

Security

Tuur Vanhoutte

5 december 2020

Inhoudsopgave

1 Security	1
1.1 Doel	1
1.2 Waarom?	1
1.3 Tegenmaatregelen	1
1.4 Risico	1
1.5 Theoretisch model	2
1.6 Bedreiging vs kwetsbaarheid	2
1.6.1 Bedreigde doelen	2
2 Bedreigingen	3
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	5
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
3 Beveiligen	8
3.1 Herhaling: kwetsbaarheden	8
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
4 Beveiligen van toegang	10
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
5	Backup	13
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
6	Penetration testing	16
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: Netwerk scanning	17
6.3.1	Network reconnaissance	17
6.4	Fase 3: Vulnerability assessment	17
6.5	Fase 4: Exploit, Access, penetratie	18
6.6	Fase 5: Maintaining access	18
7	Sociale media	18
7.1	Metadata	18
8	Social engineering	18
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
9	Wireless	20
9.1	Vreemde netwerken	20
9.2	Frequentie	21
10	Virussen en malware	21
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	23
10.4.1	Kwaadaardige links	23
11	Cloud en Software As A Service (SaaS)	24
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
12 Bring Your Own Device (BYOD)	25
12.1 Problemen	25
12.2 Mobiele apparaten	25
12.2.1 Mobile malware	26
13 Beschikbaarheid	27
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	30
13.3 Uptime	30
14 Web security	30
14.1 Vaak voorkomende problemen	30
14.2 Security scanners	30
14.3 Risico's	31
14.4 Remediation	31
15 Gegevensbescherming	31
15.1 CIA-model	31
15.2 GDPR	31
15.3 Tips	32
15.4 Acceptable Use Policy (AUP)	32
15.5 Buiten het kantoor	32
15.6 Bedreigingen van binnenin	32
15.7 Fysieke beveiliging	32
15.8 Afdwingen	33
15.9 Gedragscode voor de informatiebeheerder	33
16 Risico's	33
16.1 Impact	33
16.1.1 Events	34
16.2 Risk coping strategies	34
16.3 Risk assessment	34
16.4 Security Audit	35
16.4.1 Self assessment	35
16.4.2 Externe audit	35
16.5 Pentesting	35
16.5.1 Scope van een pentest	36
16.5.2 Resultaat van een pentest	36
16.6 Tegenmaatregelen	36
16.7 Tips	36
17 IoT Security	37
17.1 Industrial security	37
17.2 Industrial control systems (ICS)	37
17.2.1 In welke sectoren?	38

17.2.2 Protocollen	38
18 Encryptie	38
18.1 Traditionele cryptografie	39
18.2 Symmetrische encryptie	39
18.2.1 Voorbeelden	39
18.2.2 Triple DES	40
18.3 Assymetrische encryptie	40
18.4 Hashing	40
18.4.1 Eigenschappen	40
18.4.2 Voorbeelden	40
18.5 Diffie-Hellman exchange	41
18.5.1 Werking	41
18.6 Crypto algoritmes	42
18.6.1 Schneier's Law	42
18.7 Veilige websites	42
18.8 Praktisch gebruik	42
18.9 Belangrijke tips	42
18.10 PKI	42
18.10.1 Doel	42
18.10.2 Stappenplan om een tekst te versleutelen	43
18.10.3 Wat als er een Man In The Middle is?	43
18.10.4 Hoe een publieke sleutel veilig versturen?	43
19 DNS	44
19.1 Potentiële problemen met DNS	44
19.2 Attack vectors	44
19.3 Kaminsky Attack	44
19.4 DNSSEC	45
19.4.1 Algoritmes	45
19.4.2 NSEC records	45
19.4.3 NSEC3	46
20 Exploits	46
20.1 Reverse engineering	46
20.2 Fuzzing	47
20.3 Shellcode	47
21 Examenvragen	47

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

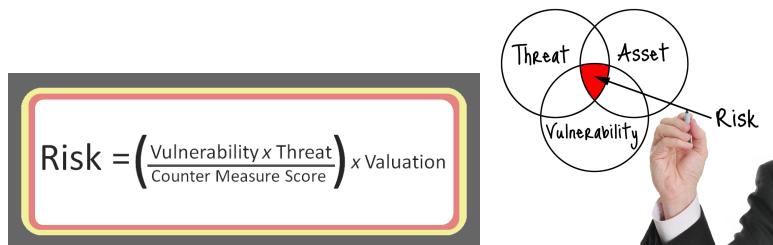
1.2 Waarom?

- 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

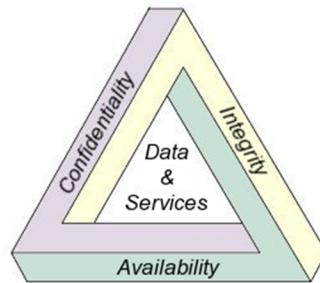
- Bepalen van de financiële impact van een incident is uitermate bedrijfsspecifiek
- **Voorbeeld:** De defacement van de website van een bakkerij is een vrij laag risico omdat er weinig financiële impact is.

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#Integrity

https://en.wikipedia.org/wiki/Information_security#Availability

1.6 Bedreiging vs kwetsbaarheid

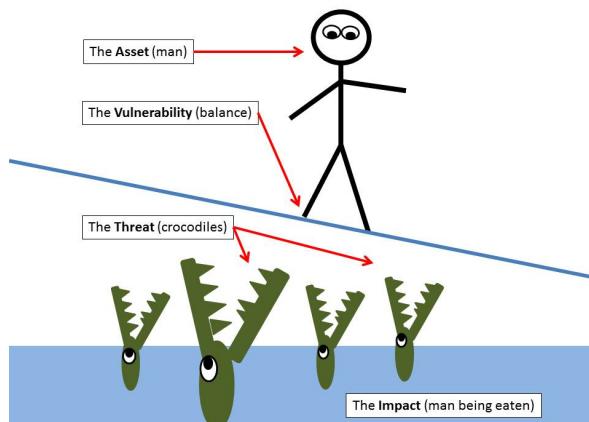
Bedreiging (threat) = potentiële negatieve actie dat een ongewenste impact heeft op een computersysteem of applicatie.

