Security

Tuur Vanhoutte

16 oktober 2020

Inhoudsopgave

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

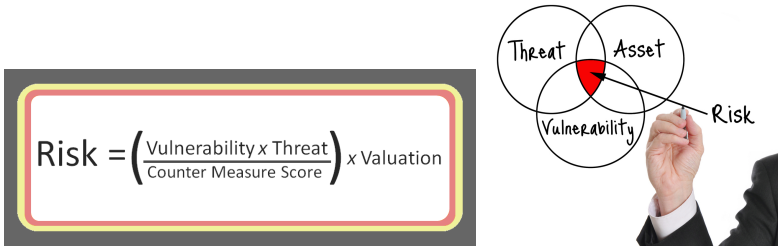
1.2 Waarom?

- 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

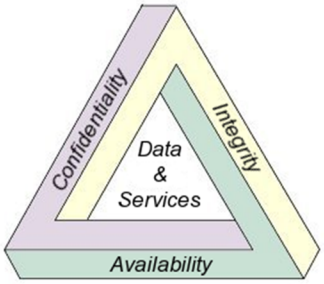
- Bepalen van de financiële impact van een incident is uitermate bedrijfsspecifiek

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#Integrity`

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

1.5.1 Voorbeelden

TODO

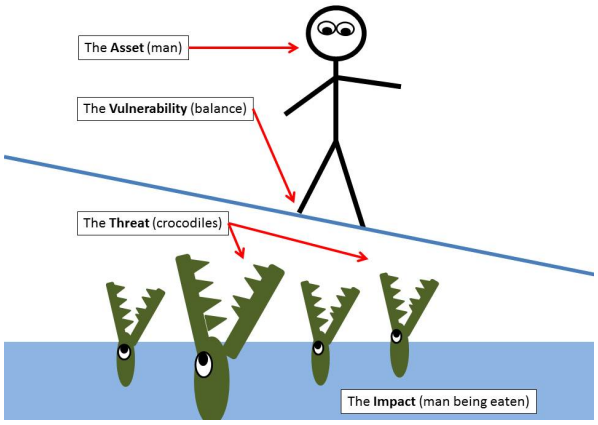
1.6 Bedreiging vs kwetsbaarheid

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/organistaties) 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 $\Rightarrow$ 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
- Specifieren 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, . . .

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 reele 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

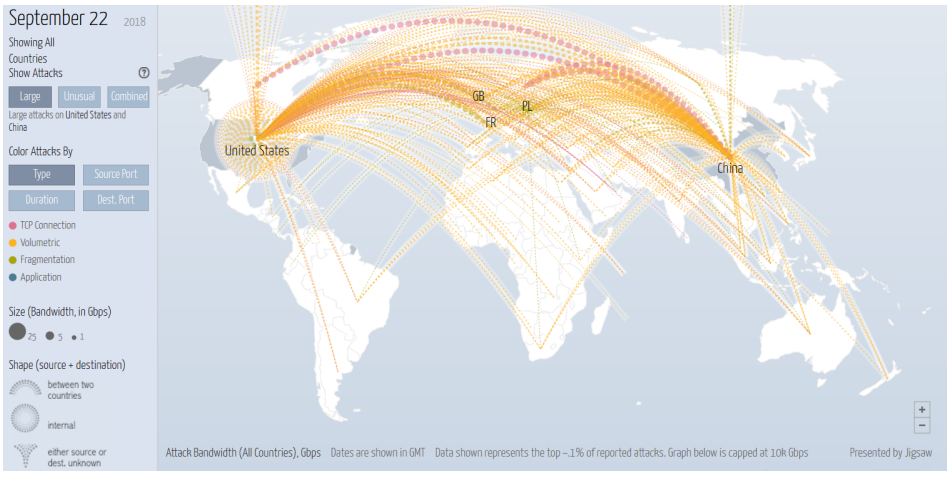
- Brand
- Stroomuitval
- Overstroming
- Diefstal
- Aanslag

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 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, ...

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 $\Rightarrow$ voorzichtig afwegen van alle parameters en belangen.

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

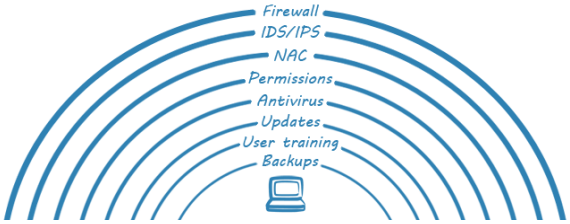
3.4 Tegenmaatregelen (mitigation)

- 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
50	0,01 sec	2 min
60	4 sec	9 uur
65	4 min	23 dagen
70	2 uur	2 jaar
75	3 dagen	51 jaar
80	66 dagen	1 332 jaar
85	5 jaar	30 000 jaar
90	122 jaar	900 000 jaar
130	600 000 000 000 000 jaar	

Wachtwoord	Entropie
12345678	27bit
azerty	29bit
v3#H!x	40bit
tomjansen	43bit
VCQh5Apx	48bit
TomJansen	52bit
T0mJan$en	59bit
eenwachtwoord	62bit
SDfSQSqmDjN5	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 verschilende 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

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 paln

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 harddisk.

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)
- Redeljk goedkoop, iets duurder dan harde schijven per GB

5.2.1 LTO Drive

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

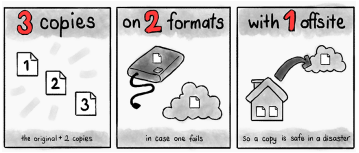
Figuur 8: LTO drive voor 1 tape

Figuur 9: LTO tape robot: 12000-15000 euro

5.3 Eigenschappen van een correcte backup

- Offline
- Beveiling tegen aanpassing (Integrity)
- Beschikbaar (Availability)
- Veilig opgeslegen (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		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?
- $\Rightarrow$ 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 = 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 Netwerk scanning

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