

# Security

Tuur Vanhoutte

20 november 2020

# Inhoudsopgave

<b>1</b>	<b>Security</b>	<b>1</b>
1.1	Doel . . . . .	1
1.2	Waarom? . . . . .	1
1.3	Tegenmaatregelen . . . . .	1
1.4	Risico . . . . .	1
1.5	Theoretisch model . . . . .	2
1.5.1	Voorbeelden . . . . .	2
1.6	Bedreiging vs kwetsbaarheid . . . . .	2
1.6.1	Bedreigde doelen . . . . .	3
<b>2</b>	<b>Bedreigingen</b>	<b>3</b>
2.1	Voorbeelden . . . . .	3
2.2	Types . . . . .	3
2.3	Phishing . . . . .	4
2.3.1	Geavanceerde vormen van phishing . . . . .	4
2.3.2	Andere vormen van phishing . . . . .	4
2.3.3	Phishing herkennen . . . . .	5
2.4	Smishing . . . . .	5
2.5	Vishing . . . . .	5
2.6	Money mule . . . . .	5
2.7	Malware . . . . .	6
2.8	Ransomware . . . . .	6
2.8.1	Voorbeelden . . . . .	6
2.9	Hardware uit onbetrouwbare bron . . . . .	6
2.10	Vreemde netwerken . . . . .	6
2.11	Social engineering . . . . .	7
2.12	Bedreigingen: 'Agenten' . . . . .	7
2.12.1	De ontslagen werknemer . . . . .	7
2.12.2	De 'hacker' . . . . .	7
2.13	Bedreigingen: gebeurtenissen . . . . .	8
2.14	Threat intelligence . . . . .	8
<b>3</b>	<b>Beveiligen</b>	<b>9</b>
3.1	Herhaling: kwetsbaarheden . . . . .	9
3.2	Shodan search engine demo . . . . .	9
3.3	ICT security . . . . .	9
3.3.1	Usability vs Security . . . . .	9
3.4	Tegenmaatregelen (mitigation) . . . . .	10
3.4.1	Defense in depth strategie . . . . .	10
3.5	ICC / Belgian Cyber Security Guide . . . . .	10
<b>4</b>	<b>Beveiligen van toegang</b>	<b>10</b>
4.1	Authorisatie vs authenticatie . . . . .	10
4.2	Beveiligingsbasissen . . . . .	11
4.3	Beveiliging op 'Weten'-basis: wachtwoorden . . . . .	11
4.3.1	Entropie . . . . .	11
4.3.2	Tips . . . . .	12
4.4	Beveiliging op 'Hebben'-basis . . . . .	12
4.5	Beveiliging op 'Zijn'-basis': biometrische beveiliging . . . . .	12
4.6	Combinatie van meerdere authenticatiemethodes . . . . .	12

4.7	Fysische toegang . . . . .	12
4.8	Privilege escalation . . . . .	13
<b>5</b>	<b>Backup</b>	<b>13</b>
5.1	Veelgebruikte backup-media . . . . .	13
5.2	LTO Tapes . . . . .	13
5.2.1	LTO Drive . . . . .	14
5.3	Eigenschappen van een correcte backup . . . . .	14
5.4	3-2-1 regel . . . . .	14
5.5	Cloud back-up . . . . .	14
5.6	Back-up policy . . . . .	15
5.6.1	Grootvader - vader - zoon-systeem . . . . .	15
5.7	Belangrijk . . . . .	16
<b>6</b>	<b>Penetration testing</b>	<b>16</b>
6.1	Black-box testing vs white-box testing . . . . .	16
6.1.1	Black-box testing . . . . .	16
6.1.2	White-box testing . . . . .	16
6.2	Fase 1: Reconnaissance . . . . .	16
6.2.1	Tools & attack surfaces . . . . .	17
6.3	Fase 2: Network scanning . . . . .	17
6.3.1	Network reconnaissance . . . . .	17
6.4	Fase 3: Vulnerability assesement . . . . .	17
6.5	Fase 4: Exploit, Access, penetratie . . . . .	18
6.6	Fase 5: Maintaining access . . . . .	18
<b>7</b>	<b>Sociale media</b>	<b>18</b>
7.1	Metadata . . . . .	18
<b>8</b>	<b>Social engineering</b>	<b>18</b>
8.1	Pretexting . . . . .	19
8.1.1	Hoe? . . . . .	19
8.2	Informatielekken . . . . .	19
8.2.1	Remediering . . . . .	19
8.3	Afluisteren . . . . .	19
8.3.1	Man in the middle attack . . . . .	19
8.3.2	Remediering . . . . .	20
<b>9</b>	<b>Wireless</b>	<b>20</b>
9.1	Vreemde netwerken . . . . .	20
9.2	Frequentie . . . . .	21
<b>10</b>	<b>Virussen en malware</b>	<b>21</b>
10.1	Virussen . . . . .	21
10.1.1	Virustechnologie . . . . .	21
10.2	Malware . . . . .	22
10.3	Hardware . . . . .	22
10.3.1	BIOS . . . . .	22
10.3.2	UEFI . . . . .	22
10.4	Misleidende informatie . . . . .	22
10.4.1	Kwaadaardige links . . . . .	23
<b>11</b>	<b>Cloud en Software As A Service (SaaS)</b>	<b>23</b>

11.1 Cloud diensten . . . . .	24
11.2 Acceptabel gebruik / Policy . . . . .	24
11.3 Migratie naar cloud diensten . . . . .	24
11.3.1 Voordelen / Unique Selling Point (USP) . . . . .	25
11.3.2 Nadelen . . . . .	25
<b>12 Bring Your Own Device (BYOD)</b>	<b>25</b>
12.1 Problemen . . . . .	25
12.2 Mobiele apparaten . . . . .	25
12.2.1 Mobile malware . . . . .	26
<b>13 Beschikbaarheid</b>	<b>27</b>
13.1 High Availability . . . . .	27
13.2 Externe netwerk bedreigingen . . . . .	27
13.2.1 Denial of Service (DoS) . . . . .	28
13.2.2 Distributed DoS (DDOS) . . . . .	29
13.2.3 Spoofing . . . . .	29
13.3 Uptime . . . . .	30
<b>14 Examenvragen</b>	<b>30</b>

# 1 Security

## 1.1 Doel

- Security awareness (bewustwording)
- Correcte nomenclatuur (communicatie)
- Advies over verantwoordelijkheden
- Inzien v/d consequenties v/h falen van security
- Situeren en herkennen van problemen
- Oplossingen correct implementeren
- Correcte methodieken toepassen

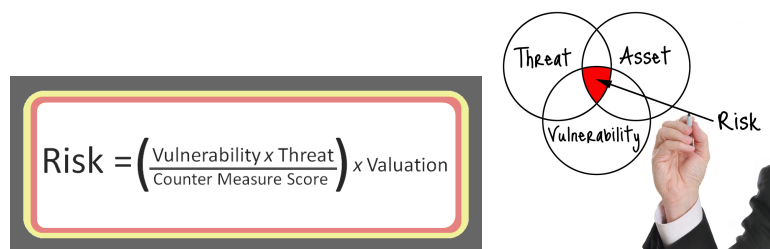
## 1.2 Waarom?