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 (externe factoren: brand, stroomuitval)

2.1 Voorbeelden

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

2.2 Types

- Systeemfouten
- Gebeurtenissen
 - Brand
 - Stroomuitval
- Intern

- Diefstal
- Wraak na ontslag
- 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, ook gestuurd door de aanvaller, 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

- Afnemer 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)

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, ...
- Interne werking van een scam center: <https://www.youtube.com/watch?v=le71yVPh4uk>

2.6 Money mule

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

- De crimineel contacteert het slachtoffer met een jobaanbieding
- De job bestaat uit het overschrijven van bedragen via zijn/haar bankrekening
- Voor elke overschrijving krijgt de money mule een deel van het geld als loon.

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 (=werknelmers) 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’ zijn synoniemen
- Bedreiging groot door grote aantallen
- Hoofdtekens (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 ⇒ 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

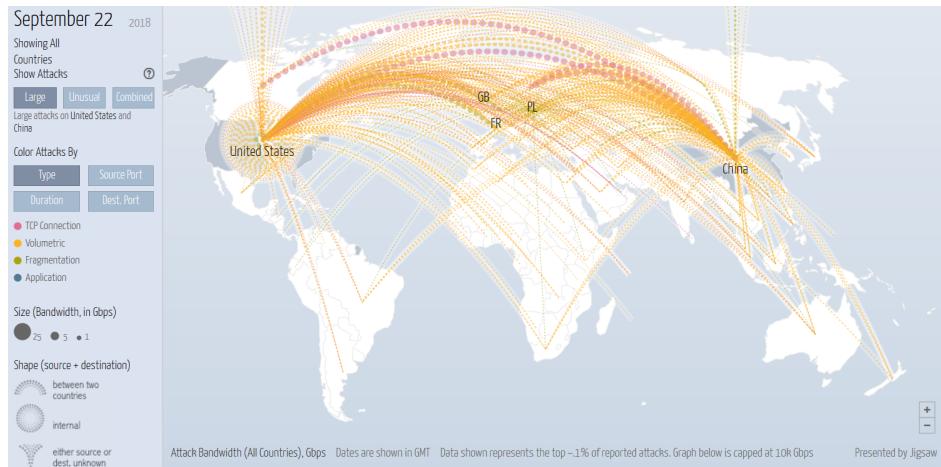
- Brand
- Stroomuitval
- Overstroming
- Diefstal
- Aanslag

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 realtime kaart

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 entrypoint
 - 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, ...
- Veel van deze devices zijn niet (genoeg) beveiligd

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. Een vingerafdruk is kopieerbaar. Een wachtwoord is veiliger want als het gekend is kan je het makkelijk vervangen. Een vingerafdruk is niet vervangbaar.

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 nodig 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 & Don'ts
- 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		SDFSQSqmDjNS	72bit
			G3j:@eQR ^TK	79bit
			ditisvrijsimpelteonthouden	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^{de} 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
- <https://xkcd.com/936/>

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. 2 vormen:

- Horizontal escalation
 - Session hijacking van een andere gebruiker
 - = toegang verkrijgen van het account van een andere gebruiker
 - Bv: Via je eigen Facebook-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

- Worden nog altijd gebruikt, up-to-date
- Open standaard
- 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 kopieën op 2 formaten, met 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		Grandfather	

Figuur 11: Grootvader-vader-zoon systeem

Bv: Elke maandag een backup op de ‘Father’-schijf, elke andere weekdag 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

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 (Open Source INTeelligence = informatie die publiek beschikbaar is)

- 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
- Maltego: programma op Kali Linux
- ...

6.3 Fase 2: Netwerk 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 assessment

- Vulnerability scanners, zoals: Nmap, Retina/Iris
 - Geeft een rapport van kwetsbaarheden op het systeem
 - Niet context-bewust: een scanner weet niet welke bestanden interessant 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
- Opelet 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.
- Opelet 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 mogelijk 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":
- https://en.wikipedia.org/wiki/The_Art_of_Deception
- De menselijke schakel in security uitbuiten
- 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 (papierversnipperaar, tegengaan van dumpsterdiving)
- Voorzichtig omgaan met vertrouwelijke info
- Geen kritische info op toestellen of prikborden
- Voorbeeld: In een bedrijf geraken via de nooduitgang door te praten met de rokers en dan samen naar binnen te wandelen, terwijl je doet alsof je daar werkt.

8.2.1 Remediering

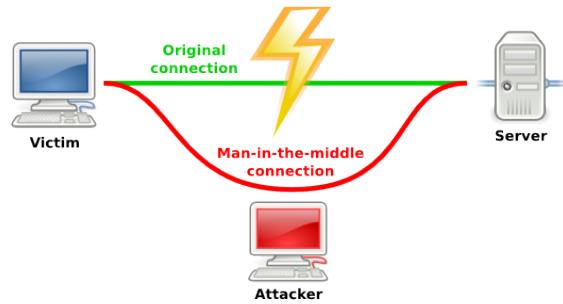
- Opleiding
- Waakzaamheid
- Strikte security policy

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

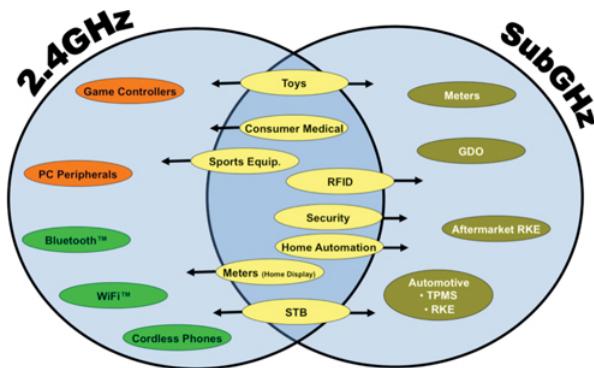
- Openbare netwerken kunnen worden afgeluisterd
- Verkeer op niet-vertrouwde netwerken kan worden afgeluisterd
- WEP-beveiliging is redelijk onveilig



