Cyber Security samenvatting 2019-2020

# Hoofdstuk 1: Cybersecurity world

## 1.1 Wat is cybersecurity?

Een set technieken die gebruikt worden om de integriteit van netwerken, programmas en data te behouden, en te beschermen tege aanvallen, schade of ongemachtigde toegang.

## 1.3 Toepassen van security aspecten in jouw leefwereld?

* Password manager
* VPN

## 1.4 Het belang van security in de opleiding aantonen, voor de 3  afstudeerrichtingen.

Applicatieontwikkeling: Vulnerabilities in code

Systemen en netwerkbeheer: Beveiligen van een server

Softwaremanagement: Educeren van externe leden

## 1.5 De 3 stappen bij het fixen van security problemen

1. Identificeren
2. Analyseren en evalueren
3. De bedreiging behandelen

## 1.6 Verschil tussen persoons identiteit en bedrijfsidentiteit

|  |  |
| --- | --- |
| Persoons-identitent | Bedrijfsidentiteit |
| * Identiteitskaart * Financiele identiteit * Online identiteit * Bedrijfsidentiteit | * Toegang (data, kennis van bedrijf) * Human factor (je wordt vertrouwd) |

## 1.7 Two-factor authentication:

* SMS
* Software/apps (op ke telefoon)
* Hardware Token

## 1.8 Wat is de GDPR?

Dit staat voor General Data Protection Regulation. Het is een data privacy wetgeving opgesteld in de EU. De wetgeving geeft individu’s de macht over hun eigen persoonlijke data, en vervolgt ook wanneer dit niet nageleefd wordt. De wetgeving wordt vooral opgelegd aan bedre

## 1.9 Soorten Threats

* Identity theft
* Types of personal records
* Threats of internet services
* Threats to key industry sectors
* Threats to people’s way of life

## 1.10 Leuke apps

|  |  |
| --- | --- |
| Ghostery | Een extension/app die sommige javascripts blokkeerd zodat het moeilijker wordt om je te tracken |
| Ublock | Browser extension, addblocker die er voor zorgt dat adds je niet kunnen volgen en bedrijven niet via ads een vingerprint van je data kan maken |
| Discornnect.me | Een bedrijf dat verschillende tools heeft om je privacy zo goed mogelijke ervaring wil geven op het net (duckduckgo) |
| Privacybadger | Browserxtension die compromis maakt tussen de gebruiker een aangename ervaring geven en content providers winst laten maken. De ads en trackers die de Do Not Track instellingen niet respecteerd wordt geblokkeerd. |
| Noscript.net | Browserectension voor het beveiligen van mozilla-based browsers, zorgt er voor dat jacascript, java, flash en andere plugins enkel van betrouwbare sites uitgevoerd worden |

# Hoofdstuk 2: Security Cube

## 2.1 De security cube

### 2.1.1 Wat is de security cube?

Een vaak gebruikt framework om beveiliging te managen. Het wordt ookwel de John McCumber cube genoemd.

### 2.1.2 De drie dimenties in de cube

1. De drie security principes (CIA triad)
2. De drie staten van informatie
3. De drie categorien van cybersecurity countermeasures

### 2.1.3 De drie security principes (CIA triad)

Dit zijn de drie principes die gebruikt worden om de cyberspace te beschermen.Deze zijn ookwel gekend als de CIA triad. Ze werken alledrie tesamen voor het beschermen van netwerk systemen.

### 2.1.3.1 Confidentiality (zorgt dat data niet zonder toestemming gebruikt wordt)

Onder confidentiality versta je het verzekeren van de privacy en het controlleren van wie toegang krijgt tot de data.

Access door AAA (Authentication, Authorization, Accounting)

Privacy != Confidentiality 🡪 Privacy heb je als je ongestoord blijft, confidentiality is wanneer iets geheim blijft.

### 2.1.3.2 Integrity (zorgt dat de data consistent, juist en betrouwbaar is)

Integrity kan je ookwel vergelijken met het behouden van de qualiteit van de data

De data moet accuraat, consistent en betrouwbaar zijn.

* + - 1. Availability (zorgt dat de data altijd toegankelijk is door de mensen met de jusite rechten)

Er moet gezord worden dat de beschikbaarheid van systemen en services altijd gegarandeerd is.

3 design principes die hier rekening mee houden:

* Eliminate single points of failure
* Provide for reliable crossover
* Detect failures as they occur

Dingen die gedaan worden om de availability te verzekeren

* Backups & maintanance
* Updates
* Disaster recovery plans
* Monitoring

2.1.3.3.4 The five nines.

Dit is een term die gebruikt wordt voor de beschrijving van een computer of een systeem met een availability van 99.999%. Dit betekend dat deze maar 5.39 minuten offline is doorheen heel het jaar.

### De drie staten van informatie

In de Cyberspace vind je heel veel critiek belangrijke data, daarom moet deze beschermd worden. De tweede dimentie van de cyber cube focust zich hier op. Om de Cyberspace te beveiligen is het nodig voor de data in alle drie de staten de beschermen.

### 2.1.4.1 Data in transit

Data in rust moet gebackup’t worden. Dit word best geautomatiseert.

### 2.1.4.2 Data in rest or in storage

Data word verstuurd via verschillende kanalen. Enkele hiervan zijn sneaker net, wired networks en wireless networks.

### 2.1.4.3 Data in process

Om deze data te beschermen wordt deze gevalideerd en gedupliceerd.

### De drie categorien van de cybersecurity countermeasures

Om de cyberspace te beschermen leunen experts op 3 skills en disciplines. De eerste is technologie. Maar alleen technologie is niet genoeg. Er moeten veel policies en prcedures en guidlines zijn die er voor zorgen dat gebruikers weten hoe ze dit goed moeten doen. Als laatst is het ook belangrijk om de gebruikers van de cyberspace bekend te maken met de gevaren.

### 2.1.5.1 Technologies als countermeasure

|  |  |  |  |
| --- | --- | --- | --- |
| **Hardware tech** | **Software tech** | **Netwerk tech** | **Cloud based tech** |
| Firewall | Software firewalls | Virtual Private Network (VPN) | Software as a service |
| Dedicated IDS | Network & port scanners | Network Acces Control (NAC) | Infrastructure as a service |
| IPS (Intrusion prevention system) | Analyzers & vulnerability scanner | Wireless accespoint security | Platform as a service |
| Content filtering services | IDS |  |  |

### 2.1.5.2 Education and training

Werknemers, studenten, etc moeten opgeleerd worden over hoe ze met vulnerabilities en andere problemen moeten omgaan. Dit begint van een jonge leeftijd aangezien de generatie al heel jong op de cyberspace aanwezig is.

Dit kan via infosessies, verplichte lessen op school, seminaries, teambuilding, cursussen, etc.

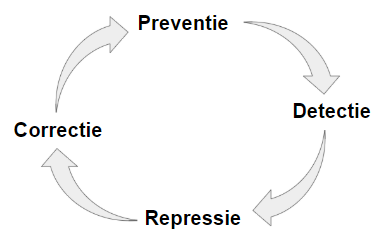
### 2.1.5.3 Cybersecurity policies en procedures

Om alles in goedde banen te lijden moeten er verschillende procedures en policies zijn opgemaakt die aangeven wat er gedaan moet worden in welke situatie. Hierdoor is iedereen ook altijd direct op de hoogte van het probleem.

## Andere begrippen en security modellen

2.2.1 The security life cycle (de beveiligingscyclus)

De beveiligingscyclus is een aaneenschakeling van maatregelen die ervoor moeten zorgen dat zaken veilig worden en veilig blijven.  De standaard beveiligingscyclus doorloopt de volgende fase: preventie, detectie repressie en correctie.

* Preventie:  het voorkomen van een beveiligingsincident.  Preventiemaatregelen zijn dus maatregelen die ervoor moeten zorgen dat er geen incident komt.
* Detectie: Wanneer iets toch door de preventiemaatregelen heen is gekomen moeten we dit zo snel mogelijk detecteren (waarnemen) zodat er actie (repressie) ondernomen kan worden.
* Repressie: Wanneer er iets negatief door de detectie maatregelen aan het licht is gekomen, wordt er direct actie ondernomen. Zodat het negatieve zo min mogelijk effect heeft.
* Correctie en correctieve maatregelen: Het herstellen van de situatie na beschadiging of verandering.

### 2.2.2 ISO 27001 SECURITY STANDARD

Is een interationaal framework voor een ISMS (International Security Management System. Het is 1 vn de meest populaire informatie security standaards wereldwijd.

### 2.2.3 Wat is een goede ‘password policy’?

\*De gebruiker kan het wachtwoord gemakkelijk onthouden.

\*\*Het is moeilijk voor een ander om het wachtwoord te raden.

\*\*\*Het is moeilijk voor een programma om een wachtwoord te raden of te ontdekken.

\*\*\*\*Een wachtwoord moet complex zijn, met cijfers, symbolen en een mix van hoofdletters en kleine letters.

### 2.2.4 Wat is 2FA? Wat zijn de voordelen?

2-Factor authentication is een extra beveiliging om te bewijzen dat jij de eigenaar van een account of toestel bent. Zo ben je extra beveiligd tegen inbreuken. 2FA werkt met "something you have", "something you are", en "something you know".

Je word voor 2 van deze 3 principes ondervraagd.

Het voordeel hiervan is dat je vooraleer je een inbreuk meemaakt de aanvaller niet alleen je wachtwoord moet achterhalen, maar daarna moet deze ook toegang krijgen via de 2FA. Dit geeft je de tijd om je wachtwoord aan te passen en nog een extra laag bescherming te gebruiken. Best neem je een random gegenereerd passwoord met letters cijfers en andere tekens.