- Niet iedereen heeft even goede bedoelingen
- Grote hoeveelheid mensen = veel potentiële slachtoffers (internet == iedereen zeer bereikbaar)
- Er is geen magische one-size-fits-all oplossing
- Verantwoordelijkheid van iedereen
- Tegenmaatregelen nemen
- Alert en voorzichtig zijn

## 1.3 Tegenmaatregelen

- Zijn slechts nuttig indien ze effectief worden gebruikt
- Lijken vaak in de weg te zitten of lastig, maar zijn noodzakelijk

## 1.4 Risico



Figuur 1: Risico

- De mate van bedreiging is niet beheersbaar
- De kwetsbaarheid is te reduceren door de implementatie van tegenmaatregelen
- Tegenmaatregelen reduceren kwetsbaarheid
- Bedrijfsimpact van het risico bepaalt de opportuniteit van de beveiligingsinvestering

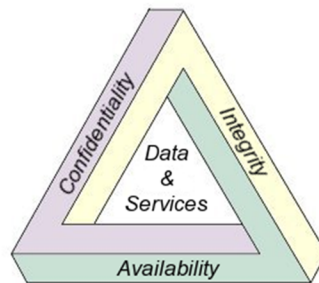
- Bepalen van de financiële impact van een incident is uitermate bedrijfsspecifiek

## 1.5 Theoretisch model

### WORDT GEVRAAGD OP EXAMEN

#### CIA-model

- Confidentiality (Vertrouwelijkheid)
- Integrity (Integriteit)
- Availability (Beschikbaarheid)



Figuur 2: CIA-model

**Vertrouwelijkheid:** gegevens kunnen *enkel* door de juiste partijen worden geraadpleegd.

**Integriteit:** gegevens zijn vaststaand en veranderen niet, tenzij de juiste, gemachtigde personen ze veranderen.

**Beschikbaarheid:** de gegevens zijn beschikbaar en te bekijken door de juiste partijen, ongeacht aanvallen zoals DDOS-attacks.

[https://en.wikipedia.org/wiki/Information\\_security#Confidentiality](https://en.wikipedia.org/wiki/Information_security#Confidentiality)

[https://en.wikipedia.org/wiki/Information\\_security#Integrity](https://en.wikipedia.org/wiki/Information_security#Integrity)

[https://en.wikipedia.org/wiki/Information\\_security#Availability](https://en.wikipedia.org/wiki/Information_security#Availability)

#### 1.5.1 Voorbeelden

TODO

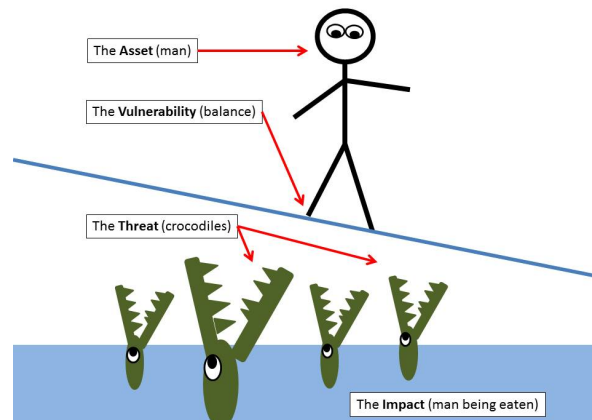
## 1.6 Bedreiging vs kwetsbaarheid

**Bedreiging (threat)** = potentiële negatieve actie dat een ongewenste impact heeft op een computersysteem of applicatie.

**Kwetsbaarheid (vulnerability)** = zwak punt in een computersysteem of applicatie die kan worden geëxploiteerd.

### 1.6.1 Bedreigde doelen

- Infrastructuur
- Gegevens
- Operationaliteit



Figuur 3

## 2 Bedreigingen

- Vallen 1 of meerdere doelen aan
- Kunnen toevallig of kwaadwillig beraamd zijn
- Gaan uit van 'agenten' (personen/organisaties) of gebeurtenissen

### 2.1 Voorbeelden

- Phishing
- Smishing
- Vishing
- Money rules
- Malware
- Hardware uit onbetrouwbare bron
- Social engineering
- ...

### 2.2 Types

- Systeemfouten
- Gebeurtenissen

- Brand
- Stroomuitval
- Intern
  - Diefstal
  - Wraak
- Extern
  - ‘Hackers’
  - Spionage

## **2.3 Phishing**

- Oplichting over email
- Vaak onwaarschijnlijk verhaal
- Vaak herkenbaar malifide links
- Soms bijzonder moeilijk herkenbaar
- Is de meest voorkomende vorm van fraude
- Is de meest uitgebuite kwetsbaarheid van een organisatie
- Zo veel mogelijk mensen bereiken, hopen dat een paar mensen toehappen.

### **2.3.1 Geavanceerde vormen van phishing**

- Spear phishing
  - doelgerichter
  - specifiek
  - afzender spoofen naar iemand die het slachtoffer persoonlijk kent, slachtoffer aanspreken met echte naam
- Double barrel attack
  - Double barrel = tweeloopsgeweer
  - Twee emails sturen: 1 heel duidelijk spam, de andere een reactie van de organisatie (bvb bank) die vraagt om op te letten voor phishing mails.
  - De tweede mail bevat vaak een link om je wachtwoord te veranderen ⇒ link naar valse site

### **2.3.2 Andere vormen van phishing**

- Bank card phishing
- CEO-Fraude
  - Impersoneren van een CEO om in zijn/haar naam een actie te verrichten
  - Bvb: leverancier contacteren om betaling op ander rekening nummer te storten
- Factuurfraude



- Vroeger: een echte factuur uit een brievenbus nemen, rekeningnummer veranderen en opnieuw in de bus doen
- Tegenwoordig: valse facturen opsturen via email

### **2.3.3 Phishing herkennen**

- Afzender controleren
- Taalgebruik
- Datum controleren: in het weekend moeilijker om om hulp te vragen aan de echte organisatie
- Slachtoffer afschrikken met gerechtelijke stappen ondernemen
- Specificeren van extra informatie (bv: u heeft op maandag 01/02/2020 om 16:04 x gedaan, daarom moet u nu y betalen)
- Slachtoffer moet stappen ondernemen om de situatie niet nog erger te maken
- Gebruik van legitieme bedrijven om de transactie te voltooien (bv iTuneskaarten, Google Play kaarten, [www.becharge.be](http://www.becharge.be))

## **2.4 Smishing**

Oplichting via: ...