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)

10.1.1 Virustechnologie

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

10.2 Malware

- Trojans
 - Software die adverteert iets goed te doen, maar slechte bedoelingen heeft
- Spyware
 - Probeer zoveel mogelijk informatie te vergaren
- Adware
 - Toont advertenties aan de gebruiker
- Scareware
 - Software met als doel je bang te maken
- RATs = Remote Access Tools:
 - Voorbeeld: Backorifice ⇒ neemt het systeem over
 - https://en.wikipedia.org/wiki/Back_Orifice
- Ransomware

10.3 Hardware

- Hardware backdoor in toestellen
- Rubber ducky
- BadUSB = USB-stick die zichzelf oplaat 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^{ste} 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

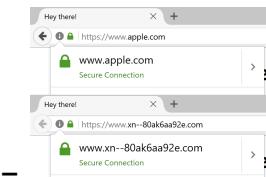
- Manipulatie van informatie
- Messagebox: welke info wordt bepaalt door wie?
- URL's: welke URL zit werkelijk achter een link?
 - www.disney.com



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
 - Hier leidt <https://apple.com> naar een andere site, want er staat niet echt apple.com maar iets dat er heel sterk op lijkt:



- 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 potentiele 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 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.

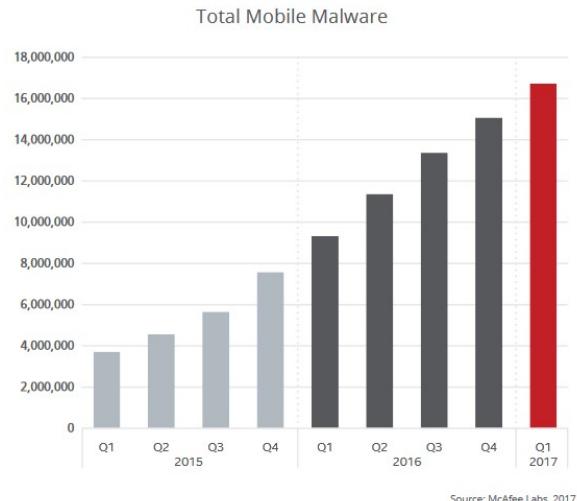
12.2 Mobiele apparaten

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

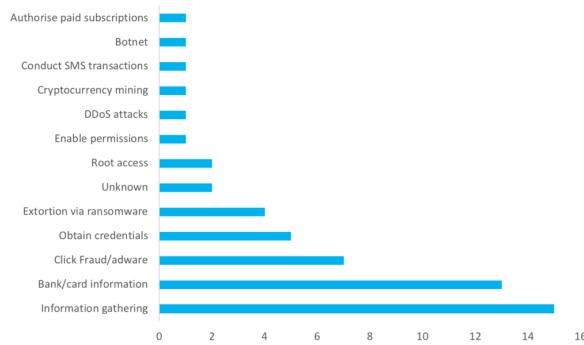
- Bevatten enorme hoeveelheid vertrouwelijke gegevens
- Wordt ook vaak gebruikt als 2de factor bij authenticatie
- Wordt vaak gebruikt om wachtwoorden terug te stellen
- Niet alle apps zijn te vertrouwen
- Een app kan info naar de ontwikkelaar doorsturen (privacysettings)
- Vergrendel je smartphone altijd

- 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

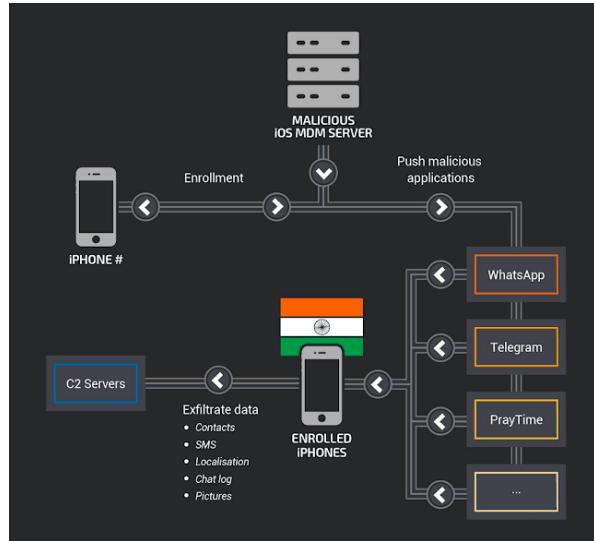


Figuur 17: Mobile malware door de jaren heen



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 voor bedrijven: Betrouwbare MDM software gebruiken zoals Samsung Knox



Figuur 19

13 Beschikbaarheid

13.1 High Availability

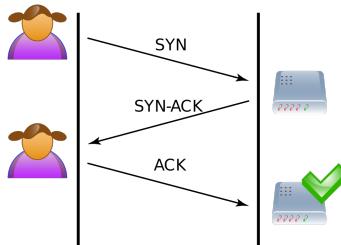
- = (bijna) altijd beschikbaar
- High availability op netwerkniveau
- High availability systemen (=always on devices)
- Clusters / load balancing (= meerdere high available servers die eenzelfde dienst kunnen bieden)
- Redundante servers
- Redundante serverruimte (disaster center, volledige verdubbeling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

13.2 Externe netwerk bedreigingen

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

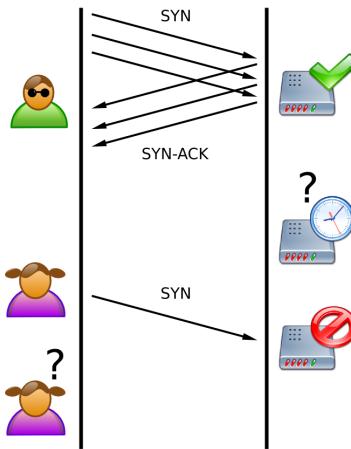
13.2.1 Denial of Service (DoS)

- 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



Figuur 20: Normal TCP/IP three-way handshake

1. De aanvaller stuurt constant SYN-pakketten van de server
2. De server stuurt een bericht SYN-ACK terug en wacht op een ACK als antwoord
3. De server blijft wachten en krijgt nooit een ACK-terug
4. Als een legetieme gebruiker probeert te verbinden krijgt die nooit een SYN-ACK terug omdat de server overbelast is.