### 2.2.5 Wat is het belang van een backup en toepassen op de cube?

Voor het grootste deel is een backup verantwoordelijk voor de availability van data. Als er iets fout gaat met de opslagmedium zijn de gegevens snel terug beschikbaar dankzij de backup.

### 2.2.6 Verschillende back-up methoden:

Lokale schijf: Via de backup op de schijf heb je altijd direct je backup, maar als de computer geinfecteerd is met malware is de data ook gecomprimeerd. Je automatiseerd de backup best.

Externe schijf: Hier heb je geen risico op ransomware etc. De usb of hardeschijs is niet altijd verbonden

Cloud-Storage: Dit is online storage. Kan zowel betalend als gratis.

# Hoofdstuk 3: Protecting secrets

## 3.1 Inleiding

### 3.1.1 Wat is cryptografie en hashing

Cryptografie is de technieque van het verbergen en/of securen van data of informatie

### 3.1.2 Waar situeerd dit zich in de security cube en waarom?

Dit kan je linken aan de CIA triad van de security cube. Confidentiality, Integrity en availability. Door te encrypteren of te hashen wordt ervoor gezorgd dat de data confidential is (enkel degene met de juiste decryption key kan de data zien). Integrity aangezien als een wachtwoord bijvoorbeeld gehasht is met een md5, deze kan je niet decrypteren en het wachtwoord zal integer blijven.

### 3.1.3 Encryptie, Hashing en salting

Encryptie 🡪 Encoding data zodat het enkel degene met de juiste key de de data kan . zien

Hashing 🡪 Calculaties die niet teruggedraaid kunnen worden

Salting 🡪 Random data toevoegen voor dat deze data gehasht word.

### 3.1.4 Het verschil tussen encoding en encryptie

Encoding 🡪 het coderen van een boodschap

Encryption 🡪 Het versleutelen van je gegevens, aan de hand van een algoritme.

## 3.2 Klassieke Cryptografie

### 3.2.1 (basic) Encryption technieques

### 3.2.1.1 Transpositie

Letters of tekens van plaats verwisselen met andere . . letters of tekens

Wordt vaak gebruikt in combinatie met fractionering . . substitutieversleutelingen

Fractionering 🡪 Opsplitsen in kleinere delen (eventueel een matrix)

### 3.2.1.2 Substitutie

Vervangen van symbolen. Dit kan op 2 manieren:

Eenvoudige substitutie 🡪 Per karakter vervangen

Polygrafisch substitutie 🡪 Per groep van karakters vervangen

Je hebt verschillende vormen van substitutie:

* Monialfabetische substitutie

Elke letter wordt vervangen met een vooropgestelt substituut (ceasar cipher, atbash)

* Homofone substitutie

Meer symbolen voor veel voorkomende symbolen bv E. Beter tegen frequentieanalyse.

* Polyalfabetische substitutie

Letters in combinatie vervangen (bv weg wordt vervangben door K) Beter tegen frequentieanalyse (bv playfaircipher)

### 3.2.1.3 One-time pad (OTP)

Dit is een encryptie technique die niet gekraakt kan worden. Er wordt gebruik gemaakt van een eenmalige “pre-shared key”. Deze is langer of gelijk aan het bericht. De plaintext is gepaired met een random secret key. Dan wordt elke bit of karakter van de text geincrypteerd door deze te combineren met de corresponderende bit of karakter van de pad.

### 3.2.1.4 Kerckhoffs principe

“The security of encryption lies in the secrecy of the keys, not the algorithm”

Nadat een bericht geincrypteerd word, moet deze secure zijn ookal weet de hacker of intercepter alle details van het algoritme. Zolang de key geheim is kan het bericht niet gekraakt worden. (DES, AES)

### 3.2.1.4.1 Kerckhoff’s vs “security through obscurity”

Security through obscurity: Het geloof in dat een system van maakt niet welke soort secure is zolang als niemand anders de mechanismes ondervind. (omgekeerde kerckhoffs)

### 3.2.2 Examples (hand-ciphers)

### 3.2.2.1 Ceasar cipher (of shift cipher)

De plaats van alle cijfers wordt een bepaald aantal keren verschoven, bijvoorbeeld a wordt c.

### 3.2.2.2 Substitution

Letters worden vervangen. Enkele voorbeelden 🡪 Ceasar Cypher, ROT13,...

### 3.2.2.3 Enigma

Electromechanische rotor cipher machine ontworpen door een duitse ingenieur

Gebruikt tijdens WO2 en gekraakt . . door Alan Turing

### 3.2.2.4 Transposition

De letters worden door elkaar gegooid.

### 3.2.3 Evolutie van de algoritmes

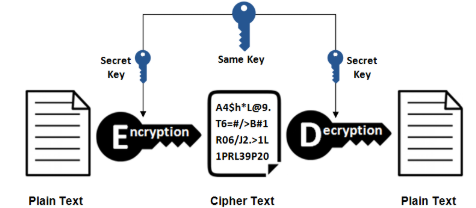
Vroeger werdt er gefocussed op de veiligheid van het algoritme zelf, maar eens dat het algoritme niet meer geheim is is de encryptie ook niet meer veilig.

Vandaag de dag werken we met het kerckhoffs principe. Er wordt meer gefocussed op de veiligheid van de keys. Zo wordt een heel algoritme niet meer onveilig eens het algoritme zelf gekraakt is.

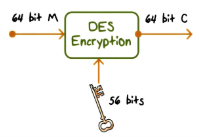
## 3.3 Moderne Cryptografie

### 3.3.1 Symmetric encryption

Ookwel gekend als private-key encryptie. (DES 3DES, AES). Dit is een snelle encryptiemethode. Dezelfde key wordt gebruikt voor het en en decrypteren van data. Zolang de key niet in de verkeerde handen valt of intercept wordt is de data confidential.

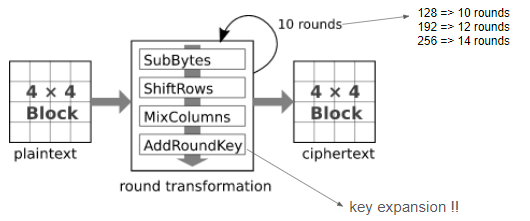


|  |  |
| --- | --- |
| **Voordelen** | **Nadelen** |
| Simpel | Dezelfde key voor de als encrypteren |
| Snel (tegenover assymetrisch) | Key management (beide party’s moeten de key kennen) |
| Efficient | veel mensen kunnen de key kennen dus geen securiheid van identiteit |

3.3.1.1 DES (Data Encryption Standard)

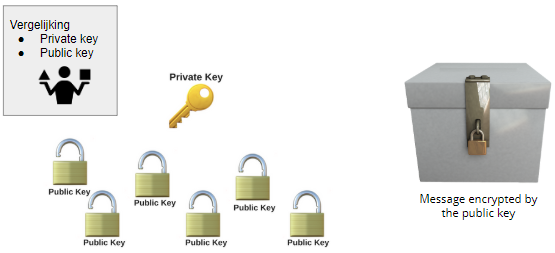
* Symmetrisch
* Block cipher
* Sleutel 🡪 64 bits (56 bits + 8 controle bits)
* 64bit input = 64bit output
* NIET SECURE SINDS 1995

3.3.1.2 AES (Advanced Encryption Standard)

* Block cipher
* Key = 128, 192 en 256 bits (10, 12 en 14 rounds)
* 4\*4 matrix (128 bits)
* Diffusion 🡪 1 bit changes, more parts of the encrypted message change
* Confusion 🡪 Make a relation between the key and the ciphertext as complex as possible

### 3.3.3 Asymmetric encryption

Ookwel gekend als public-key encryption (RSA, EIGamal, Diffie hellman, ECC). Er worden verschillende keys gebruikt. Een private key voor het encrypteren van data en een public key voor het decrypteren. Vanwegen de 2 keys wordt er voor accountability gezorgd. Er kan nagegaan worden waar de data van komt door de public key.

$

|  |  |
| --- | --- |
| **Voordelen** | **Nadelen** |
| Geen sleutels versturen voor het bericht wordt verstuurd | Redelijk traag |
| Confidentiality | Moeilijker dan symmetrisch |
| Weinig data |  |

3.3.3.1 RSA (designed by ron **R**ivest, adi **S**hamir en len **A**dleman)

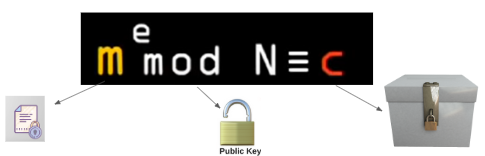
Dit is een assymetrisch encryptiealgoritme dat zich baseerd op het factoriseren van het product van 2 grote priemgetallen. Het wordt gebruikt bij bijvoorbeeld OpenSSL.

**Encryptie:**

e mod N → “wiskundig slot”  = ‘public key’

m →  boodschap

me mod N = C → C = Gesloten boodschap =  encrypted message



Decryptie:

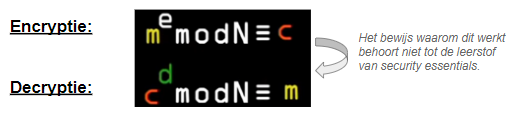
e mod N = → “wiskundig slot”  =  public key

m= →  boodschap, message

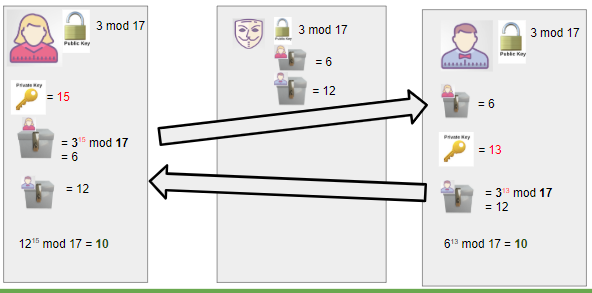
me mod N = C → C = Gesloten boodschap =  encrypted message

d = → Private key

cd mod N = m → Decryptie (met private key d)



### 3.3.3.2 Diffie Hellman

Dit is een cryptografisch protocol om sleutels uit te wisselen. Het wordt gebruikt bij een onbeveiligd communicatiekanaal om geheime encryptiesleutels uit te wisselen

3.3.3.3 ECC (Elliptic-Curve Cryptography)

Assymetrisch encryptie logaritme gebaseerd op elliptische curves. Met kleinere keys.