- SMS
- Whatsapp
- Facebook
- ...

## **2.5 Vishing**

= Voice Sollicitation

- Mensen bellen je op en maken je wijs dat ze u willen helpen om een probleem op te lossen
- Vaak pc overnemen met teamviewer en dergelijke
- Geld vragen om pc te 'herstellen'
- Zie ook: refund scams, IRS scams, ...

## **2.6 Money mule**

= iemand die zijn/haar bankrekening laat misbruiken voor criminele activiteiten.

- De crimineel contacteert het slachtoffer met een jobaanbieding
- De job bestaat uit het overschrijven van bedragen via zijn/haar bankrekening
- Voor elke overschrijving

## **2.7 Malware**

= Software met als doel kwaad te berokkenen

- Trojan
- Adware
- Virus / worm
- Ransomware
- Browser Malware
- Ook op smartphone

## **2.8 Ransomware**

Maakt de data op je PC onbruikbaar tot je losgeld betaalt aan de criminelen.

- 'Kidnappen' van bestanden: bestanden openen niet langer mogelijk
- Poging tot innen van losgeld
- Vaak via phishing
- Enkel een backup van de gegevens kan voldoende beschermen

### **2.8.1 Voorbeelden**

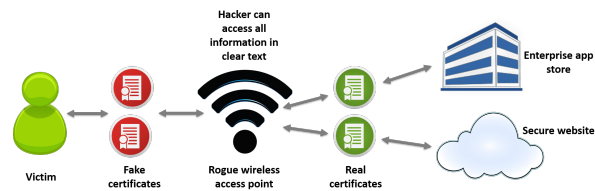
- Wildfire\_locker
- Wannacry
- Cryptolocker
- Bad Rabbit

## **2.9 Hardware uit onbetrouwbare bron**

- USB Rubber ducky
  - USB-stick die ergens gedropt wordt (= drop attack), het slachtoffer vindt de USB stick en stopt hem in zijn/haar computer (bvb uit nieuwsgierigheid).
  - De USB stick werkt als een toetsenbord en typt een attack script op de pc van het slachtoffer
  - Doel: volledige controle over PC, met bvb remote access (RAT = Remote Access Tool).

## **2.10 Vreemde netwerken**

- Openbare netwerken kunnen worden afgeluisterd
- Verkeer op niet-vertrouwde netwerken kan worden omgeleid



Figuur 4: Vreemde netwerken

## 2.11 Social engineering

Een techniek waarbij een crimineel een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken.

## 2.12 Bedreigingen: 'Agenten'

- Entiteiten waarvan de bedreiging uitgaat
- Zijn intern (=werknemers) of extern aan het bedrijf
- Kwetsbaarheid voor een agent wordt bepaald door zijn:
  - Toegangsniveau
  - Kennis
  - Motivatie

### 2.12.1 De ontslagen werknemer

- Heeft toegang (nog steeds?) tot de organisatie
- Heeft kennis over de werking van de organisatie
- Heeft een sterke negatieve motivatie

### 2.12.2 De 'hacker'

De stereotiepe 'hacker':

- De blueprint opgevoerd door de media
- Is gebaseerd op reële figuren
- Vormt een rolmodel voor een bepaalde subcultuur
- Het woord 'hacker' is vaak nietszeggend
- 'Script kiddies', 'Wannabees', 'Crackers'
- Bedreiging groot door grote aantallen
- Hoofddeksels (hacker ethics):
  - Black hat (=informatiecrimineel, voor persoonlijk gewin)
  - White hat ('for the greater good', 'etische hacker')
  - Gray hat (iets tussen de twee)

De 'ethical' hacker = iemand die beveiligingen breekt om te tonen dat ze onveilig zijn

- Goed of slecht voor security?
- Vb: security by obscurity (= niemand weet hoe het werkt dus het is veilig  $\Rightarrow$  reeds vele malen slecht idee gebleken)
- Penetration testing (= verificatie van beveiliging, maar: mag niet ongevraagd, anders illegaal)
- Soms grijze zone
- Meldingsplicht? Welke wetgeving?
- Responsible disclosure: firma inlichten ipv volledig internet

## 2.13 Bedreigingen: gebeurtenissen

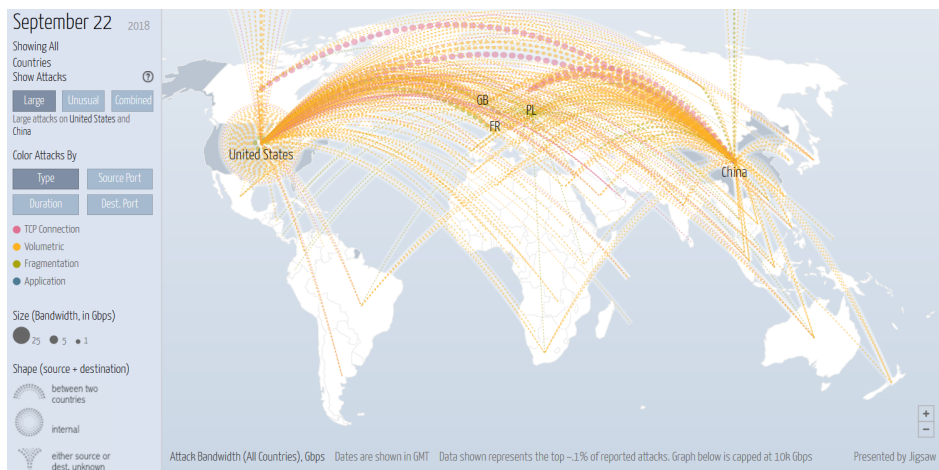
- Brand
- Stroomuitval
- Overstroming
- Diefstal
- Aanslag

## 2.14 Threat intelligence

- 'Know your enemy'
- Noodzakelijk om risico in te schatten
- Bijgevolg elementair om te beslissen over opportuniteit van **tegenmaatregelen**

Real-time maps

- <https://www.fireeye.com/cyber-map/threat-map.html>
- <http://cybermap.kaspersky.com/>
- <http://map.ipviking.com/>



Figuur 5: Threat intelligence

## 3 Beveiligen

### 3.1 Herhaling: kwetsbaarheden

- Software vulnerabilities
  - Geen updates
  - Foutief patch management
- Interne toegang
  - Misbruik machtigingen
  - Wraak / ontslaan van werknemer
- Extern bereikbare diensten
- Phishing / spear phishing
  - The human factor
  - Meest gebruikte entypoint
  - Email (SMTP) is niet geauthentiseerd

### 3.2 Shodan search engine demo

- <http://www.shodanhq.com>
- Zoekt naar geconnecteerde devices
- Webcams, videofoons, windturbines, waterkrachtcentrales, PLC's, ...