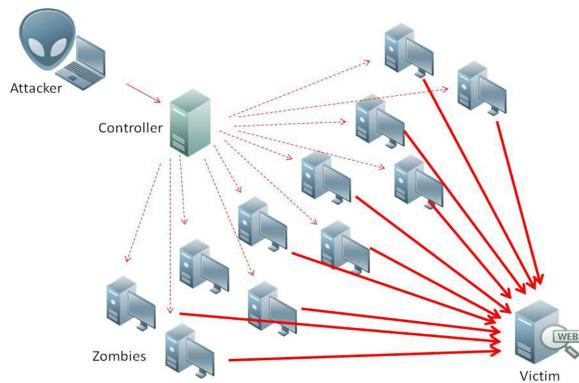
Figuur 21: SYN Flooding

- 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 \Rightarrow 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 \Rightarrow system crash
 - Tegenwoordig: Ping Flooding: overbelasting \Rightarrow minder toegankelijkheid van normaal internetverkeerd

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 \Rightarrow 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: 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 Web security

- Een belangrijke attack surface / point of entry (PoE)
- Belangrijk naar reputatie (defacement, minder vertrouwen na een hack)
- CMS-Systemen (wordpress, drupal, joomla, ..)
- Authenticatie omzeilen / escalation
- OWASP: <https://www.owasp.org>

14.1 Vaak voorkomende problemen

- Injection (bvb SQL injection, command injection, ...)
- Cross site scripting (XSS)
- Cookie stealing
- Zie OWASP Top 10: top 10 meest voorkomende technieken

14.2 Security scanners

Tools om websites te scannen op gekende kwetsbaarheden:

- Nessus
- Nikto

- OpenVAS
- OWASP Mantra
- Burpsuite

14.3 Risico's

- Defacement: de aanvaller verandert de website om bvb klanten weg te jagen
- Lek van credentials
- Reputatie van het bedrijf
- Diefstal (bij bvb webshops)
- Totale controle van server & alle systemen
- ...

14.4 Remediation

- Don't be stupid
- Gebruik sanitation libraries (no DIY!)
- Update site framework, plugins & libraries
- Prepared statements for SQL (om SQL injection tegen te gaan)
- Authentication frameworks

15 Gegevensbescherming

15.1 CIA-model

- Confidentiality: Gegevens confidentieel houden: beschermen tegen derden
- Integrity: Waken over integriteit van gegevens: beschermen tegen ongeoorloofde aanpassingen
- Availability: Gegevens beschikbaar houden: beschermen tegen verlies

15.2 GDPR

= General Data Protection Regulation

- AVG = Algemene Verordening Gegevensbescherming
- Persoonsgegevens = alle gegevens die kunnen gebruikt worden om iemand te identificeren.
- Anonimiseren of pseudonimiseren van gegevens is mogelijk
 - Geanonimiseerde gegevens = gegevens waarvan geen persoonsgegevens kunnen worden achterhaald
 - Gepseudonimiseerde gegevens = gegevens waarvan persoonsgegevens alleen kunnen worden achterhaald als de gegevens naast de persoonsgegevens worden gelegd.
- Goedkeuring voor verwerking is noodzakelijk

- Er moet een reden zijn om gegevens te verwerken of op te slaan

15.3 Tips

- Let op met afdrukken
- Clean desk policy: laat geen (gevoelige) informatie zomaar op je bureau liggen
- Sla gegevens centraal op
- Sla gegevens enkel op in door de organisatie goedgekeurde locaties en media
- Laat absoluut geen gegevensdragers (USBs, HDDs, ...) rondslingerend
- Vernietig gegevens die niet langer bijgehouden moeten worden
- Vernietig gegevens volgens de voorschriften van de organisatie

15.4 Acceptable Use Policy (AUP)

= Acceptabel gebruik van gegevens

- Geeft vaak de indruk de gebruiker 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!

15.5 Buiten het kantoor

- Let op met openbare netwerken: houd u steeds aan de voorschriften / policy (VPN)
- Deel nooit interne informatie met derden
- Wees waakzaam over wie er kan meeluisteren (kan gebruikt worden bij social engineering)
- Opgepast voor diefstal, gegevens kunnen mogelijk worden uitgelezen van een toestel zelfs indien dit beveiligd was
- Opgepast met aansluiten van of op externe apparatuur (USBs, netwerkabels, projector)

15.6 Bedreigingen van binninnen

- Grootste aandeel van veiligheidsproblemen wordt veroorzaakt door een actie van binninnen
- Spring zorgvuldig om met gepriviligeerde informatie
- Vaak worden documenten onbewust doorgestuurd
- Wees alert op mogelijke beïnvloeding

15.7 Fysieke beveiliging

- Probeer diefstal te voorkomen
 - Gebruik maken van gepaste beveiliging
 - Bewaar ‘intressante’ spullen uit het zicht

- Houd de werkplaats opgeruimd zodat geen confidentiele informatie zichtbaar is
- Wees indachtig waar print-outs en documenten liggen. Scherm deze af voor onbevoegden
- Meld steeds verdachte activiteiten aan een bevoegd persoon

15.8 Afdwingen

- Afdwingen van de AUP
- Door de gebruikers te informeren
- De noodzakelijkheid te duiden
- Awareness creëren bij de gebruikers

15.9 Gedragscode voor de informatiebeheerder

- Voorbeeld ADM gedragscode
- Wat mag een beheerder doen?
- Waar stopt de privacy van een gebruiker?
- ⇒ CAO 81 (=Collectieve arbeidsovereenkomst nr 81)
 - = Bescherming van de persoonlijke gegevens van werknemers t.o.v. de controle op online-communicatiegegevens
 - Meer info op leho bij Modules (cao-81.pdf)