3.3.4 Symmetrische encryptie VS Asymetrische encryptie

|  |  |
| --- | --- |
| **Symmetrische encryptie** | **Asymmetrische encryptie** |
| Shared-secret key | Public key |
| Key length 80 – 256 bits | Key length 512 – 4096 bits |
| Share a secret key | Dont share a secret key |
| Fast | Slow |
| DES, 3DES, AES, IDEA, RC2, Blowfish, BCRYPT | RSA, ELGamal, ECC, Diffie hellman |

### Het verschil tussen block en stream cipher

|  |  |
| --- | --- |
| **Stream Cipher** | **Block Cipher** |
| 1 Bit per keer | 1 Blok data per keer |
| Minder tijd in beslag | Meer tijd in beslag |
| Sneller | Trager |
| Hardware implementatie makkelijk | Software implementatie is makkelijk |
| Minder code | Meer code |

### 3.3.5 Key management

Om een goede keymanagement te voorzien moet je op de volgende dingen letten:

1. Scalability

Beheren van een grote hoeveelheid keys

1. Security

Zorgen voor goede bescherming tegen hackers of kwaadaardige insiders.

1. Availability

Zorgen dat data toegankelijk is voor gebruikers met de juiste authorisatie

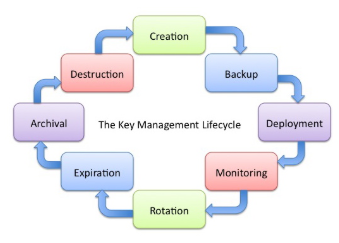
1. Heterogeniety

Meerdere databases, applicaties en standaarden ondersteunen

1. Governance

Een policy-gedreven acces control en beveiliging voor data. Inclusief het naleven van gegevensbeschermingsvereisten.

### 3.3.5.1 The key management lifecycle



### 3.3.5.2 Protocols voor keymanagement

SSL (HTTPS), SSH, PGP, IKE, VPN, Bitcoin

### 3.3.5.3 Werking HTTPS

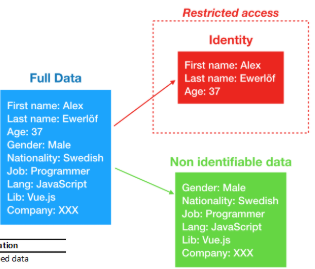
1. Er wordt een HTTP request gestuurd
2. Er wordt onderhandeld met de browser over de key
3. Het HTTP request wordt geencrypteerd met AES en verstuurd naar de website
4. De browser ontvangt het request en stuurt een response (de website)

### 3.4 Andere methodes om secrets te beschermen

3.4.1 Steganography

Het verbergen van data in een grafische, audio of ander text file.

In een foto:

Pixels bestaan uit 8 bits, waarvan de laatste bit telkens gemanipuleerd wordt om de data hier in toe te voegen. De laatste bit wordt gebruikt omdat door deze te veranderen de kleur niet fel veranderd.

In text:

Unicode Homoglyphs

3.4.2 Data masking

Gevoelige data vervangen door data die geen belangrijke informatie bevatten om de onderliggende info te beschermen.

Aan de hand van substiution, shuffling of nulling out.

Het is belangrijk omdat zo de data beschermd kan worden tegen kwaadaardige insiders of hackers. Het wordt vooral toegepast in bedrijven.

# Hoofdstuk 4: Ensuring integrity

## 4.1 Integrity & hashing

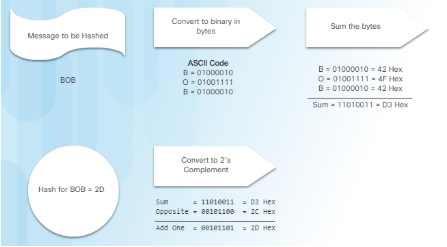
### 4.1.1 Wat is hashing

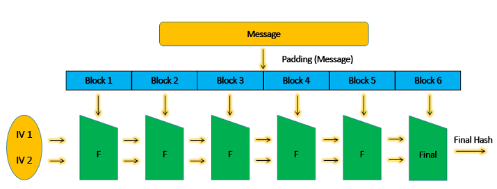
Hashing is een mathematisch algoritme dat data van een willkeurige grote mapt in een fixed-size bit string (hash)

Een hash functie heeft de volgende eigenschappen:

* Dezelfde input geeft dezelfde hash
* Als de input veranderd veranderd heel de hash
* Je kan vanuit de hash het bericht niet meer terug halen, het is one way.
* De lengte van de input maakt niet uit
* De lengte van de output is altijd hetzelfde

Hoe werkt het?



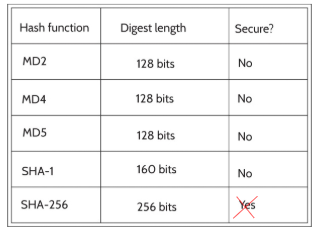


### 4.1.2 Encryption vs Hashing

Encryption 🡪 Houd in dat data geencodeerd wordt zodat het enkel toegankelijk is met de juiste key

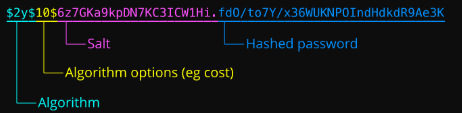
## 4.2 Hashing algorithms

### 4.2.1 Broken Hashing algorthms

Broken hashing algorithms zijn hashing algorithms die niet meer secure zijn.

* MD5 (niet secure voor passwords)
  + Wordt gebruikt voor te checken of een file integer is (examen school)
* SHA (Secure Hashing Algorithm)
* SHA-1
  + Een versie van SHA die een 160bit hash produceerd.
* SHA-2
  + Een versie van SHA die met verschillende grotes werkt
    - SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
* SHA-3
  + Totaal anders van 1 en 2. Is gebaseerd op Keccak

### 4.2.2 Secure Hashing algorithms

* BCrypt
  + Gebaseerd op blowfish (SYMMETRISCH)
  + Default salting
  + Gebruikt herhalingen
  + 
* SCrypt
  + Gebruikt KDF functions om beter te beschermen tegen bruteforce (er is hierdoor meer ram nodig om te bruteforcen)
  + Customisable
* Argon2
  + Won 2012 hashing competition (voor passwoorden)
  + Meer GPU en RAM geheugen nodig om te bruteforcen
  + Customisable
  + Nieuwer
  + Gebruikt ook salting

### 4.2.3 Salting

Salting is het toevoegen van random data voor je de data door een hash functie laat gaan.

Belangrijk om te weten:

* Gebruikt een pseudo random numergenerator
* Moet uniek zijn voor elk passwoord
* NOOIT HERGEBRUIKEN
* Hash altijd op de server in een web applicatie

Wat is het verschil met pepper?

Pepper voegt statische waardes toe, deze worden niet opgeslagen in de database, de salt wel. Als je zowel salt als pepper toevoegt is het wachtwoord langer en meer uniek.

### 4.2.4 Hashing and attacks

* Alles onder sha-256 is niet secure
* SHA-1 > MD5
* SHA-2 is vulnerable voor bruteforce attacks
* BCrypt kan aangevallen worden met een heel dure parallel dictionary attack.

### 4.2.4.1 Collision

Een collision attack is een poging om twee hashes te vinden die dezelfde hash value hebben maar een andere input. Hash functies hebben een variabele lengte en een voorgekozen output, wat kan leiden tot collisions. Indien er zo een collision voordoet verhoogt dit de kans op man in the middle attacks.

### 4.2.4.2 Cracking hashes

### 4.2.4.2.1 Bruteforce Attack

Proberen een geheim te achterhalen door alle mogelijke combinaties te proberen.

### 4.2.4.2.2 Dictionary attack

Met gebruik van een voorgecompilede lijst opties wordt het geheim achterhaald. Op deze lijst staan enkel de opties die de grootste kans hebben om te werken (bijvoorbeeld makkelijke wachtwoorden zoals “wachtwoord”).

### 4.2.4.2.3 Rainbow table attack

De aanvaller loopt door het algoritme met alle mogelijke in put die alle mogelijk output geeft. De lijst kan bruteforce, dictionary of hybrid zijn. Gebaseerd op deze lijst van outputs heeft de aanvaller altijd een herbruikbare tabel die inputs en outputs aan elkaar mapt.

### 4.2.5 HMAC

Keyes-hash message authentication code

Er wordt gebruik gemaakt van een extra secret key die bij de hashfunctie gestoken wordt. Hierdoor is er een extra laag security.

## 4.3 Hashing & applications

### 4.3.1 Waar worden hashes gebruikt?

Wachtwoorden, cyptocurrency, berichten versturen, hash tables, checksums, fingerprints...

## 4.4 Toepassingen op hashing & encryption

### 4.4.1 Digital signatures & certificates

### 4.4.1.1 Digital signatures

Wiskundige methode om de authenticiteit en integriteit van data te checken

Maakt gebruik van public key encryption en hashing

### 4.4.1.2 Certificates (verifying trust) SSL

Een digitaal certificaat kan je vergelijken met een electronisch passpoort.

