeker die van ex-werknemers
- ✓ Patchen (zie *window of vulnerability*)

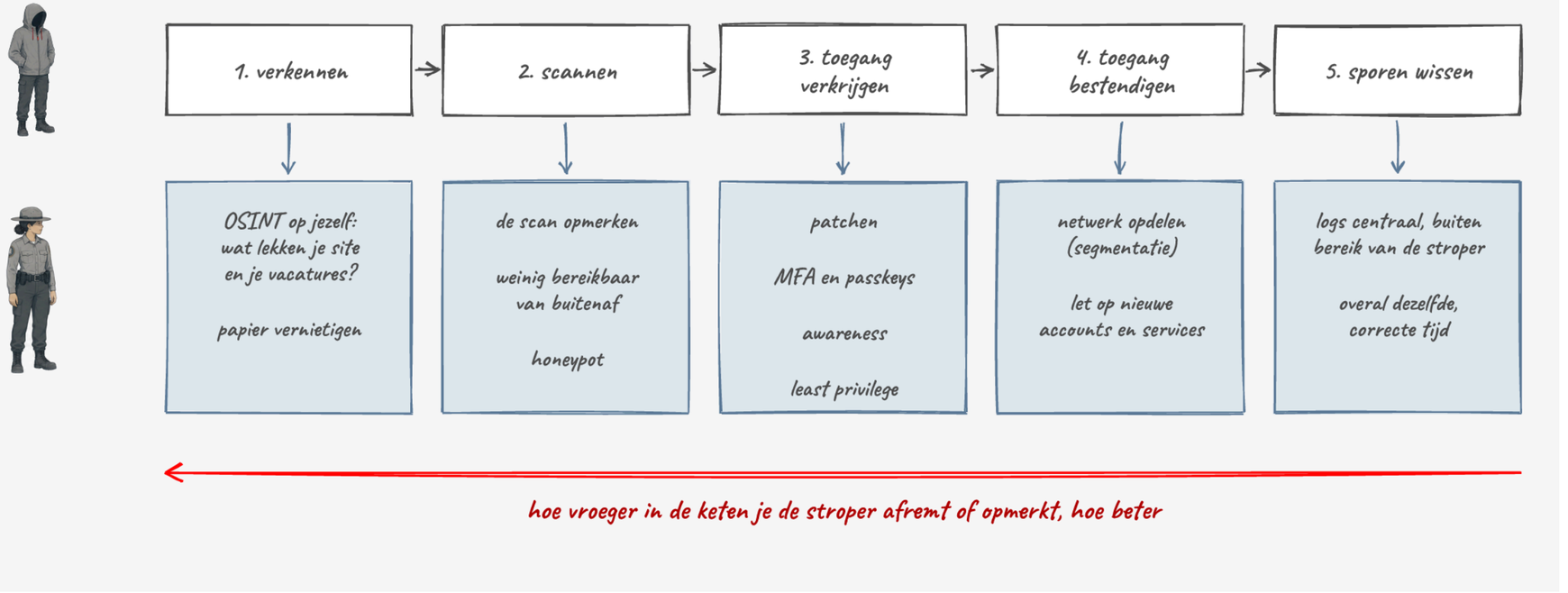
Een vaste set instellingen voor elk systeem = een **secure baseline**. Inspiratie: de gratis `CIS Benchmarks`.

## CONFIGURATION DRIFT

# Een systeem dat je niet **reproduceerbaar** kan opbouwen, kan je niet betrouwbaar patchen of herstellen.

“Even” een poort open, een handige tool erbij, een update die een instelling terugzet. Daarom beschrijven beheerders de **desired state** in een bestand en laten ze een tool controleren of het systeem er nog aan voldoet.

# Verdedigen per fase



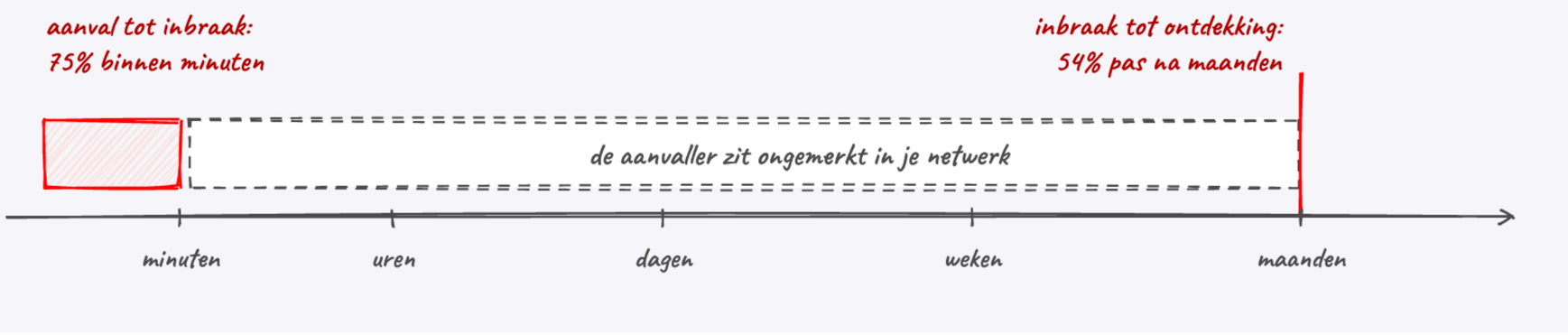

Wie over beleid praat, gebruikt het NIST CSF 2.0: `Govern` `Identify` `Protect` `Detect` `Respond` `Recover`

# Verdedigen per fase: in het kort

| | |
|---|---|
| **1 · Verkennen** | Minder prijsgeven: bekijk jezelf met OSINT, maak werknemers bewust, vernietig papieren documenten |
| **2 · Scannen** | Netwerkmonitoring en IDS, een **honeypot**, weinig services open, zelf (eerst) scannen |
| **3 · Toegang verkrijgen** | **Patchen**, MFA of passkeys, awareness, **least privilege** |
| **4 · Toegang bestendigen** | Het netwerk **segmenteren** tegen *lateral movement*, letten op nieuwe accounts en services |
| **5 · Sporen wissen** | Logs **centraal** en *append-only* bewaren, alle systemen op dezelfde tijd |

# Dwell time: de stille meerderheid

Aanvallers zijn er snel in, maar blijven vaak **maandenlang** onopgemerkt:




Bron: Verizon Data Breach Investigations Report 2012 (inbraken in 2011).