16 Risico's

- De mate van bedreiging is niet beheersbaar
- De kwetsbaarheid is te reduceren door de implementatie van tegenmaatregelen
- Risico wordt uitgedrukt in euro per tijdeenheid: hoeveel geld zullen bedreigingen mij kosten?
- Bedrijfsimpact van het risico bepaalt de opportuniteit van de beveiligingsinvestering
- Bepalen van de financiële impact van een incident is uitermate bedrijfsspecifiek

$$\text{Risk} = \left(\frac{\text{Vulnerability} \times \text{Threat}}{\text{Counter Measure Score}} \right) \times \text{Valuation}$$

Figuur 23

16.1 Impact

Specifieke bedrijfsimpact == **Business Impact Analysis (BIA)**

- = Analyse van impact op een bepaald bedrijf

16.1.1 Events

- = Een gebeurtenis die een bepaalde impact heeft op het bedrijf
 - Bv: beschadiging van de server door een brand
 - Oplossing: backup terugzetten
 - Twee soorten doelen die moeten gehaald worden:
 - RPO: Recovery Point Objective
 - * Bepaalt wat je terugzet bij een backup
 - * Bv: RPO van 1 week ⇒ elke week een backup maken van alle bestanden
 - * Gevolg: ⇒ Laatste backup maximum 1 week oud
 - RTO: Recovery Time Objective
 - * Wanneer moeten we weer operationeel zijn?
 - * Bv: 1 dag ⇒ maximum een dag later terug operationeel, als een backup terugzetten max. 1 dag duurt

16.2 Risk coping strategies

Als je een risico hebt, kan je deze dingen doen:

- Risk Acceptance (aanvaarden)
- Risk Avoidance (vermijden)
- Risk Mitigation (tegenmaatregelen nemen, risico verlagen)
- Risk Transference (risico bij iemand anders leggen)
- Ignore it (NIET OK)

⇒ **Risk management**

16.3 Risk assessment

- Hoe vinden we kwetsbaarheden? ⇒ Security audit
- Hoe meten we een bedreiging? ⇒ Threat intelligence



Figuur 24: Risk Management Process

16.4 Security Audit

- Self assessment
- Externe audit
 - Penetration test
 - Bv: Red teaming
 - Red vs Blue: 2 teams
 - Blue team verdedigt, Red team valt aan op een realistische manier
 - Blue team weet niet per se dat er zal aangevallen worden

16.4.1 Self assessment

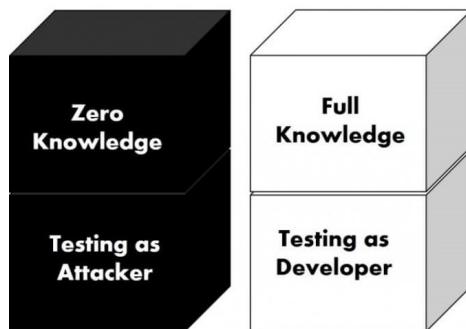
- Incident response plan
- Review van de procedures
- Interne opleiding/informatie
- Controle van back-up en recovery procedures

16.4.2 Externe audit

- Pentest (penetration test) laten uitvoeren
- Red-teaming (vs blue team)
- Gebruik van offensieve technieken
- Identificeert zwakheden

16.5 Pentesting

- Black box testing
- White box testing
- Grey box testing = combinatie van de twee. Als de Blackbox test niets opleverd kan je vragen voor bvb credentials van een user account, om dan daarmee verder te black box testen.



Figuur 25: Black-box vs White-box testing

16.5.1 Scope van een pentest

- Scope definiëren: wat mag/kan getest worden
- Minimaliseren van bedrijfsimpact
- Behouden van de relevantie van de test
- Negatieve impact is niet uit te sluiten
- Opletten met derde partijen

16.5.2 Resultaat van een pentest

- ⇒ Pентest report
- Lange lijst (potentiële) kwetsbaarheden
- Is geen 'score' of 'certificaat'
- Duidelijk resultaat:
 - Transparant
 - Prioriteiten
 - Aanbevelingen

16.6 Tegenmaatregelen

= Mitigation

- Corporate policy - Training - Awareness
- Coding practices
- Testing (pentesting)
- Vulnerability management
- Backup
- Disaster recovery plan
- Fysieke security
- Firewall / IDS / IPS

16.7 Tips

- Security is geen taak maar een proces
- Security is nooit 'af' maar in constante flux
- Informeer gebruikers (awareness) (herhaaldelijk)
- Ga voor de 'quick wins'
- Elimineer 'low-hanging fruit'
- Update software, infrastructuur en tools
- Maak een corporate policy

- Maak een disaster recover plan
- Zorg voor een correcte back-up

17 IoT Security

- Security vaak afwezig of slecht geïmplementeerd
- Privacy?
- Cloud interface / versleuteling communicatie
- Firmware vaak niet beschikbaar of worden niet geupdated

17.1 Industrial security

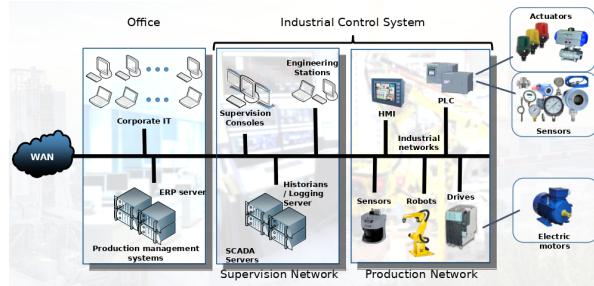
- Stuxnet
 - = worm in Siemens-apparatuur
 - Gebouwd om PLC's te infecteren met als doel een defect te veroorzaken in nucleaire installaties
 - <https://nl.wikipedia.org/wiki/Stuxnet>
- Oorzaak: Andere prioriteiten: CIA <> AIC
- Langere levensduur van systemen
- Moeilijker patchmanagement (conformiteit)
- SCADA interface op ICT netwerk voor ERP

17.2 Industrial control systems (ICS)

- Robots
- Sensoren
- Productiemachines
- **Securityprobleem:** men wil alles linken met elkaar en met het internet



Figuur 26: Industrial control system (ICS)



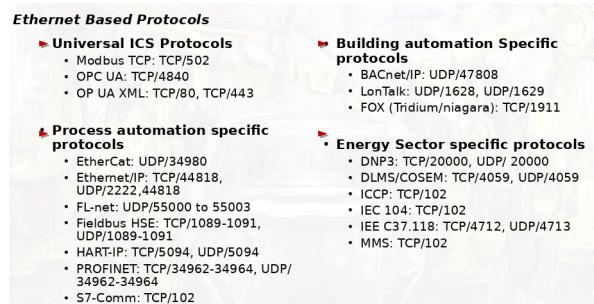
Figuur 27: ICS schema

17.2.1 In welke sectoren?

Overall:

- Kernenergie
- Olie & gas
- Transport
- Water
- Pharmabedrijven
- Groene energie
- ...