De volgende informatie vind je op een certificaat:

* Een set van domeinen waar deze gebruikt voor wordt
* Start en eind data
* Info over de eigenaar
* Een public key waar het certificaat mee geencrypteerd wordt.
* Een signature van een betrouwbare bron.

Certificaat formats:

PEM 🡪 .pem, .crt, .cer, .key (meest gebruikt, base64)

DER 🡪 .der of .cer (binair)

PFX 🡪 .pfx of .p12 (base64)

Voorbeelden hashes

**Whirlpool** :38dc9541ee079f2fbf22436ad15f68a7acb243d2d2403ce4bd88292a53ffe3c75

53060830c8ce64be7c119f2b6798837dfae2f808ee0760f7affb39fdc531ad6

**SHA1** : 2c94e1eee28a78b6cc3dc3b17ef9002f11425d69

**SHA2** : 0bf89f0f6d18b045dedcdf743c943df0eb7c424807c2cff0d6fc7c9b

**SHA3:** c264ad26e3cda4f29414fdb09efd3675b5122678157e4ca3df4b3dba0a6bbe95d8e

51d5591835875370822c664b1b1986c9a2b33006b7be8acaba63829461a13

**MD4** : 37700c1c0452c714934efda1ff3fe2ed

**MD5:** 7cedf866eb281deb66b7b78fd712bcad

**HMAC:** 5cf22ca6519c812d4d6537f0cc983012 (Key: 15926, Alg: MD5)

**Bcrypt:** $2a$10$vXKWLmR3TmVGQfLpdISblu4dNZpx8ULdx60injCPVcDo3hggnvBfO

**Scrypt:** YVhwbwPSejDtYkjeE4Mf5dGxMJnsvHH2rf1giMMLrr4= (Salt: peper)

# Hoofdstuk 5: Protecting domains

## 5.1What to protect → the security cube en beveiligingscyclus

## 5.2Availability

Het is belangrijk om te zorgen voor het feit dat informatie op elk moment beschikbaar is voor de gebruikers met de juiste rechten. Sommige types van security attacks ontzeggen deze toegang, ofwel om ongemak te veroorzaken, of voor andere verdere attacks.

Goal of protecting availability 🡪 Streven naar de five nines.

### 5.2.1 High availability

Goal of protecting availability 🡪 Streven naar de five nines. AKA availability van 99.999%. Max 5.26 minuten downtime per jaar. Om dit te bekomen moeten alle fouten opgelost worden direct als ze zich voordoen, en er moet een goed ontwerp (plan of protocol) zijn waar ze op kunnen vertrouwen om dit te doen. Dit kost wel meer en is iets complexer.

De volgende factoren zijn een bedreiging voor de Five Nines:

Natuurampen, Hardware failures, sabotage, software attacks of errors, …

### 5.2.2 Measures to improve availability

Five Nines Obsolete?

Het is nu ook mogelijk om een availability van 99.9999999999% te hebben, maar als er data zoek gaat of de server begeeft het duurt het 12 uur deze data te restoren.

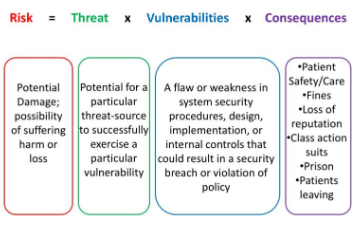
## 5.3Assets

### 5.3.1 assets management

= Het inkaart brengen van alle “bezittingen”

Asset management manages the lifecycle and inventory of technology assets including devices and software.

→ reduces the different asset types.



**Information Technology Infrastructure Library**, meestal afgekort tot **ITIL**, is ontwikkeld als een referentiekader voor het inrichten van de beheerprocessen binnen een [ICT](https://nl.wikipedia.org/wiki/Informatie-_en_Communicatietechnologie)-organisatie. Dit betekend dat de organisatie moet weten welke componenten het slachtoffer kunnen zijn van security risks, inclusief:

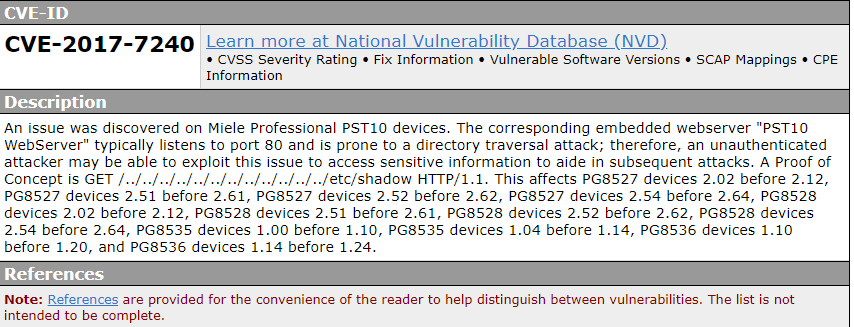
* Every hardware system
* Every operating system
* Every hardware network device
* Every network device operating system
* Every software application
* All firmware
* All language runtime environment
* All individual libraries

### 5.3.1.1 Asset classification

1. Determine the proper asset identification **category**. (information, physical, software, service)
2. Establish asset **accountability** by identifying the **owner** for all information assets and application software.
3. Determine the **criteria for classification**. (top secret; secret; confidential; public trust; and unclassified.)
4. Implement a classification schema.

### 5.3.2 Asset Management – CVE

🡪 Common Vulnerabilities and Exposure. Het is een Databank met informatie over kwetsbaarheden in computersystemen en netwerken.

Deze standard bevat: Een CVE ID, een samenvatting van de vulnerabilitie en referenties. 

### 5.3.3 Risk Analysis

🡪 Is het process van analyseren van gevaren van natuurlijke en door de mens veroorzaakte gebeurtenissen. Zen gebruiker voert een asset-identificatie uit im te bepalen welke items moeten worden beschermd

Met 4 doelen:

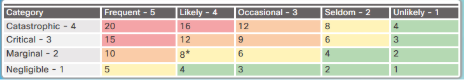
* Identificeren van assets en hun value
* Identificeren van zwakheden en bedreidingen
* De kans en impact van de geidentificeerde bedreigingen berekenen
* Bekijken of de impact van de bedreiging even fel doorslaat als de kost van de countermeasure

Dit kan op 2 manieren:

1. Quantitatieve risk analyse 🡪 op basis van de kost van de asset



1. Qualitatieve risk analyse 🡪 Op basis van meningen en scenarios



5.3.3.1 Reduce the risk

Mitigation(mitigatie) 🡪 De ernst van het verlies of de kans dat het optreed wordt verminderd. Het geeft een balans ussen negatieve impact en tegenmaatregelen

Er zijn vier veelvoorkomende manieren om risico's te verminderen!

1. Accepteren van het risico dat noodplannen voor dat risico met zich meebrengt.
2. Het risico verminderen door extra controls te implementeren

Stapsgewijs software te ontwikkelen en zorgen voor regelmatige updates en patches om kwetsbaarheden en misconfiguraties aan te pakken.

1. Het risico vermeiden door de aanpak volledig te veranderen
2. Het risico naar een third party transferen.

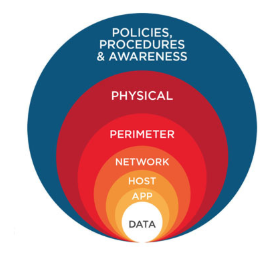
Uitbestedingsdiensten, inkoopverzekeringen of onderhoudscontracten zijn allemaal voorbeelden van risico-overdracht.

Een goed risicobeheersingsplan kan twee of meer strategieën omvatten.

## 5.4Defense

### 5.4.1 Defense in depth

Defence in depth biedt geen ondoordringbaar cyberscherm, maar het helpt een organisatie het risico te minimaliseren door het een stap voor te blijven op cybercriminelen.

Als er maar één verdediging is om gegevens en informatie te beschermen, hoeven cybercriminelen alleen die verdediging te doorbreken. Om ervoor te zorgen dat gegevens en informatie beschikbaar blijven, moet een organisatie verschillende beschermingslagen maken.

Op 4 manieren:

* Layering

Layering is creating a barrier of multiple defenses that coordinate together to prevent attacks

* Diversifying
* Limiting
* Security trough obscurity (geen valid defense mechanism)
* Simplicity

### 5.4.2 Redundancy

= Het invoegen van extra componenten die niet direct nodig zijn, maar gebruikt worden als de andere componenten het indeens begeven.

Redundancy in:

Application 🡪 RAID (Redundant Array of Indexpensive Disks)

Infrastructure 🡪 Fail-Over (procedure waar een systeem automatisch de controle doorgeeft aan een duplicaat van het systeem als deze een fout detecteerd)

Organisation 🡪 Documentatie, handovers four-eyes principle

Network 🡪 Fysieke redundancy 🡪 loops! Router redundancy

### 5.4.2.1 RAID

### 5.4.2.1.1 RAID 0 (STRIPPING)

De data wordt parallel naar 2 disks geschreven en verdeeld.

Voordeel:

Snel

Nadeel:

Onbetrouwbaar als 1 van de disks defect is.

### 5.4.2.1.2 RAID 1 (SPIEGELEN)

De arrays spiegelen van de ene drive naar de anderen. Je hebt altijd 2 drives met dezelfde data

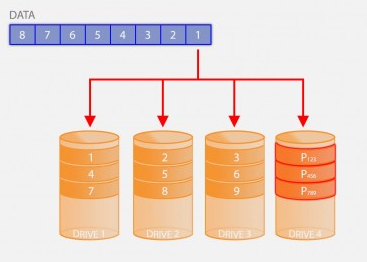
Voordelen:

Betrouwbaar en eenvoudig

Nadeel:

Niet efficient qua gebruik van opslagcapaciteit.