### 3.3 ICT security

- Is zeer complex
- Omvat erg veel, zeer diverse kennisdomeinen
- Wordt erg vaak over-gesimplificeerd

#### 3.3.1 Usability vs Security

##### Extremen:

- Totale security is enkel mogelijk bij onbestaande usability
- Optimale usability is enkel mogelijk bij onbestaande security

In elke security implementatie zijn deze 3 factoren nodig:

1. Security
2. Functionality
3. Ease of Use

We moeten zoeken naar een gebalanceerde compromis voor alle stakeholders.

Een bruikbare infrastructuur kan nooit 100% veilig zijn ⇒ voorzichtig afwegen van alle parameters en belangen.

**Voorbeeld:** een fingerprint reader: handig, maar niet zo veilig. Iemand met slechte bedoelingen kan de vingerafdruk kopiëren.

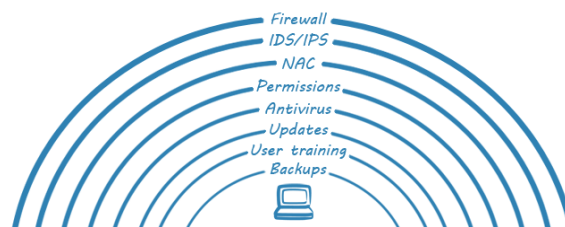
### 3.4 Tegenmaatregelen (mitigation)

- Corporate policy - Training - Awareness
- Coding practices
- Testing (Pentesting)
- Vulnerability management
- Backup
- Disaster recovery plan
- Fysieke Security
- Firewalls / IDS / IPS

#### 3.4.1 Defense in depth strategie

##### WORDT GEVRAAGD OP EXAMEN

- Layered security
- Strategie bij incident
- Plannen en documenteren
- Nooit alle eieren in 1 mandje leggen



Figuur 6: Layered security

### 3.5 ICC / Belgian Cyber Security Guide

- Checklist
- Do's & Dont's
- Gratis te downloaden: <http://iccbelgium.be/becybersecure/>

## 4 Beveiligen van toegang

### 4.1 Authorisatie vs authenticatie

- Authorisatie = een gebruiker kan bepaalde dingen wel of niet doen, afhankelijk van zijn/haar beveiligingsniveau

- Authenticatie = is de gebruiker wel wie hij/zij beweert te zijn? Controleren met 1 of meer beveiligingsbasissen.

## 4.2 Beveiligingsbasissen

### WORDT GEVRAAGD OP EXAMEN

3 opties:

- Weten
- Hebben
- Zijn

## 4.3 Beveiliging op 'Weten'-basis: wachtwoorden

- Meest gebruikte bron van authenticatie
- Moet voldoende sterk zijn
  - Lengte (minstens 12 tekens)
  - Verschillende soorten tekens
  - Geen bestaande woorden of logische sequenties

### 4.3.1 Entropie

= 'wanorde'

= hoeveel mogelijkheden er zijn  $\Rightarrow$  hoe sterk een wachtwoord is

Bits entropie	Supercomputer	GPU versnelde PC	Wachtwoord	Entropie
50	0,01 sec	2 min	12345678	27bit
60	4 sec	9 uur	azerty	29bit
65	4 min	23 dagen	v3#H!x	40bit
70	2 uur	2 jaar	tomjansen	43bit
75	3 dagen	51 jaar	VCQh5Apx	48bit
80	66 dagen	1 332 jaar	TomJansen	52bit
85	5 jaar	30 000 jaar	T0mjAn\$en	59bit
90	122 jaar	900 000 jaar	eenwachtwoord	62bit
130	600 000 000 000 000 jaar		SDfSQSqmDjN5	72bit
			G3j:@eQR[^TK	79bit
			ditsvrijsimpelteonthouden	123bit
			DitWachtwoordIsGemakkelijk	149bit

Figuur 7: Entropie van een wachtwoord

- Entropie = uitgedrukt in bits
- Beste wachtwoorden zijn vooral voldoende lang
- Opgelet voor wachtwoorden in woordenlijsten
- Vaak gebruikte wachtwoorden zijn gekend
- Enorme lijsten met wachtwoorden zijn beschikbaar

- Vaak succesvolle aanval op anders toch complexe wachtwoorden
- <https://howsecureismypassword.net/>
- <https://haveibeenpwned.com/>

#### 4.3.2 Tips

- Gebruik geen logisch patroon
- Mijd hergebruik voor verschillende diensten (ook niet azertyTwitter en azertyFacebook, etc)
- Wijzig je wachtwoorden regelmatig
- Leen nooit een wachtwoord uit aan iemand anders
- Gebruik waar mogelijk een 2<sup>de</sup> factor voor authenticatie (2FA) of multi-factor authenticatie (MFA)
- Maak eventueel gebruik van een wachtwoordkluis
- Let erop door de organisatie goedgekeurde wachtwoordkluis-software te gebruiken
- Noteer wachtwoorden NOOIT waar deze door derden kunnen worden achterhaald

#### 4.4 Beveiliging op 'Hebben'-basis

- Smartcards
- Dongles
- Transponder (=soort sleutel)
- Digipass (=merk van authenticatiediensten en -producten)
- Google Authenticator (=smartphone-app)

#### 4.5 Beveiliging op 'Zijn'-basis': biometrische beveiliging

- Iris-scanner
- Vingerafdruk
- Stem

#### 4.6 Combinatie van meerdere authenticatiemethodes

- 2FA en MFA
- Bij voorkeur kiezen tussen methodes op *verschillende* werkingsbasis

#### 4.7 Fysische toegang

- Onvergrendelde schermen
- Toegangscontrole serverroom
- Hardware aanpassingen of diefstal
  - Asset management software
- Toegang tot het netwerk



- Introductie van vreemde software
- Opstarten vanaf andere media

## 4.8 Privilege escalation

= zichzelf op een ander gebruikersniveau zetten

- Horizontal escalation
  - Session hijacking van een andere gebruiker
  - = toegang verkrijgen van het account van een andere gebruiker
  - bv: inloggen in Facebook en via je account in het account van een andere gebruiker geraken
- Vertical escalation
  - = 'privilege elevation'
  - Meer machtigingen verwerven