17.2.2 Protocollen



Figuur 28: Industriële communicatie

- Deze protocollen zijn niet echt ontwikkeld met veiligheid in het achterhoofd
- Alleen voor basisfunctionaliteit op meestal oude systemen
- Potentiële problemen (bv Shodan)

18 Encryptie

- Gaat over:

- Geheimhouding
- Authenticatie
- Integriteit behouden
- Helpt niet met beschikbaarheid (vaak het omgekeerde effect)
- Nonrepudation (=onweerlegbaarheid)
 - "In authenticiteit, een dienst die zorgt voor het bewijs van de integriteit en oorsprong van de data, beide in een onvergetelijke relatie, welke geverifieerd kan worden door elke derde partij op elk moment"
 - https://nl.wikipedia.org/wiki/Onweerlegbaarheid#Crypto-technische_betekenis

18.1 Traditionele cryptografie

- Substitutie
- Transpositie
- One-time pad

Voorbeeld: ROT-13: Schuif elke letter in een zin 13 plaatsen op in het alfabet:

'Een leesbare zin' ⇒ 'Rra yrrfoner mva'

18.2 Symmetrische encryptie

- Alleen Geheimhouding
- **Geen** authenticatie
- Eenvoudig
- Snel (performant)

18.2.1 Voorbeelden

- DES
 - Block-cipher van 64 bit
 - 16 encryptiecycli met telkens andere subkey
 - Bitlengte van de sleutel is bepaald, 56bit is tegenwoordig te laag
- AES
 - = Rijndael (originele naam)
 - Advanced Encryption Standard
 - Veiliger dan DES
- IDEA
- CAST-128
- Blowfish (variabele sleutellengte)

18.2.2 Triple DES

- Met 2 of 3 sleutels
- Verhoogde veiligheid
- Kan in hardware

18.3 Assymetrische encryptie

- Public key encryptie, bv: **RSA, ECC**
- Geheimhouding
- Authenticatie
- Werkt met sleutelparen
 - Private sleutel (=geef je aan niemand)
 - Publieke sleutel (=geef je aan iedereen)
- Zeer berekeningsintensief
- Het is niet mogelijk om de private sleutel te berekenen uit de publieke sleutel

18.4 Hashing

= een bepaalde string van variabele lengte omzetten in iets met vaste lengte en vast format.

18.4.1 Eigenschappen

- Variabele inputlengte
- Vaste outputlengte
- Kleine inputvariatie resulteert in grote outputvariatie
- Niet reversibel

18.4.2 Voorbeelden

- MD5
 - MD5 is gekraakt: het is mogelijk om expres dezelfde hash te genereren uit een verschillende input via het MD5 algoritme.
 - Daarom niet (meer) betrouwbaar
- De SHA2-familie:
 - SHA256
 - * Wordt als opvolger gezien van MD5
 - SHA512
 - * Wordt tegenwoordig gebruikt om Linux-wachtwoorden veilig op te slaan
- ...

18.5 Diffie-Hellman exchange

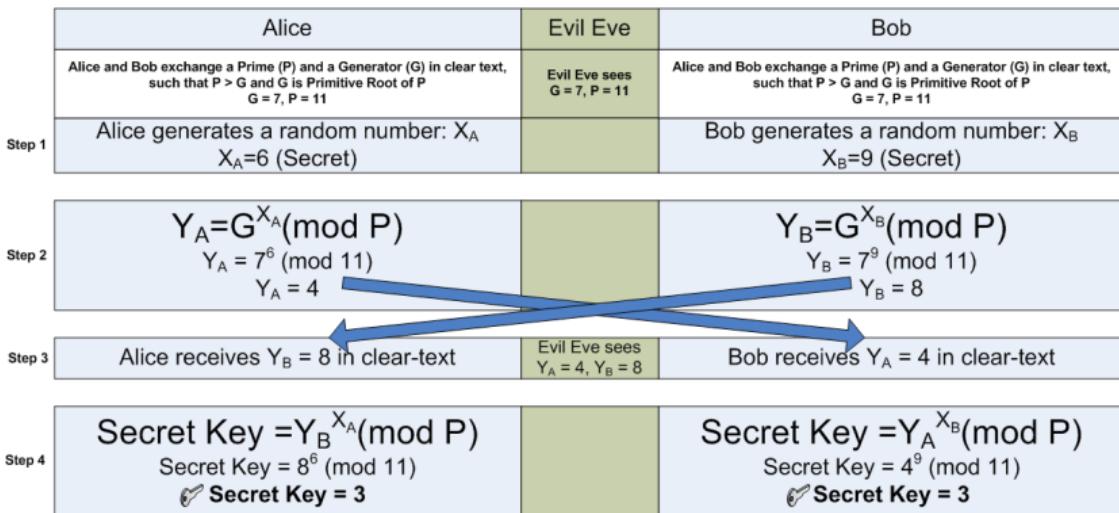
- Uitwisselen van een shared secret (key) zodat die key kan gebruikt worden om berichten te versleutelen
- Basis: <https://www.youtube.com/watch?v=NmM9HA2MQGI>
- Wiskundige uitleg: https://www.youtube.com/watch?v=Yjrfm_oR00w

18.5.1 Werking

Hoe werkt een Diffie-Hellman exchange tussen 2 mensen Alice en Bob, met een aanvaller Eve in de midden (Man in the middle)?