### 5.4.2.1.3 RAID 3 + 4 (Stripping met partitionering)

Deze twee lijken erg op elkaar, maar raid 3 werkt op Byte niveau, en 4 op blok niveau. Deze raid is erg ongebruikelijk

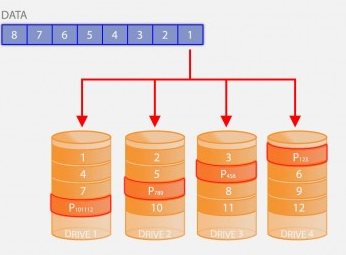
Voordeel:

Zeer betrouwbaar

Nadeel:

De snelheid is niet geweldig.

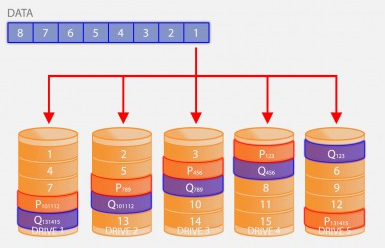
### 5.4.2.1.4 RAID 5

Deze werkt hetzelfde als raid 4 op blokniveau. Maar indeplaats van het schrijven van alle partities op 1 drive, worden deze verdeeld over alle schrijven. Als er dan 1 schijf defect is, kan de data altijd nog opgehaald worden met behulp va, de andere schijven.

Voordeel:

Betrouwbaar en snel

Nadeel:

Heeft geen nadeel, maar raid heeft een vergelijkbare snelheid maar betere betrouwbaarheid

### 5.4.2.1.5 RAID 6

Dit kan je zien als een uitbreiding op RAID 5. Idpv parities in 1 nlok, zijn er 2 blokken met partities. De data kan gered worden zelfs als er 2 drives falen.

Voordeel: Heel erg betrouwbaar en snel.

### 5.4.3 Disaster recovery

Wie is verantwoordelijk voor dit proces?

Wat heeft het individu nodig om het proces uit te voeren?

Waar voert het individu dit proces uit?

Wat is het proces?

Waarom is het proces kritisch?

**Preventieve maatregelen** omvatten controles die voorkomen dat zich een ramp voordoet. Deze maatregelen trachten risico's te identificeren.

**Detectiemetingen** omvatten controles die ongewenste gebeurtenissen ontdekken. Deze maatregelen leggen nieuwe potentiële dreigingen bloot.

**Corrigerende maatregelen** omvatten besturingselementen die het systeem herstellen na een ramp of een gebeurtenis.

## 5.4.4 Incident response plan

* Preparation
* Detection and reporting
* Analyses
* Containment & neutralization
* Post-incident activity

## 5.5Besturingssysteem Beveiliging - Basis computerbeveiliging

### Updates

### 5.5.1 Computer security

* Automatische updates
* Patch management (zie verder)
* Virusscanner

Hoe werkt het? 🡪 heft een database met gekende virussen en checkt deze

* Host-based firewalls & IDS (Intrusion detection system) (ongewenst verkeer tegenhouden en analyseren)
* Secure communications (HTTPsecure + VPN)

### 5.5.1.1 Patch management

Het beslissen welke patches geschikt zijn voor welke systemen

Ervoor zorgen dat de patches correct zijn geplaatst

Testen van systemen na de installatie van patches en het documenteren van alle bijhorende procedures.

### 5.5.2 hardening

Risicos minimaliseren en bij een incident wordt de impact berekend

### 5.5.2.1 System hardening

1. Minimaliseren
   1. Nauwlijks gebruikte programmas uitschakelen
   2. Minimaliseren van rechten voor personen en processen
2. Functiescheiding
3. Isloleren

Volgens de NSA security conigurationguides en CIS benchmark

### 5.5.2.2 Server hardening

Securing Remote Access

* RDP
* Telnet
* SSH/SCP

Administrative Measures

* Privileged accounts
* Service Accounts
* Group Policies

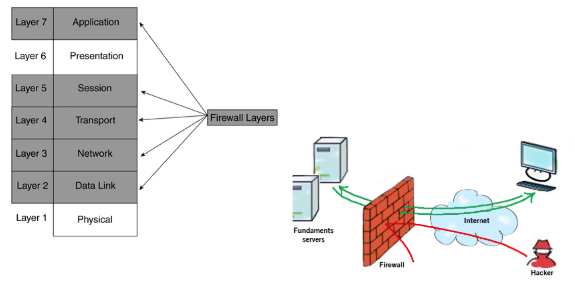
Logs & alerts aanzetten!

### 5.5.3 Network security

### 5.5.3.1 Firewall

Packet filtering firewall (network ACL en transport layer Extended IP ACL)

Application firewall, Statefull firewall, Softwarematige firewalls, Hardware firewalls



### 5.5.3.2 IDS

= Intrusion Detection System (een alarmsysteem voor als er een indringer is in het systeem)

IPS = Intrusion Prevention system (detecteerd een aanval en onderneemt actie)

### 5.5.3.2.1 SNORT (IDS)

* Not “application aware”
* No multithreading
* No file extraction

### 5.5.3.2.2 SURICATA (IDS)

* Supports Application layer detection rules
* Identify HTTP of SSH traffic
* Multithreading
* File extraction

### 5.5.3.3 Honeypot

= een val voor een hacker

Je lokt de kacher, en De hacker verdoet veel tijd aan onbelangrijke en valse info. Dit zorgt ervoor dat de hacker confused wordt en je kan informatie vergen over de hacker op deze manier.

Dit wordt ook gebruikt om spam te detecteren.

### 5.5.4 Content protection

File Access Control

* Principle of Least Privilege
* Use separate Service accounts!

File Encryption

* File encryption
  + Filevault
  + Veracrypt
* Disk encryption
  + BitLocker
  + FDE

# Hoofdstuk 6: Malware & Deception

## 6.1 Malware

Vroeger was malware een specifiek type van virus, maar vaandaag de dag staat het gekend als een verzamelnaam voor verschillende soorten kwaadaardige software zoals virussen, trojan horses, spyware, ransomware,...

### 6.1.1 Types of malware

### 6.1.1.1 Virus

Een virus is een stukje kwaadaardige code die aan een andere file vast zit en zichzelf kan copieeren. Een virus kan onschuldig zijn, maar ook veel schade aanrichten. Het kan een specifieke foto tonen, maar het kan ook files beschadigen of verwijderen.

Kenmerken:

* Verspreid door email, downloads, media
* De vroegste versies van malware waren vaak virussen
* Het moet manueel geactiveerd worden (bv open een bijlagen in een mail)
* Simpele stukjes software

Voorbeelden: Yankeedoodle, Frodo, Kenzero

### 6.1.1.2 Worm

Een worm is een type malware dat zichzelf kan clonen, en zichzelf zo onafhankelijk kan verspreiden.

Kenmerken:

* Activeerd zonder tussenkomst van de gebruiker
* Repliceerd zichzelf en maakt gebruik van zwakheden van netwerken.
* Vaak gecombineerd met backdoors of een payload (informatie over een computernetwerk)
* Wordt verspreid via payload

Voorbeelden: WannaCry, email worms, ...

### 6.1.1.3 Trojan horse

Een trojan horse is malware dat zich verstopt heeft in een ander stuk software, vaak ook in combinatie met andere malware. Vaak zitten deze in “gratis” software, downloads en attatchments.

Kenmerken:

* Verstopt zich
* Zit bij gratissoftware
* Misbruikt de privileges van de gebruiker die deze onbewust gebruikt.

Voorbeelden: Rootkit, Backdoor, Trojan-Banker, Trojan-DDOS,...

### 6.1.1.4 Logic bomb

Logic bombs worden gebruikt om een stukje kwaadaardige code te triggeren. Deze trigger kan een datum of tijd zijn, of wanneer er een bepaald programma geopend wordt.

Kenmerken:

* Triggerd mallwara adhv handelingen of events.

Voorbeelden:

Worden gebruikt voor: Het aanvallen van OS/software services, files verwijdere, databases saboteren, ...

### 6.1.1.5 Ransomware

Ransomware is een soort malware die data op je pc gijzelt en je hiervoor een aardige som geld laat betalen. Vaak wordt dit via bitcoin gedaan aangezien dit veilig is voor de hacker. Het wordt vaak gecombineerd met tojan horses.

Kenmerken:

* Gijzelt data op de pc
* Encryptie
* Betalen voor te decrypteren
* De prijs loopt altijd op

Voorbeelden: WannaCry, Locky, Jigsaw, Bad rabbit

### 6.1.1.6 Cryptojacker

Cryptojacker is een soort trojan horse dat op het geinfecteerde toestel cryptocurrency gaat minen.

Kenmerken:

* Gebruit het toestel om Cryptocurrency minen
* Hacker verdient geld met je pc
* Je pc wordt snel trager door het harde werk dat er altijd gebeurd.

### 6.1.1.7 Backdoor & rootkits

Een backdoor is een stukje software of code die iemand toegang geeft tot een systeem zonder dat deze persoon de juiste gebruikers authenticatie heeft.

Een rootkit is hetgene dat gebruikt wordt om deze backdoor te maken. Een rootkit exploit de vulnerabilities van het systeem en veranderd de system files en privileges zodat de backdoor gebruikt kan worden.

Kenmerken:

* Vaak gecombineerd met keyloggers, monitoring tools, ...
* Ook gebruikt op servers en software.