## 5 Backup

- Essentieel voor het beschermen van data
- Concrete back-up policy
- Disaster recovery plan

### 5.1 Veelgebruikte backup-media

- Tape
- Harddisk
- USB-stick
- Cloud-backup

**RAID is geen backup:** beschermt niet tegen meeste risico's. Helpt alleen bij falen van de hard-disk.

### 5.2 LTO Tapes

LTO = Linear Tape Open = open standaard

- Worden nog altijd gebruikt, up-to-date
- Hoge capaciteit (10-12TB per tape)
- Hoge transfer rate (500MB/s)
- Redelijk goedkoop, iets duurder dan harde schijven per GB

### 5.2.1 LTO Drive

- Toestel om LTO Tapes te lezen/schrijven
- Heel duur (duizenden euros)



Figuur 8: LTO drive voor 1 tape



Figuur 9: LTO tape robot: 12000-15000 euro

## 5.3 Eigenschappen van een correcte backup

- Offline
- Beveiling tegen aanpassing (Integrity)
- Beschikbaar (Availability)
- Veilig opgeslagen (Confidentiality)
- Betrouwbaar

## 5.4 3-2-1 regel



Figuur 10: 3-2-1-regel: 3 copies, 2 formats, 1 offsite

## 5.5 Cloud back-up

- Wat met aansprakelijkheid?
  - Je hebt geen controle over het systeem
- Wat met beschikbaarheid?
  - Niet zo makkelijk om de hele backup te downloaden uit de cloud (bandbreedtelimieten, snelheid, ...)
- Wat met vertrouwelijkheid?

- Wie heeft allemaal toegang tot de data?
- Wetgeving?
- Wel zeer eenvoudig en gemakkelijk

## 5.6 Back-up policy

- Hoge back-up frequentie
- Goede back-up strategie
- Type back-up
- Opslag van back-up:
  - Dicht bij de server voor snelle toegang
  - Op een andere locatie voor veiligheid
- Controle van integriteit back-up
- Testen van disaster-recovery plan

### 5.6.1 Grootvader - vader - zoon-systeem

**WORDT GEVRAAGD OP EXAMEN**

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
	1 Father	2 Son	3 Son	4 Son	5 Son	6
7	8 Father	9 Son	10 Son	11 Son	12 Son	13
14	15 Father	16 Son	17 Son	18 Son	19 Son	20
21	22 Father	23 Son	24 Son	25 Son	26 Son	27
28	29 Father	30 Son	31 Son	Son	Grandfather	

Figuur 11: Grootvader-vader-zoon systeem

**Bv:** Elke maandag een backup op de 'Father'-schijf, elke andere weekday een backup op de 'Zoon'-schijf, elke maand een backup op de 'Grootvader'-schijf.

- Back-uprotatie:
  - Meerdere backups, waarbij de oudste backup wordt overschreden bij het maken van een nieuwe backup.
  - Zo heb je altijd een chronologische opeenvolging van backups
- Archivering
- Backup moet zowel:
  - Actueel zijn
  - Voldoende teruggaan in de tijd

[https://en.wikipedia.org/wiki/Backup\\_rotation\\_scheme#Grandfather-father-son](https://en.wikipedia.org/wiki/Backup_rotation_scheme#Grandfather-father-son)

## 5.7 Belangrijk

- CIA-model over de hele lijn
- Moet worden getest
- Moet effectief worden uitgevoerd

## 6 Penetration testing

= testen van security

- Wat gebeurt er *echt*?
- Wat kan de hacker doen?
- ⇒ bewustwording van security
- Wettelijke beperkingen: toestemming nodig van eigenaar!

### 6.1 Black-box testing vs white-box testing

#### 6.1.1 Black-box testing

- Binnenbreken zonder dat je iets weet over het target
- Iets van waarde proberen uit het systeem te halen
- Je weet niet wat/waar je moet aanvallen
- Minder efficient

#### 6.1.2 White-box testing

- Gaan kijken naar de serverruimte, rondleiding krijgen van eigenaar
- Documentatie doorlezen
- Volledige toegang tot infrastructuur, om te kijken wat er beter kan
- Consulting, raad vragen
- Demonstratieve luik is helemaal weg: moeilijker om te tonen aan de eigenaar wat een hacker zou kunnen doen.
- Veel efficienter

### 6.2 Fase 1: Reconnaissance

Reconnaissance = Information gathering = OSINT

- Verzamelen van informatie over het target
  - Algemene info
  - Bedrijfsinfo
  - E-mailadressen
  - Organigram (=hiërarchie van het bedrijf)

- Leveranciers
- ...
- Inzetbaar voor social engineering
- Spear-phishing

#### **6.2.1 Tools & attack surfaces**

- Google!
- DNS
- Sociale netwerken
- Bedrijfssite
- ...

### **6.3 Fase 2: Network scanning**

- nmap : overlopen van services op het systeem
- port-scanners
- SNMP
- Wireshark / sniffing
- ...

#### **6.3.1 Network reconnaissance**

- Sniffing
- Port scanning
- OS fingerprinting
- Detectie van gebruikte software
- DNS zone data
- Information harvesting

### **6.4 Fase 3: Vulnerability assesement**

- Vulnerability scanners, zoals: Nexpose, Retina/Iris
  - Geeft een rapport van kwetsbaarheden op het systeem
  - Niet context-bewust: een scanner weet niet per se welke bestanden intressant zijn
  - Heel veel informatie
- Identificatie uit CVE (common vulnerabilities and exposures) database

## 6.5 Fase 4: Exploit, Access, penetratie

- De gevonden kwetsbaarheden uitbuiten (exploiten)
- Toegang verkrijgen tot het systeem
- Opgelet naar beschikbaarheid/vertrouwelijkheid/legaliteit

## 6.6 Fase 5: Maintaining access

- Het behouden van de verkregen toegang
- Covering tracks: sporen proberen uit te wissen
- Proberen zo veel mogelijk in-memory te doen: geen permanente wijzigingen aanbrengen aan het systeem.
- Opgelet naar beschikbaarheid/vertrouwelijkheid/legaliteit

# 7 Sociale media

- Oversharing: alles in detail delen met iedereen
- Mensen hebben niet door wat de impact daarvan is
- <https://www.youtube.com/watch?v=F7pYHN9iC9I>
- Op sociale media posten = vertellen aan willekeurige vreemden
- Deel nooit een foto van je bankkaart op sociale media

## 7.1 Metadata

= data over data

**Voorbeeld:** als je een foto trekt wordt daar veel metadata over opgeslagen (=EXIF-data)

- Plaats en GPS-locatie
- Exacte tijd/datum
- Cameramerk en type
- ...