1. Alice en Bob wisselen een priemgetal P en een getal G (=generator).
 - $P > G$
 - G is een primitieve wortel van P
 - https://en.wikipedia.org/wiki/Primitive_root_modulo_n
 - Eve ziet P en G
2. Alice en Bob kiezen een willekeurig getal A en B die ze geheim houden.
3. $Y_A = G^{X_A} \pmod{P}$ en $Y_B = G^{X_B} \pmod{P}$
4. Alice geeft Y_A aan Bob, Bob geeft Y_B aan Alice. Eve ziet Y_A en Y_B .
5. De secret key voor Alice is $Y_B^{X_A} \pmod{P}$, voor Bob $Y_A^{X_B} \pmod{P}$

Diffie Hellman Key Exchange



Copyright ©2009, Saqib Ali
<http://www.xni-dev.com>

Figuur 29: Voorbeeld met $P = 11, G = 7, X_A = 6, X_B = 9 \Rightarrow$ secret key is 3

18.6 Crypto algoritmes

18.6.1 Schneier's Law

Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break. It's not even hard. What is hard is creating an algorithm that no one else can break, even after years of analysis. And the only way to prove that is to subject the algorithm to years of analysis by the best cryptographers around.

- **Laat het ontwerpen van crypto over aan professionals**
- <http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html>

18.7 Veilige websites

- HTTPS ipv HTTP voor 'veilige' verbindingen
- Kwaadwillige sites kunnen ook HTTPS gebruiken
- SSL betekent enkel dat gegevens niet kunnen worden afgeluisterd

18.8 Praktisch gebruik

- SSL certificaten
- E-mail versleutelen
- E-mail afzender identificatie
- Websites
- API's
- ...

18.9 Belangrijke tips

- Gebruik steeds een correct algoritme voor de toepassing
- Checksum != hashing
- CRC (cyclic redundancy check) is OK voor foutcontrole, niet voor authenticatie
 - Voorbeeld: check op rekeningnummers / creditkaarten

18.10 PKI

= Public Key Infrastructure

- Assymetrische encryptie: met public en private key

18.10.1 Doel

Het versturen van een geheim bericht over een onveilig medium.

18.10.2 Stappenplan om een tekst te versleutelen

1. Alice en Bob willen communiceren
2. Alice en Bob maken elk een sleutelpaar (private en public)
3. De publieke sleutel van Alice sturen we naar Bob
4. De publieke sleutel van Bob sturen we naar Alice
5. Alice wil een tekst veilig doorsturen
6. Alice maakt een hash van de tekst. De tekst wordt versleuteld met behulp van haar private sleutel
7. Bob decodeert de sleutel met behulp van de publieke sleutel van Alice

18.10.3 Wat als er een Man In The Middle is?

Man in the middle = Eve

1. Eve stuurt een publieke sleutel naar Alice en zegt dat die van Bob is
2. Eve stuurt een publieke sleutel naar Bob en zegt dat die van Alice is
3. Eve kan berichten sturen in naam van Alice en Bob

18.10.4 Hoe een publieke sleutel veilig versturen?

Gebruikmaken van een CA (=Certificate Authority)

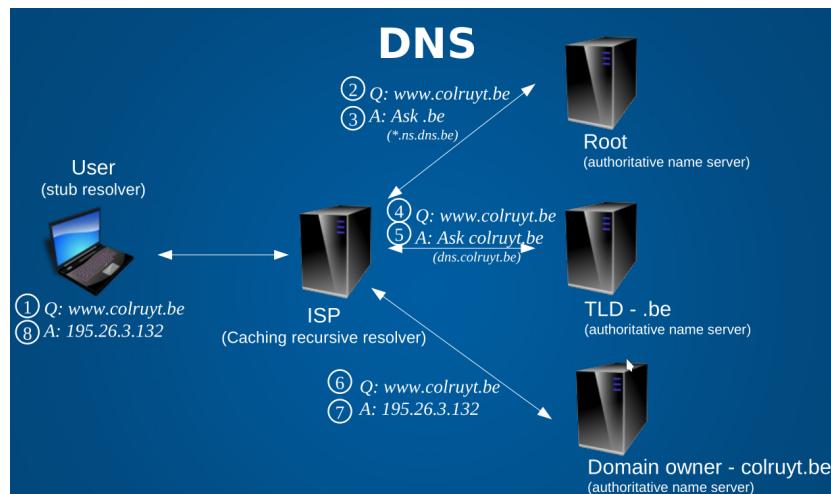
- Gecentraliseerde autoriteit
- Zowel Alice als Bob aanvaarden de autoriteit van de CA
- De CA genereert een sleutelpaar (publiek en privaat)
- Iedereen kent de publieke sleutel (inbouwen in alle computers, zit in de Certificate Store van Windows of wordt via browsers meegegeven)
- Alice stuurt haar eigen publieke sleutel deze keer niet naar Bob, maar naar de CA. Bob doet hetzelfde
- De CA zal de public key van Alice versleutelen met zijn eigen private key. Alice krijgt deze gehandtekende publieke sleutel terug.
- Alice heeft nu een publieke sleutel die is voorzien van een digitale handtekening van de CA.
- Nu zal Alice haar publieke sleutel gehandtekend naar Bob sturen
- Communicatie kan nu veilig verlopen.