### Botnets

Een botnet is een collectie bots (geinfecteerde systemen) die geinfecteerd zijn met een malware (vaak trojan horse). De hackers hebben de systemen van de bots onder controle en kunnen dit botnet gebruiken om taken uit te voeren of bijvoorbeeld DDOS attacks te doen.

Kenmerken:

* Hackers hebben de bots onder controle
* Gebruiken de bots voor malafide doeleinden
* DDOS

### 6.1.2 The worst times of HUMAN MALWARE

* I am above your rules
* I trust everyone
* Ill click everything atleast once
* Fool me once, shame on you, fool me twice shame on me.
* Feel the need, the need for speed.
* Patches? I DON’T NEED THEM.

## Defending against malware

Op welke manieren kan je je toegoei beschermen tegen malware:

* Common sense
* Goed aware van de gevaren
* Antivirus software
* Up-to- date software(PATCHES!!!!)

## 6.3 Email and browser attacks

### 6.3.1 Spam

Spam, oftewel junkmail wordt gebruikt om via advertisements te scammen. Het is ook een methode om malware te verspreiden of aanvallen uit te voeren. Vaak worden deze mails in bulk verstuurd, zijn ze opgemaakt met google vertaler en soms zien deze er heel echt uit.

Kenmerken:

* Geen onderwerp
* Taalfouten
* Google vertaler
* Hyperlinks en attatchments die raar zijn
* E-mail van de verzender is exotisch of allemaal letters en cijfers.

### 6.3.2 Spyware

Software die informatie verzameld over de activiteit van de gebruiker.

Tools used: Keystrokes, browsing history, wachtwoorden…

Spyware komt niet enkel voor op de computer maar ook op telefoons.

### 6.3.3 Addware

Adware geeft pop-up ads, en gewone ads om hier geld mee te verdienen. Je vind dit op websites, als popups, en in zoekmachines, ...

### 6.3.4 Scareware

Scareware is gemaakt om gebruikers te overtuigen een bepaalde keuze te maken op basis van angst.

Je krijgt bijvoorbeeld ineens een venster open waar je het blauwe windowsscherm ziet, of met een waarschuwing dat je computer besmet is met een virus. als je dan er op klikt of bijvoorbeeld op de knoppen die er bijstaan kan je vaak spyware of malware op je device krijgen.

### 6.3.5 Phishing

Phishing is een vorm van fraude waar gebruik gemaakt wordt van social media, berichten, emails en zo voort. Iemand doet zich voor als iemand anders om zo login gegevens of bankinformatie te verzamelen.

### 6.3.6 Phishing variants

* Via e-mail
* Via Whatsapp/Instant messaging
* Vishing (via de stem met bellen of zo, microsoft callers, neppe nummers)
* SmiShing (via sms)
* Spearphishing 🡪 phishing naar een specifiek persoon of met een bepaald doel
* Whaling 🡪 Phishing naar mensen met hoge profielen toe (politiekers etc)
* Pharming 🡪 De gebruiker doorsturen naar een identieke fraudulente site
* Browser plugin + Browser poisoning 🡪 plugins zijn niet veilig, ze vragen altijd toegang tot java of flash.
* SEO Poisoning 🡪 Search Enginge Optimisation 🡪 kwaadaardige websites worden hoger gerankt bij bepaalde keywords

## Defending against email and browser attacks

Hoe verdedig je tegen browser en email attacks?

* Common sense
* Spam wilters gebruiken
* Mailservers configureren
* Download geen exotische plugins
* Installeer ALTIJD DIRECT software updates.

## 6.5 Deception

### 6.5.1 Social engineering

Social engenieering is een non-technische manier om informatie te verzamelen om mensen te manipuleren om bepaalde acties uit te voeren. Social engeneering hangt vooral af van dingen zoals willingnes, goodwil of weakness.

Vaak is het heel subtiel met onschuldige vragen om eerst het vertrouwen van iemand te winnen.

Maakt gebruik van verschillende technieken, zowel tehnisch (phishing, whaling, ... ) als niet technisch (intimidatie, vertrouwen, authoriteit).

### 6.5.1.1 Taktieken

* Onschuldig beginnen
* Combinatie van technische technieken (phishing, whaling,...) en non-technische technieken (authority, intimidation, trust,... )
* Pretexting
* Something for something

### 6.5.1.2Non-technische technieken (genoemd in taktieken)

* Authority
  + Usage of official authorities
* Intimidation
  + Usage of negative or non excistent consequences
* Scarity & Urgency
  + Time constraints
* Trust
  + Be your friend
* Familaity & liking

### 6.5.2 Deception methods

### 6.5.2.1 Shoulder Surfing

Observeer vanover de schouder mee om gevoelige data zoals pincodes, toegangscodes en wachtwoorden te achterhalen.

### 6.5.2.2 Dumpster diving

Door de trash gaan om informatie/data te achterhalen. Dit onthoud je met “one man’s trash isanother mans treasure”

### 6.5.2.3 Impersonation

Je voordoen als iemand anders, bijvoorbeeld een werknemer die je contacteerd voor belanstingsfraude..

### 6.5.2.4 Hoaxes

Iemand de weg omlijden of tricken. Vaak wordt dit via mail of social media gedaan (denk maar an al de neppe artikels tijdens corona).

### 6.5.2.5 Piggybacking

Meelopen met een geauthoriseerd persoon om toegang te krijgen tot een veilige locatie. Dit wordt gedaan door je bij een grote groep te voegen, of om te lijken alsof iemand je begeleid.

### 6.5.2.6 Tailgating

Mensen die de regelsaan hun laars lappen opzoeken hiervoor en telkens mee door de deur gaan.

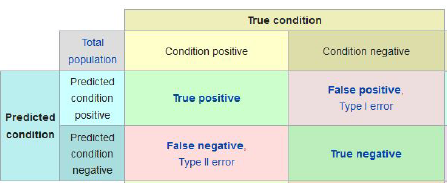
## 6.6 Defending against deception

1. Training
2. Policies
3. Awareness
4. Geen wachtwoorden en gegevens doorsturen via mail of chat, deze worden intercept.
5. Niet op ongekende links of bijlagen klikken

## 6.7 Extra informatie

### 6.7.1 Confusion matrix

Bij de confusion matrix wordt de verwachte uitkomst vergeleken met de uiteindelijke uitkomst.



### 6.7.2 Obfuscated Javascript

Dit soort javascript wordt gemaakt in source of machinecode. Deze is moeilijk tot niet leesbaar voor de mens maar de computer kan dit wel verstaan en uitvoeren.

Waarom wordt het gebruikt:

* De grootte van de code wordt aangepast (kleiner)
* Buisiness logica verbergen voor andere
* Reverse engineering is heel moeilijk
* Bij javascript wordt de download tijd ook veranderd als het script obfuscated is.

Obfuscation != Encryption!

Het verschil:

* In javascript, kan de browser geen geencrypteerde code uitvoeren
* Encrypteerde code moet altijd gedecrypteerd worden
* Obfusceerde code moet niet gedeobfusceerd worden om te werken

6.7.3 PUP (Potentially Unwanted Program)

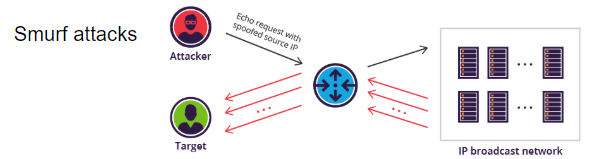
Dit is een programma dat de gebruiker toegang tot downloaden heeft gegeven, maar nogsteeds ongewild is omdat er mss spyware, adware meegedownload worden met dit programma.

# Hoofdstuk 7: Attacks

## 7.1 Cyber attacks / basis technieken

### 7.1.1 DDos (Distributed denial of service)

Een Denial-Of-Service attack is een sort network attack. Een DoS attack resulteert in de onderbreking van services voor gebruikers, devices of applicaties. Een Ddos Attack wordt vaak gedaan met een botnet. Alle bots in dit net zullen er voor zorgen dat de services overbelast worden en onderbroken worden. De payload wordt te hoog.



### 7.1.2 Sniffing

Sniffing wordt ookwel gezien als met je neus zitten tussen andere mensen hun data. De aanvaller kijkt mee door de packets en snift of hij nergens belangrijke of geheime informatie kan bekrijgen via het dataverkeer.

Hoe vermeiden?

ALTIJD via httpS en VPN werken.

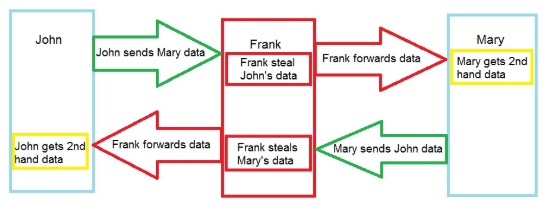
### 7.1.3 Spoofing

Spoofing is een goed voorbeeld van een impersonation attack, bij het spoofen wordt er misbruik gemaakt van een vertrouwde band tussen twee systemen. Er wordt een ander ip en mac adress gebruikt. Deze soort attack wordt vaak gebruikt bij man in the middle attacks.

3 Soorten:

* MAC adress spoofing
* IP Spoofing
* DNS spoofing

### 7.1.4 Man in the middle



Replay attack 🡪 een attacker neemt een deel van de communicatie op tussen 2 hosts en verstuurd dit stukje communicatie later.

