Security

Tuur Vanhoutte

28 september 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

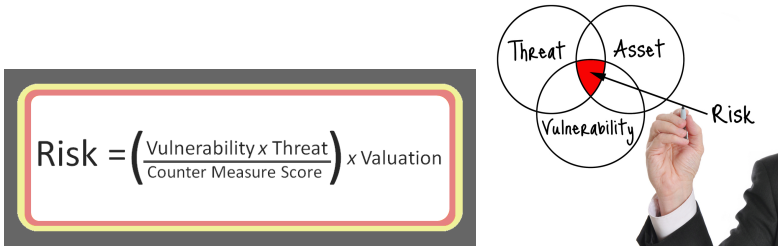
1.2 Waarom?

- 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

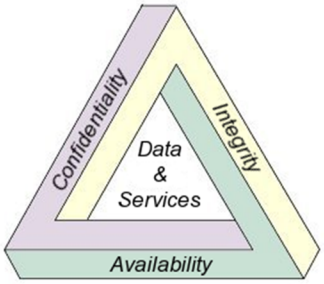
- Bepalen van de financiële impact van een incident is uitermate bedrijfsspecifiek

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

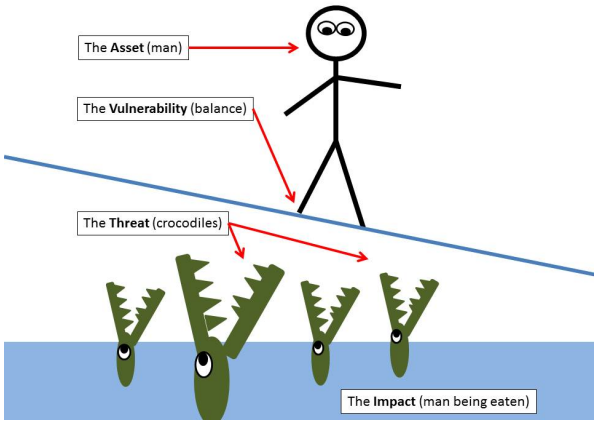
1.6 Bedreiging vs kwetsbaarheid

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

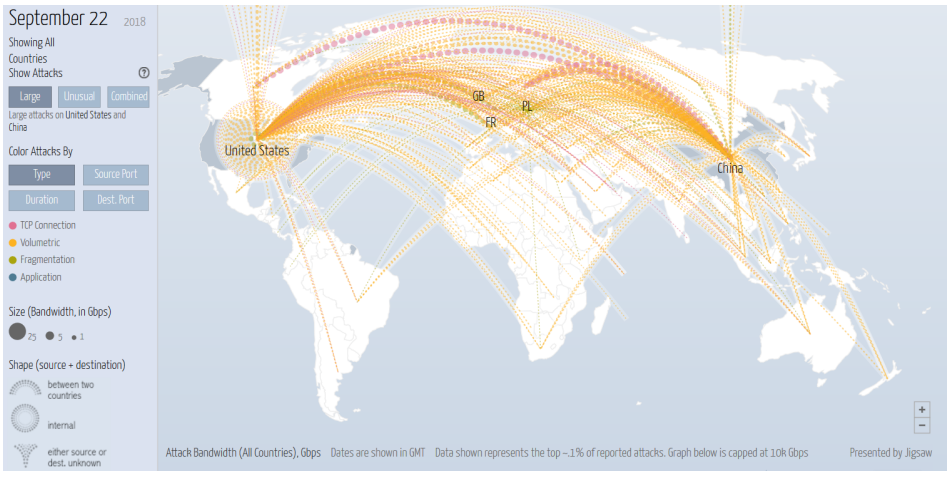
- Brand
- Stroomuitval
- Overstroming
- Diefstal
- Aanslag

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 any implementation of security controls all three factors:

1. Security
2. Functionality
3. Ease of Use

are to be carefully considered; searching for the balanced trade-off for all stakeholders."

Een bruikbare infrastructuur kan nooit 100% veilig zijn $\Rightarrow$ voorzichtig afwegen van alle parameters en belangen

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

- Layered security
- Strategie bij incident
- Plannen en documenteren

Figuur 6: Layered security

3.5 ICC / Belgian Cyber Security Guide

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