Er zijn wel nog 2 problemen:

1. De private key van de CA mag NOOIT gekend worden. Indien wel gekend \Rightarrow hernieuwen
2. Er bestaan ook Fake CA's (al gebeurd bij Dell)

19 DNS

Wordt gebruikt om een FQDN (Fully Qualified Domain Name) om te zetten naar een IP-adres



Figuur 30: Werking DNS

19.1 Potentiële problemen met DNS

- Een van de oudste protocollen op het internet
- Gemaakt in de tijd waar hosts gekend en vertrouwd waren
- Het design van DNS is onveilig, security was toen geen vereiste

19.2 2 Attack vectors

1. Channel
 - = De verbinding tussen de servers, de clients en de resolvers
2. Data (in caches)
 - = Wat er wordt verstuurd
 - Kwetsbaar voor:
 - Man-in-the-middle attack
 - Wijziging van data (ip adressen van betrouwbare sites vervangen door eigen ip adres)
 - Kaminsky attack

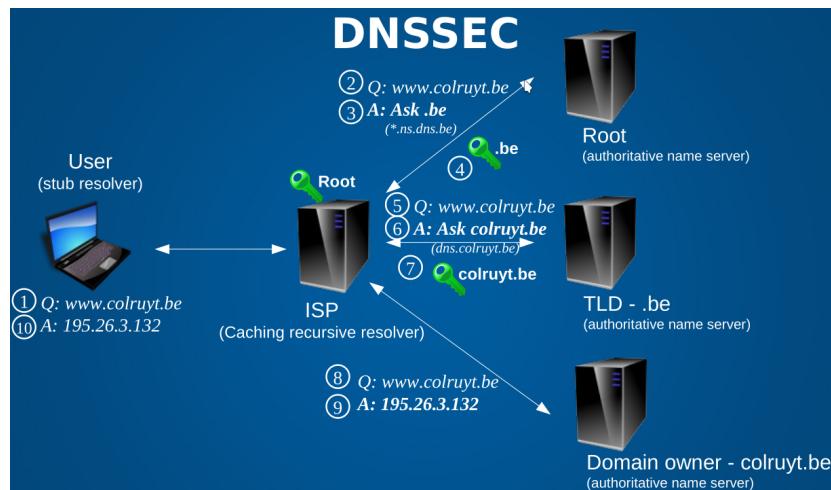
19.3 Kaminsky Attack

- = DNS spoofing / DNS cache poisoning
- Je zorgt dat de resolver geen gecachte informatie heeft over een bepaald domain
 - Je vraagt informatie over dat domein.
 - Je geeft direct een antwoord met je eigen informatie

- Zo zorg je ervoor dat elke client die informatie vraagt de verkeerde informatie krijgt
- https://www.youtube.com/watch?v=7MT1F003_Yw

19.4 DNSSEC

- = DNS Security Extensions
- Gemaakt om het DNS protocol te voorzien van een digitale handtekening
- Beveiligen tegen bovenstaande attack vectors
- Met publieke en private sleutels
- Omdat de publieke sleutel zichtbaar is voor iedereen, is die na heel lange tijd kraakbaar ⇒ sleutel moet na bepaalde tijd verlopen
- Daarom worden 2 types sleutels gebruikt:
 1. Zone Signing Key (ZSK): korter, kwetsbaarder, moet sneller vervangen worden
 2. Key Signing Key (KSK), wordt gebruikt om de sleutels zelf te authenticeren, cryptografisch sterker



Figuur 31: DNSSEC

19.4.1 Algoritmes

- Vroeger: MD5
- Nu: RSA

19.4.2 NSEC records

Probleem: Die gepubliceerde informatie wordt enkel gecertificeerd voor records die al bestaan. Er is niets dat men tegenhoudt om een nieuw subdomain te maken voor een bestaand domein om daar een soort Kaminsky attack op toe te passen. ⇒ Manier nodig om te zeggen of een subdomain bestaat of niet.

Oplossing: NSEC records

- Record die subdomein bijhoudt
- Elke record verwijst naar de volgende entry
- De records staan in alfabetische volgorde
- Problemen:
 - Meer belasting op systeem
 - Alle records zijn enumereerbaar
 - = **Zone walking**

```

• $ORIGIN dns.be.
@ SOA ....
  NS    ns.dns.be.
  DNSKEY ....
  NSEC  mail.dns.be. SOA NS  DNSKEY NSEC RRSIG
mail A   192.168.10.2
  NSEC  www.dns.be. A NSEC RRSIG
www A   192.168.10.3
  TXT   DNS.be Webserver
  NSEC  dns.be. A NSEC TXT RRSIG

```

The diagram shows a blue box containing a snippet of a zone file for 'dns.be.'. A bracket is drawn under the 'NSEC' and 'dns.be.' entries. Two arrows point from the text 'Types of current record' and 'Next record' to this bracketed area.

Figuur 32: Het NS-record bestaat altijd ⇒ de rest is enumereerbaar via de NSEC records

Dit is dus een zeer groot probleem

19.4.3 NSEC3

- NSEC records worden gehashed
- Nog altijd alfabetisch

20 Exploits

= stukjes code om een bepaalde kwetsbaarheid uit te buiten

- Reversing
- Decompilers
- Debuggers

20.1 Reverse engineering

- Let op met IL-talen (Intermediate Language) = Java/.NET/..., alles dat Reflection ondersteund
- Obfuscatie is mogelijk, maar gebeurt meestal volgens vaste methodes, dus deobfuscatie kan gebeuren

20.2 Fuzzing

- Random dingen proberen tot iets onverwachts gebeurt
- Dit kan je dan onderzoeken (in een debugger) en uitbuiten (met bv een buffer overflow of een use-after-free)

20.3 Shellcode

- = ASCII-gecodeerde uitvoerbare code
- Shellcode in memory proberen te krijgen om te exploiteren
- Om bijvoorbeeld te springen over een if-statement
- Let op voor Endianness: Little Endian != Big Endian. Heel veel protocollen keren de volgorde van de bytes om.

21 Examenvragen

- Wat is een buffer overflow?
- Hoe beveilig je tegen een buffer overflow?
- Geef een paar voorbeelden van vulnerability scanners
 - (penVas, Nessus, Nikto, wpscan, joomscan ...)
- Types encryptie + voorbeelden
- Wat is AES? Wat is RSA? Nadelen?
- Wat is het verschil tussen checksums en hashing?
- Het Diffie-Hellman-protocol wordt gebruikt om...
 - Een shared secret uit te wisselen
- Volgens de GDPR moet je een nette werkplaats hebben, waar of niet waar?
 - Waar: Clean desk policy