### 7.1.5 Zero-day

Een threat die probeert misbruik te maken van vulnerabilities die onbekend zijn voor anderen of de software ontwikkelaar

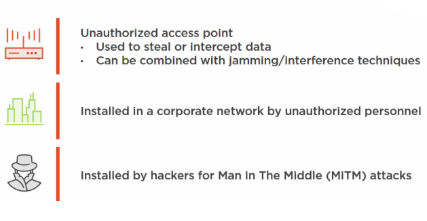
Een zeroday is een software hardware of firmware fout die onbekend is voor de maker ervan. De naam komt van het feit dat de fout nogniet gefixt is door de professionals. Deze fouten zijn heel moeilijk om te vinden en bijna onmogelijk om tegen te beschermen.

### 7.1.5 Keylogger

Keyloggers zijn devices die werken op verschillende platformen (PC, mobiel, zelfs ATM”s voor de code van je kaart). Ze loggen op welke toetsen je klikt, en wanneer. Er bestaan zowel hard als software keyloggers.

## 7.2 Wireless & Mobile attacks

### 7.2.1 Rouge Access Points

Dit is een accespoint dat gemaakt is om data te stelen of intercepten. Deze vind je vaak op plaatsen zoals in het centrum van een grote stad, veel mensen willen wifi dus ze verbinden zich met de gratis wifi. 

### 7.2.2 WEP & WPA attacks

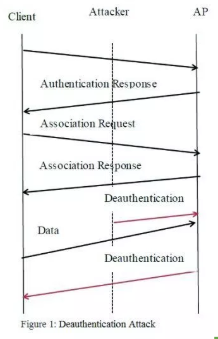
### 7.2.2.1 WEP (Wired Equivalent Privacy)

WEP is een security algoritme voor fireless netwerken (IEEE 802.11). Het algoritme maakt gebruik van een key voor het encrypteren.

Eigenschappen

* Key encryption
* No key management
* Same key for everyone
* De key kan intercept worden door het netwerkverkeer in de gaten te houden

Problems IV (Initialization Vector) 🡪 component van het cryptografisch systeem

* Een 24-bit field, wat te klein is
* Het is in cleartext, dus leesbaar voor iedereen
* Het is statsich, dus identische key streams zullen elkaar herhalen op een druk netwerk.

### 7.2.2.2 WPA (Wi-fi Protected Access)

WPA is een security standard die gebruikt wordt om draadloze verbindingen te beveiligen. Dit protocol is gemaakt om de WEP te vervangen. Bij deze versie is het niet meer mogelijk om aandehand van het netwerk verkeer de key te achterhalen.

### 7.2.2.3 DeAuthentication attack

Als iemand de verbinding met een accespoint wil verbreken wordt er een deauthentication frame verstuurd van de gebruiker naar de AP en ook terug. Een attacker kan eenn deauthentication frame naar een draadloos accesspoint sturen, met een gespoofd MAC adres van het slachtoffer, in de naam van het slachtoffer. Hierdoor valt de connectie weg.

### 7.2.3 Defending against wireless & mobile attacks

1. Maak gebruik van ingebouwde functies zoals authenticatie en encryptie die je in de configuratiesettings aan kan passen
2. Zet devices die je niet vertrouwd in de demilitarized zone (DMZ) waar de onbetrouwbare devices zoals email en webservers zitten
3. Gebruik tools die je je netwerk beter leren kennen en afbakenen.

## 7.3 Application attacks

### 7.3.1 OWASP (Open Web Application Security Project)

### 7.3.2 Cross-Site Scripting (SSX)

Cross-Site Scripting is het uitvoeren van scripts met malicious code in op een zwakke webapplicatie.

Wat kan het een ssx attack?

* Scripts uitvoeren
* Sessies highjacken
* Websites beschadigen
* Gebruikers onbewust dingen laten doen die ze niet willen

Non-Persistent XSS 🡪 speciaal gecrafte urls die via blog, email etc wordt verspreid

DOM-Based XSS 🡪 Kan zowel persistent als non persistent zijn.

Persistent XSS 🡪 serverbased en kan op de pc van het slachtoffer de code uitvoeren op een geinfecteerde site.

### 7.3.3 Code injection

Code injection is het invoegen van code in invoegvelden op een webpagina, die er normaal niet horen. Soms worden deze invoervelden gefilterd om geen ongewilde commandos uit te voeren maar dit kan vaak omzeild worden.

Het wordt gebruikt om data aan te passen, verwijderen of te verkrijgen.

Hoe bescherm je je er tegen?

* Prepared statements
* Whitelist input
* Validate

### 7.3.4 Remote Code Execution (RCE)

Het uitvoeren van kwaadaardige code met als doel controle te krijgen over het systeem van het slachtoffer met de privileges van de gebruiker. De code wordt uitgevoerd vanop een afstand, dit kan ook via een remote server dus kan van overal afkomen.

# Hoofdstuk 8: Pentesting

## 8.1 Information gathering

### 8.1.1 Enumeration

Een computeractiviteit waar gebruikersnamen, en informatie over groups, shares en services van computers op een netwerk opgevraagd worden.

Bijvoorbeeld netwerk enumeration is het ontdekken van hosts of services in een netwerk.

### 8.1.1.1 Host enumeration

Host enumeration is uitvinden van welke services er aan het runnen zijn op een host.

Dit kan gedaan worden via de default gateway (met ipconfig), maar je kan ook de meest common ports en ip adressen testen die gelinkt zijn aan servers.

Wordt gebruikt:

* Extracting user names and id’s
* Extracting information using default password
* Brute force active directory
* Extract information using DNS zone transfer

### 8.1.2 Zenmap/Nmap

Nmap, kort voor Network mapper is een open source security scanner dat een snelle scan kan maken van ranges, devices of waardevole informatie over devices op je netwerk kan geven.

Wordt gebruikt voor:

* Network exploration
* Security auditing
* Scan large networks
* Routine tasks
* Host discovery
* OS detection
* Port scans
* Host detection
* Network inventory
* FIND AND EXPLOIT vulnerabilities
* ....

De GUI van Nmap is Zenmap.

Nmap commans:

* -sV: Find services & version
* -O: OS detection
* -F: Fast/limited
* -T4: Skip timeouts
* -p: Define scan range
* -sn: ping scan

### 8.1.3 In Web applications

* Robots.txt of sitemap.xml

### 8.1.3.1 Dir/Dirbuster

## 8.2 Tools used in applications

## 8.3 Security driven testing of applications

## 8.4 OWASP Top 10

## Vakjargon Thema 1:

|  |  |
| --- | --- |
| Term | Explanation/verklaring |
| Exploit | Software dat misbruik van een flaw in een systeem maakt voor malicious doeleinden |
| Attack | Aanval |
| Countermeasure | Is een actie die wordt ondernomen om een aanval af te weren of er tegen in te gaan. |
| Risk | Risico |
| Security policy | De grote lijnen van hoe een organisatie wordt beveiligd tegen threats, inclusief hoe er gehandeld moet worden als er een security breach is. |
| Threat | Dreiging |
| Vulnerability | Kwetsbaarheid |
| Interception (threat) | Data onderscheppen wanneer dit in transport is |
| Interruption (threat) | Een proces stoppen waardoor iets zou crashen |
| Modification (threat) | Een programma, data of systeem aanpassen waardoor deze andere instructies uitvoerd of onleesbaar word |
| Cybersecurity | Het principe elektronische apparatuur / software / data te beveiligen |
| Breaches | Inbreuken |
| Weaknesses | Zwakheden |
| Malicious | Kwaadaardig |
| Malware | Een samenvatting van verschillende viruses, ransomware en spyware. Het is kwaadaardige software gemaakt door cyberattackers. |
| Hacker | Een persoon die een computer, netwerk of andere skills gebruikt om een technisch probleem te overkomen. |
| White hat hacker | Een hacker met goede intenties |
| Black hat hacker | Een hacker met slechte intenties |
| Gray hat hacker | Is een hacker die soms de wet breekt, maar geen slechte bedoelingen heeft. |
| Cybercrime as a service | Het hacken van een bedrijf om de security van een bedrijf te verbeteren. |
| Script kiddie | Een persoon die denkt dat hij/zij een hacker is maar eigenlijk gewoon voorgeschreven scripts gebruikt. Zoals bv een ddos aanval doen . |
| Hacktivists | Iemand die ongeauthoriseerd toegang heeft tot bestanden of netwerken en deze misbruikt voor sociale of politieke doeleinden |
| Cyber criminals | Iemand die een computer gebruikt om illegale handelingen uit te voeren. Fraude, identiteis diefstal, ... |
| Ethical hacking | Het hacken van netwerken of systemen, met als doel deze te verbeteren door informatie over de hack te geven. |
| Zero-Day | Een nieuwe ondekte exploit, hack, etc. |
| Confidentiality | Beroepsgeheim. Dit is de plicht om te zwijgen over feiten en gegevens tegen derden.. |
| VPN | Een tool die je verbinding encypteerd en je verborgen houd terwijl je surft. Er wordt een veilige verbinding gegarandeerd. |
| Firewall | Een network security system dat al het in en uitgaand verkeer monitord. Het beschermt een netwerk tegen misbruik van buitenaf. |
| CERT | Computer Emergency Response Team. Een team dat beveiligingsincidenten in netwerken en computers afhandelt. Ze proberen de schade te beperken |
| CSIRT | Computer Security Incident Response Team. Een team dat beveiligingsincidenten in netwerken afhandelt. |
| Cyberwarfare | Oorlog die digitaal gevoerd wordt |
| PII (pii) | Personal Identifiable Information. Informatie voor het indentificeren van een persoon |
| IPsec | Beveiligen van het internetprotocol d.m.v. encryptie of authenticatie. |