Dit is mogelijks bruikbare informatie bij aanvallen. Het kan ook soms een **informatielek** zijn voor de organisatie waarvoor je werkt.

# 8 Social engineering

- Zie Kevin Mitnick's "The art of deception"
- De menselijke schakel in security
- Misbruik van inherente psychologische kenmerken van mensen
- Vertrouwen, hulpvaardigheid, empathie, ... misbruiken

## 8.1 Pretexting

= Het creëren van een scenario om het slachtoffer te engageren zodat het slachtoffer makkelijker informatie weggeeft of acties onderneemt die het slachtoffer normaal niet zou doen.

### 8.1.1 Hoe?

- Vertrouwen verkrijgen in uniform, met een impersonatie, ...
- Over telefoon, gebruik van interne lijn, ...
- Over email, spoofing, ...

## 8.2 Informatielekken

- Afval met gevoelige inhoud vernietigen (tegengaan van dumpsterdiving)
- Voorzichtig omgaan met vertrouwelijke info
- Geen kritische info op toestellen of prikborden
- In een bedrijf geraken via de nooduitgang door bvb te praten met de rokers en dan samen naar binnen te wandelen, terwijl je doet alsof je daar werkt.

### 8.2.1 Remediering

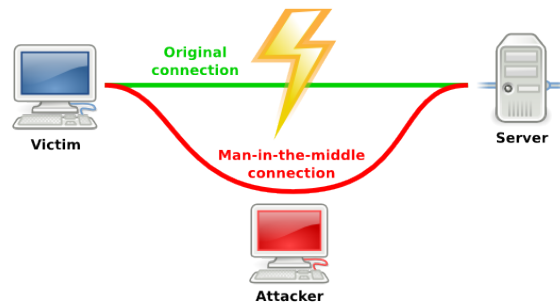
- Opleiding
- Waakzaamheid
- Strike security policy

## 8.3 Afluisteren

- Op het draadloos netwerk
- Op de kabel
- Sniffing (=de diefstal/interceptie van data via het onderscheppen van netwerkverkeer)
- Hubs vs Switches: sniffing op een hub is veel eenvoudiger, worden ook minder gebruikt

### 8.3.1 Man in the middle attack

- WiFi MITM (bvb met openbare hotspots)
- Evil-twin access point:
  - = Een access point die je zelf controleert met dezelfde SSID als een ander access point in de omgeving
  - Mensen connecteren op uw access point ⇒ je ziet hun inloggegevens
  - Je kan uw access point verbinden met internet, zodat die mensen inloggen op Facebook, Email ⇒ die inloggegevens kan je dan ook onderscheppen
- Vrij simpel implementeerbaar
- Bv: met een WiFi Pineapple



Figuur 12: Man in the middle attack

### 8.3.2 Remediering

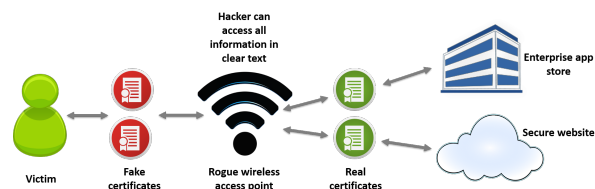
- Intelligente switches met port-shutdown
- Encryptie: versleuteld internetverkeer (geen FTP, HTTP, Telnet, . . . . Beter: SFTP, HTTPS, SSH)

## 9 Wireless

- WiFi
  - Vrijwel overal aanwezig
  - Laptop, tablet, . . .
  - Maar stopt niet aan de eigendomsgrens
- NFC
- Bluetooth
- Wireless keyboards, muizen, . . .

### 9.1 Vreemde netwerken

- Openbaren netwerken kunnen worden afgeluisterd
- Verkeer op niet-vertrouwde netwerken kan worden afgeluisterd
- WEP-beveiliging is redelijk onveilig

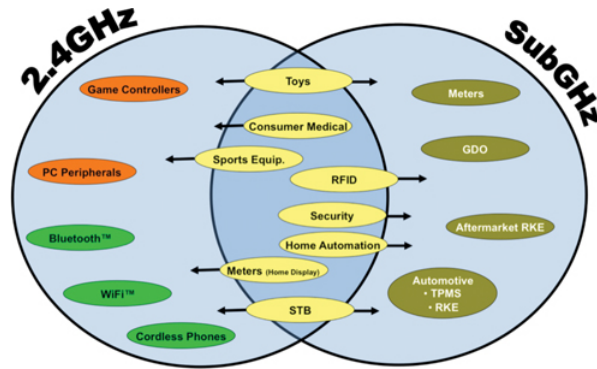


Figuur 13: Vreemd netwerk m.b.v. een rogue wireless access point



## 9.2 Frequentie

- Twee kampen: 2.4GHz (en 5GHz) vs SubGHz
- Alles dat hogere bandbreedte nodig heeft  $\Rightarrow$  2.4 en 5GHz
- Alles dat niet zo veel bandbreedte nodig heeft  $\Rightarrow$  SubGHz



Figuur 14: 2.4GHz/5GHz vs SubGHz

## 10 Virussen en malware

### 10.1 Virussen

- Bestandsvirussen (.exe en .com)
- Bootsectorvirussen
- Macrovirussen
- Wormen = virus zonder symbiant (=drager)
- Virustechnologie

#### 10.1.1 Virustechnologie

- Polymorphisme
  - = het virus gaat zichzelf gaan wijzigen
- Hybride
  - = virus met meer dan 1 infectiemethode
- Multipart
  - = virus dat uit meerdere delen bestaat, modulair
- Stealth
  - = virus dat zichzelf gaat verbergen
- Droppers
  - = software dat virulente code gaat inbrengen (droppen) in het systeem om daar achter te laten

## 10.2 Malware

- Trojans
  - Software die adverteert iets goed te doen, maar slechte bedoelingen heeft
- Spyware
  - Probeert zoveel mogelijk informatie te vergaren
- Adware
  - Toont advertenties aan de gebruiker
- Scareware
  - Software met als doel je bang te maken
- RATs = Remote Access Tools:
  - Bv: backorifice ⇒ neemt het systeem over
- Ransomware

## 10.3 Hardware

- Hardware backdoor in toestellen
- Rubber ducky
- BadUSB = USB-stick die zichzelf oplaad om dan een stroomstoot te geven aan de computer. Kan de USB-bus kapot maken of zelf het hele moederbord

### 10.3.1 BIOS

BIOS = Basic Input/Output System

= firmware die onder andere het besturingssysteem van een PC opstart

- Chernobyl virus ⇒ 1<sup>ste</sup> virus die BIOS wist

### 10.3.2 UEFI

= Unified Extensible Firmware Interface, vervangt tegenwoordig de BIOS op computers):

- Is universeel en uitbreidbaar
- UEFI "Bootkit" voor Windows 8
  - Bootkit = rootkit die voor het operating system wordt geladen, tijdens de UEFI
  - Kan full disk encryption systemen ontgrendelen
- Rakshasa = hardware backdoor, praktische aanval theoretisch mogelijk

## 10.4 Misleidende informatie

- Manipulatie van informatie
- Messagebox: welke info wordt bepaalt door wie?
- URLs: welke URL zit werkelijk achter een link?