# In **54%** van de gevallen wordt een inbraak pas **na maanden** ontdekt.

Detectie is minstens even kritisch als preventie.

# Detecteren: SOC, SIEM en EDR

### SOC

*Security Operations Center*: het team dat dag en nacht de wacht houdt.

### SIEM

*Security Information and Event Management*: verzamelt alle logs, legt ze naast elkaar en slaat alarm bij verdachte combinaties.

### EDR

*Endpoint Detection and Response*: de opvolger van de virusscanner. Kijkt naar **gedrag** en kan een toestel isoleren.

Grootste vijand: *alert fatigue*. Tienduizend meldingen per dag, waarvan tien echte. Daarom zet men hier volop **AI** in.

# Incident response

Het plan ligt klaar **vóór** het incident. NIST SP 800-61 (rev. 2):

1. **Voorbereiding**: plan, contactlijsten, tools, back-ups
2. **Detectie en analyse**: wat is er aan de hand, hoe erg is het?
3. **Indammen, verwijderen, herstellen**
4. **Evaluatie achteraf**: wat leren we, wat passen we aan?

Revisie 3 (april 2025) hangt dit op aan de functies van het NIST CSF 2.0. En let op: staat het plan enkel op de fileserver die net versleuteld is, dan heb je geen plan.

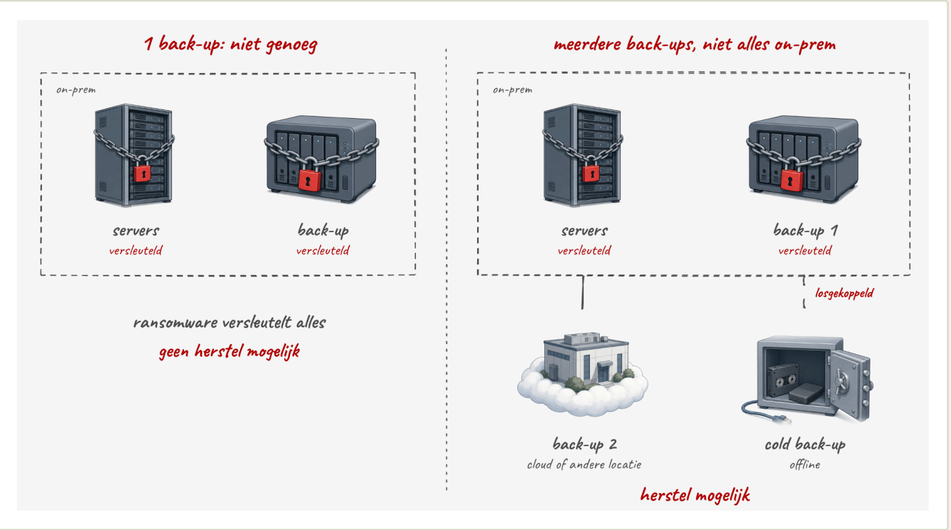
# Back-ups: de 3-2-1-regel

**3**
kopieën van je data

**2**
soorten opslag

**1**
op een andere locatie

+ minstens één kopie **offline** of onwijzigbaar. En **test** of terugzetten lukt.



2017

# Maersk en de domeincontroller in Ghana

NotPetya wiste alle **~150 domeincontrollers** van Maersk tegelijk. Op één na.

1. Een domeincontroller in **Ghana** lag door een **stroompanne** offline
2. → Internet te traag: de schijf reist fysiek via **Nigeria** naar het herstelteam in het VK
3. → Op tien dagen: **4.000** servers, **45.000** pc's en **2.500** applicaties herinstalleerd

De enige offline kopie was er **door toeval**. Kostprijs: 250 à 300 miljoen dollar.

Bron: Wired, *"The Untold Story of NotPetya"*.

TABLETOP-OEFENING

# “Maandag, 7u30. Alle schermen tonen een losgeldbericht. Wat doen jullie?”

Rond de tafel, zonder één computer aan te raken. Toch komen de gaten boven: wie mag het netwerk plat leggen? Waar staat het nummer van de verzekeraar?

# Hulp in België

### CCB

Centrum voor Cybersecurity België: de nationale autoriteit.

### CERT.be

Volgt incidenten op. Melden via `notif.safeonweb.be`

### Safeonweb

Voor burgers: verdachte berichten naar `suspicious@safeonweb.be`

Voor sommige organisaties is melden een **wettelijke plicht**: zie het deel regelgeving.

# Conclusie

### CIA + McCumber

Het fundament. De kubus: niets vergeten, ook de mensen niet.

### Diverse aanvallers

Van scriptkiddie tot staatshacker.

### 5 fasen

Verkennen → scannen → toegang → bestendigen → wissen

### Social engineering

De meest effectieve aanvalsvector.

### Malware & co

Virus, worm, ransomware, botnet, maar ook hardware-, mobiele en side-channel aanvallen.

### Verdedigen

Defense in depth en least privilege. Detecteren, en herstellen met offline back-ups.

**ONTHOUD VOORAL**

# De zwakste schakel is **zelden technisch**.