## Vakjargon thema 3:

|  |  |
| --- | --- |
| Encryption | Het versleutelen van je gegevens, aan de hand van een algoritme. |
| Decryption | Versleutelde gegevens ontcijferen. |
| Cryptanalysis | Decrypteren van codes of geheimschriften. |
| Cryptography | Encrypteren van gegevens met als doel ze beschermen. |
| Algorithm | Het aantal stappen dat je zet om een bepaald doel te bereiken. |
| Key (Cryptography) | Een stuk data dat wordt gebruikt om geëncrypteerde berichten of data de in- of decrypteren. |
| Steganography | Een geheime schrijfkunst, waar er informatie wordt verborgen in onschuldig ogende objecten zoals tekst of afbeeldingen |
| Security through obscurity | Een ouder principe van security, waarbij een systeem veilig is zolang zijn zwakheden verborgen blijven. |
| Kerckhoff’s principle | Een principe uit de cryptografie: “The security of encryption lies in the secrecy of the keys! Not in the algorithm.” Wat betekent dat het niet erg is als het algoritme bekend is door heel de wereld, de key moet geheim blijven. Zolang deze geheim blijft is de encryptie veilig. |
| PKI (public key infrastructure) | Alle processen, protocollen, diensten etc.. die betrekking hebben op het versleutelen van gegevens. |
| Brute force | het kraken van codes door alle mogelijke combinaties uit te proberen. |
| The enigma machine | Een oude codeermachine, ontwikkeld in de jaren twintig door Alan Turing. Het werd tijdens de oorlog vooral gebruikt om veilig berichten door te geven. |
| Entropy (als concept gebruik bij cryptography) | Entropie is de basis waarop alle  cryptografische functies werken. Entropie, in cybersecurity, is een maat voor de willekeur of diversiteit van een functie. Gegevens met volledige entropie zijn volledig willekeurig en er zijn geen betekenisvolle patronen te vinden. Lage entropie gegevens bieden de mogelijkheid om waarden te voorspellen. Dus de maat voor de kwaliteit van cryptografische functies is het meten van de entropie van hun output. |
| Confusion (als concept gebruik bij cryptography) | Confusion betekent dat elk binair cijfer (bit) van de cijfertekst afhankelijk moet zijn van verschillende delen van de sleutel, waardoor de verbindingen tussen de twee onzichtbaar worden. De eigenschap Confusion verbergt de relatie tussen de cijfertekst en de sleutel.Deze eigenschap maakt het moeilijk om de sleutel uit de cijfertekst te vinden en als één enkel bit in een sleutel wordt gewijzigd, worden de meeste of alle bits in de cijfertekst beïnvloed. |
| Diffusion (als concept gebruik bij cryptography) | Diffusie betekent dat als we een enkel bit van de platte tekst veranderen, dan zou (statistisch) de helft van alle bits in de cijfertekst moeten veranderen, en wederom zou op dezelfde manier, als we een bit van de cijfertekst veranderen, dan zou ongeveer de helft van de plain tekst moeten veranderen. |
| Session key | Dit is een symmetrische key die random gegenereerd is maar 1 keer gebruikt kan worden worden. |
| Ephemeral key | Ephemeral keys of vluchtige sleutels zijn geen specifieke vorm van sleutels maar het zijn slechts kortstondige sleutels binnen een sleutel configuration protocol. |
| Block cipher | Dit is een encryptie methode die gewone tekst convert naar ciphertext, door de gewone tekst blok per blok te converteren. |
| Chiper | Een geheime of vermomde manier van schrijven. |

|  |  |
| --- | --- |
| Chiper text | Geëncrypteerde tekst. |
| Keyspace | Dit refereert naar de set van alle mogelijke permutaties van een key |
| Hash | Een digitale vingerafdruk die iedere tekenreeks of bestand via een reeks getallen identificeert. |
| Monoalphabetic ciphers | Een soort substitutieversleuteling waarbij voor het te versleutelen bericht één enkel substitutie-alfabet wordt gebruikt |
| Plain text | Tekst die niet voorzien is van grafische opmaak. |
| Polyalphabetic ciphers | Een vorm van substitutieversleuteling waarbij het substitutie-alfabet tijdens de versleuteling verandert. |
| Stream cipher | Een symmetrische cipher waar plaintext bits gecombineerd worden met een pseudo random getallen (opeenvolging van willekeurige getallen zonder samenhang). |
| Symmetric key | Dit is een sleutel die gebruikt wordt voor zowel het versleutelen als het ontcijferen van data. |
| Asymmetric key | Er worden 2 sleutels aangemaakt. Met de public key wordt de data geëncrypteerd.. Enkel degenen met de private key kunnen deze decrypteren. |
| Cryptanalysis | Het onderzoeken geëncrypteerde berichten en deze decrypteren. |
| Frequency Analysis | Het onderzoeken van patronen of hoe vaak een letter voorkomt in een ciphertext, met als doel deze ciphertext te ontrafelen. |
| Superseded Cryptographic Keys | Verouderde cryptografische keys.  (Cryptografische key: een groep van random karakters in een bepaalde volgorde, die gebruikt worden voor het de- of encryptie van data) |
| Obfuscation (in cryptography) | Het onduidelijk of ingewikkeld maken van data (ipv transformeren door encryptie) |
| Cryptology | De wetenschap van het maken en breken van geheime codes. |

## Vakjargon thema 5

|  |  |
| --- | --- |
| Uptime | Het aantal percent dat een machine (of gewoon computer) werkend en available is. |
| Availabiltiy | De waarscheinlijkheid dat een systeem zal werken hoe deze moet werken in een bepaalde tijdsspanne |
| Asset | Elk object of alles dat een waarde in de organisatie heeft |
| Vulnerability | Een zwakte van deze asset |
| Threat | Elk mogelijk gevaar |
| Risk | Een gevaar dat een gebruik maakt van een zwakte |
| Control | Maatregel om het risico te doen minderen |
| Asset management | In kaart brengen van alle bezittingen van een bedrijf of instantie |
| Asset identification | Wat doet elk asset? |
| Asset classification | In categorien verdelen van elke asset |
| Risico analysys | Is het process van analyseren van gevaren van natuurlijke en door de mens veroorzaakte gebeurtenissen. Zen gebruiker voert een asset-identificatie uit im te bepalen welke items moeten worden beschermd |
| CVE | Common Vulnerabilities and Exposure. Het is een Databank met informatie over kwetsbaarheden in computersystemen en netwerken. |
| Mitigatie (Mitgation) | De ernst van het verlies of de kans dat het optreed wordt verminderd. Het geeft een balans ussen negatieve impact en tegenmaatregelen |
| SOP | Standard Operation Procedure 🡪 gedefineerde methodes die een task of operatie uitvoeren |

## Vakjargon Thema 7

|  |  |
| --- | --- |
| Term | Explanation |
| Zombies | Dit is een computer die geïmplanteerd is met een daemon (een  achtergrondprogramma dat requests behandeld) dat onder de controle is van een hacker, zonder dat de computergebruiker hiervan op de hoogte is.  Zombies worden vaak gebruikt voor DDOS attacks. |
| Maliciously  Formatted  Packets | Een netwerk packet waar malafide code in verwerkt is. |
| ICMP packets | Internet Control Message Protocol packets, geven je informatie over errors die zich voor hebben gedaan tijdens de transport van ip packets. Het ICMP protocol wordt uitgevoerd op de internet layer van het TCP/IP model. |
| Evil Twin attack | Dit is een soort Wi-Fi attack dat misbruik maakt van het feit dat de meeste devices enkel de naam van een draadloos netwerk zien. Hierdoor kan de gebruiker het “Evil Twin” per ongeluk zien als zijn veilige thuisnetwerk, waardoor de hacker de inloggegevens van het netwerk in zijn bezit krijgt. |
| ARP | Address Resolution Protocol is een protocol dat gebruik maakt van een ip adres om het fysieke adres van een computer te achterhalen. Dit wordt gedaan aan de hand van een ARP request. Deze wordt via een broadcast gestuurd, en het device waarvan het ip-adres gelijk is aan dat van het ARP request, stuurt zijn fysiek adres door met een ARP response. |
| MAC | Een Media Access Control Address is het fysieke identificatienummer van elk device op een netwerk. |
| Domain Name  Service | De DNS zorgt ervoor dat we kunnen communiceren via IP-adressen. De dns vertaald de domeinnaam van een webbrowser naar een ip-adres. Waardoor we hiermee verbinding kunnen maken. De DNS kan het ip-adres ook vertalen naar een domeinnaam. |
| cryptographic authentication | Met behulp van grafische sleutels wordt er gecheckt of bepaalde gegevens correct zijn. |
| Session Token | Een sessiontoken wordt aan je toegekend als je je bijvoorbeeld ergens inlogt.  Er wordt gecheckt of je gegevens kloppen en in ruil krijg je de sessiontoken. Deze zorgt dat je aangemeld kan blijven. Eenmaal je je uitlogt vervalt deze. |
| DMZ | Een Data Management Zone is een veilige server die een extra security laag toevoegt aan een netwerk. Het gedraagt zich als een buffer tussen de LAN en het internet. Het is vernoemd naar de demilitarized zones van het leger, die gebruikt werden als een barrière tegen de vijand. |
| Metasploit | Dit is een framework gebaseerd op de programmeertaal Ruby, dat je de mogelijkheid geeft om exploit code te schrijven, testen en uitvoeren. In dit  framework kan je allemaal tools gebruiken om aanvallen te doen, vulnerabilities te zoeken, etc. Het is een penetration testing framework, dat hacken makkelijk maakt. Een belangrijke tool voor veel hackers en defenders. |
| Sandbox | Een virtuele omgeving waar je nieuwe of ongeteste software/code veilig kan runnen |
| Disclosure | Dit is een process waar de analyse van software vulnerabilities zo vroeg mogelijk worden vrijgegeven, zodat iedereen aan deze data kan. |