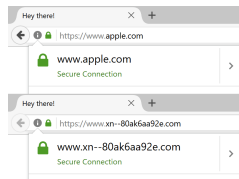
- `<a href="site.evill-haxsor.whatever">www.disney.com</a>`



Figuur 15: Messagebox

### 10.4.1 Kwaadaardige links

- Link kan een ander doel hebben dan wordt weergegeven
- Opgepast voor homograaf-URL (punycode)
  - Bvb Cyrilische tekens in een URL:



- Controleer de link!



- 'Open folder to view files' kan eigenlijk een link zijn naar een .exe als de maker van de software het zo noemt



## 11 Cloud en Software As A Service (SaaS)

- Er bestaat een onderscheid tussen Personal / Private / Public Cloud
  - Personal = servers in eigen huis
  - Private = iemand anders zijn systemen, eigen privéruimte
  - Public = iemand anders zijn systemen, gedeelde ruimte
- Afhankelijk van aanbieder van de "hosted service"

- CIA analyse blijft relevant in de cloud, enkele potentiële problemen:
  - Confidentialiteit: PRISM (=afluistersysteem van de Amerikaanse afluisterdienst NSA)
  - Integriteit: Malware / Synolocker (=ransomware voor Synology NAS-systemen) / ...
  - Beschikbaarheid: Internet Carriers / overheden

### 11.1 Cloud diensten

- Kan zeer handig zijn
- Een extra dienst is een extra risico
- Meerdere clouddiensten = de informatie staat op meerdere plaatsen
- De organisatie kan zelf niet weten waar alle informatie is opgeslagen
- Gebruik enkel de door de organisatie aanbevolen en goedgekeurde clouddiensten



Figuur 16

### 11.2 Acceptabel gebruik / Policy

- Geeft vaak de indruk de gebruiker van te willen beperken
- Probeer een balans te vinden tussen acceptabel risico en bruikbaarheid
- Is noodzakelijk om de systemen beheersbaar te houden
- Dient steeds strikt te worden opgevolgd

### 11.3 Migratie naar cloud diensten

- E-mail / groupware oplossingen
- Allicht veiliger dan een eigen exchange-server
- On-line boekhoudsoftware
- Onfeilbaar? Perfect?
- Threat model / risk analysis: analyse van meest kwetsbare onderdelen
- Zijn er andere threats dan bij een lokale server?

### 11.3.1 Voordelen / Unique Selling Point (USP)

- Toegang van overal
- Samenwerken met derden
- Automatische back-up

### 11.3.2 Nadelen

- Vendor lock-in: het is vaak omslachtig om van de ene naar de andere clouddienst over te stappen
- Vertrouwelijkheid: kan je de service wel vertrouwen?
- Prijs?
- Continuïteit?

## 12 Bring Your Own Device (BYOD)

= mensen gebruiken hun persoonlijke apparaten op het werk / om te werken.

### 12.1 Problemen

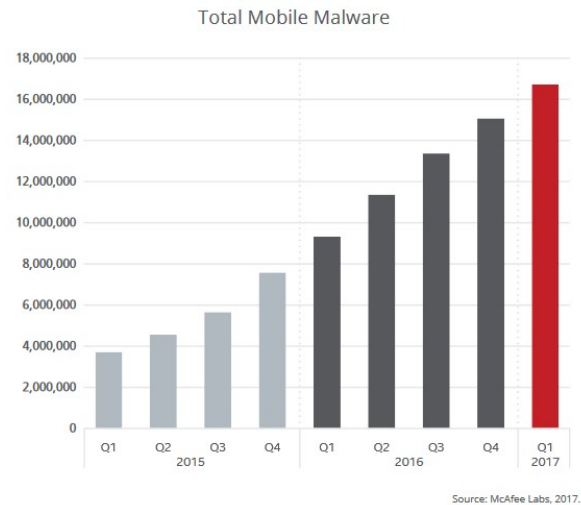
- Potentieel gebruik door derden in thuisomgeving
- Diverse apps worden binnengebracht (malware)
- Compatibiliteitsproblemen
  - Sommigen gebruiken Windows, sommigen macOS, sommigen Linux.
- Problemen met ondersteuning
  - De IT-dienst moet een hele groep apparaten ondersteunen in plaats van enkel degene die ze geven aan werknemers.

### 12.2 Mobiele apparaten

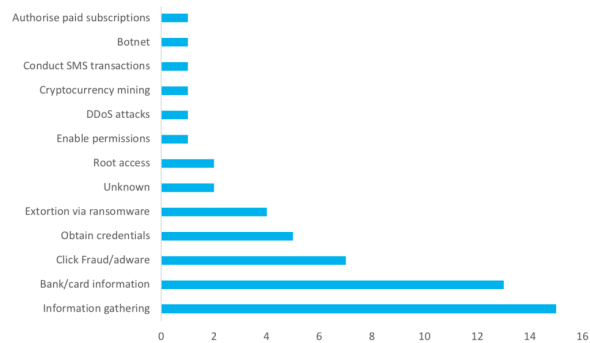
Mobiele apparaten bevatten heel veel gevoelige info en zijn daarom een groot doelwit:

- Bevatten enorme hoeveelheid vertrouwelijke gegevens
- Wordt ook vaak gebruikt als 2de factor bij authenticatie
- Wordt vaak gebruikt om wachtwoorden terug te stellen
- Niet alle apps zijn te vertrouwen
- Een app kan info naar de ontwikkelaar doorsturen (privacysettings)
- Vergrendel je smartphone altijd
- Gebruik geen telefoon met gevoelige gegevens voor spelletjes
- Opgepast voor misleidende meldingen en advertenties
- Laat je smartphone niet door derden gebruiken (bijv. door kinderen)

### 12.2.1 Mobile malware

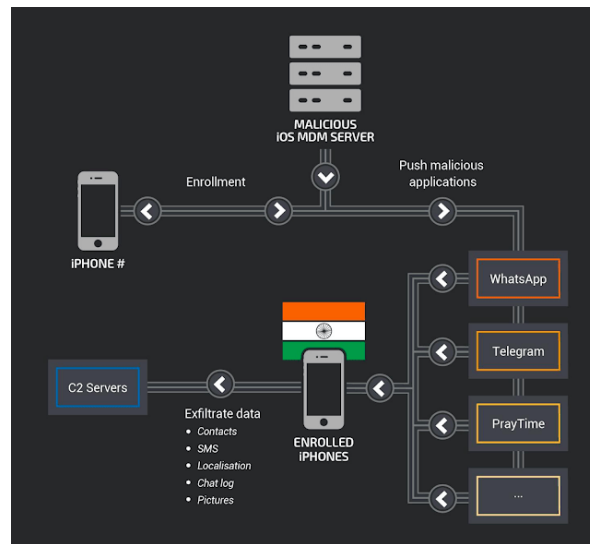


Figuur 17: Mobile malware door de jaren heen



Figuur 18: Voornaamste types exploits op Android

- De meeste problemen op Android
- De ergste problemen op iPhone
  - MDM (Mobile Device Management)
  - = software om een toestel te beheren, configureren, ...
  - = Volledige remote controle, apps/malware op afstand installeren
  - Fake MDM software bestaat op iPhone, minder op Android
- Oplossing: MDM software zoals Samsung Knox



Figuur 19

## 13 Beschikbaarheid

### 13.1 High Availability

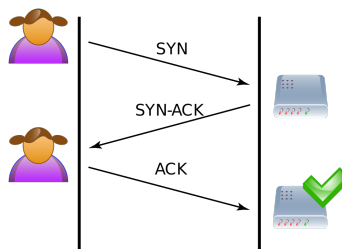
- = (bijna) altijd beschikbaar
- High availability op netwerkniveau
- High availability systemen (=always on devices)
- Clusters / load balancing (= meerdere high available servers die eenzelfde dienst kunnen aanbieden)
- Redundante servers
- Redundante serverruimte (disaster center, volledige verdubbeling van een datacenter)
- Virtualisatie:
  - deel van infrastructuur abstraheren
  - Problemen oplossen in VMs

### 13.2 Externe netwerk bedreigingen

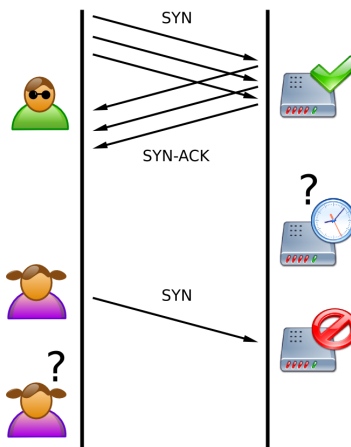
- (Distributed) Denial of Service: (D)DOS
- Portscanning
- Sniffers
- Man in the Middle (MITM)
- Spoofing
- ...

### 13.2.1 Denial of Service (DoS)

- E-mail bommen: vloedgolf van vele en/of grote e-mails, om de computer of mail service lam te leggen
- Logic bomb: een soort tijdbom. De code wordt geactiveerd wanneer een bepaalde actie gebeurt
- Repetitive login
- SYN-Flooding
  - Misbruik maken van het TCP/IP protocol
  - Constant SYN-pakketten sturen met foute bron-IP-adressen
  - De server krijgt geen ACK omdat hij de SYN-ACK stuurt naar het verkeerde IP-adres.



Figuur 20: Normal TCP/IP three-way handshake



Figuur 21: SYN Flooding

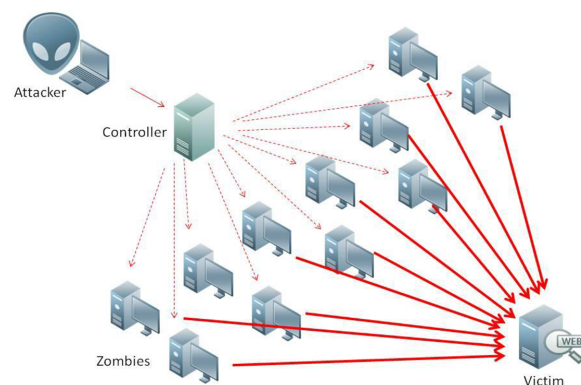
- UDP-Flooding
  - Misbruik maken van het UDP protocol
  - Een groot aantal UDP pakketten sturen naar willekeurige poorten van een target
  - Het target zal:
    1. Kijken of een applicatie luistert naar die poort
    2. Vaststellen dat geen applicatie luistert naar die poort



- 3. Antwoorden met een ICMP Destination Unreachable pakket
  - Het target zal constant hiermee bezig zijn ⇒ kan geen service aanbieden aan echte clients
- Ping of death
  - Een normale ping is minder dan 100 bytes groot
  - Het is mogelijk om pings van een andere grootte (max. 65535 bytes) te sturen
  - Op oudere systemen: buffer overflow mogelijk ⇒ system crash
  - Tegenwoordig: Ping Flooding: overbelasting ⇒ minder toegankelijkheid van normaal internetverkeer

### 13.2.2 Distributed DoS (DDoS)

- DoS simultaan uit verschillende locaties
- Zeer moeilijk tegen te houden
- Meestal zijn de drones geïnfecteerde thuis-PCs



Figuur 22: DDoS

### Hoe een DDoS tegenhouden?

- Capaciteit uitbreiden (maar dit is zelden economisch interessant)
- DDoS-beveiliging & caching dienst zoals CloudFlare DDoS Protection
  - Caching
  - Grote server-redundantie over de hele wereld
  - Keerzijde: CloudFlare is eigenlijk een Man In The Middle attack: CloudFlare zit altijd tussen client en server ⇒ alle verkeer leesbaar door CloudFlare

### 13.2.3 Spoofing

= Het vervalsen van informatie in de header:

- IP spoofing
- MAC spoofing

- Email spoofing
- ...

### 13.3 Uptime

Uptime != Availability

- 99.9% available = 8.76 uur per jaar onbeschikbaar
- 99.999% available = 5.26 min per jaar onbeschikbaar
- Wordt vaak genoteerd als '3 nines' (=99.9%), '5 nines' (=99.999%)
- Als je voor '5 nines' availability betaalt, vertaalt dit niet noodzakelijk naar uptime:
  - Stel: je hebt een webshop die meerdere services nodig heeft (website, backend, database, ...)
  - Elke service heeft '5 nines' availability
  - Als 1 van de services down is, stopt de hele webshop met werken (=downtime)
  - ⇒ het kan dus zijn dat de uptime kleiner is dan de 99.999% waarvoor je betaald hebt

## 14 Examenvragen

- Wat is een buffer overflow?
- Hoe beveilig je tegen een buffer overflow?