Week 7a Beveiliging

Juridische context vindt men terug in art. 24 en art 32 AVG.

Beveiligen komt neer op het reguleren van toegang tot goederen zaken.

De doelen van beveiliging, CIA

- Confidentiality, denk aan de documenten op wikileaks, afluisteren bijvoorbeeld
- Integrity, denk aan nep webshops
- Availability, ransomware, het niet onbeschikbaar maken van bestanden

Van kwetsbaarheid in systemen tot schade

- Kwetsbaarheid
- Methode om de kwetsbaarheid in het systeem te misbruiken
- Hierdoor is sprak van een dreiging
- Er wordt overgegaan tot een aanval
- Een succesvolle aanval wordt een incident genoemd
- Het incident veroorzaakt schade
- Uiteindelijk moet een maatregel worden getroffen om de kwetsbaarheid te verminderen

Er zijn verschillende actoren.

Het type actor wordt bepaald door het aantal resources en de vastberadenheid (tijd en doorzettingsvermogen).

Zo zijn er 4 verschillende groepen hackers te onderscheiden:

1. Resources laag, vastberadenheid laag, Vandaal
2. Resources laag, vastberadenheid hoog, Activist
3. Resources middel, vastberadenheid middel, Cybercriminelen
4. Resources hoog, vastberadenheid hoog, Natie-staten (denk aan Rusland/China)

Distributed Denial of Service Attack (DDoS)

Een bekende vorm van hacken, via een zogeheten worm wordt één systeem geïnfiltreerd, vanuit dat systeem gaat die worm verder in andere systemen vaak zonder dat de eigenaren dan wel gebruikers van die systemen het doorhebben. Wanneer de hacker genoeg systemen geïnfiltreerd denkt te hebben kan hij alle systemen tegelijk een bepaalde handeling laten uitvoeren, wat ertoe kan leiden dat de server/systeem het aantal aanvragen niet aankan en het op die manier platgooit

Risicoanalyse

Het risico wordt berekend door de kans dat een bepaalde aanval succesvol afgezet tegen de mogelijke schade dat een aanval zou kunnen aanrichten. Dit wordt weergegeven in relatieve begrippen, laag, midden en hoog. Wat in een matrix weergegeven dus 9 mogelijke uitkomsten heeft, bijvoorbeeld kans midden schade hoog.

Week 7b Beveiligingsmaatregelen

Netwerk beveiliging

De communicatie tussen gebruikers en website moet versleuteld zijn zodat mensen niet kunnen inzien wat jij naar de webserver communiceert, denk aan de inlognamen. Dit is bijvoorbeeld te zien aan een groen slotje voor de websitenaam, dit wordt TLS of SSH genoemd. Dat groene slotje wordt gecreëerd d.m.v. certificaten versleuteling.

VPN

Een Virtual Private Network kan worden gebruikt om af te schermen dat jij gebruik maakt van een website. De Internet Service Provider (ISP) kan niet zien wat jij stuurt naar een webserver maar wel dat je iets stuurt en naar welk IP-adres. Wil je dit voorkomen kan je gebruik maken van een VPN die als tussenschakel in de keten zorgt dat de ISP niet kan zien met wie je als gebruiker communiceert omdat het bericht van gebruiker naar VPN versleuteld is.

Firewall

Kenmerken:

- Filteren op poort of IP-adres
- Kijken of het pakketje wat verstuurd wordt door mag op basis van afzender, wordt vaak onderscheid gemaakt tussen intranet (binnen verkeer) of het internet (buiten verkeer).
- Kan alleen als data niet versleuteld is

Intrusion detection Systemen (IDS)

Het monitoren van het netwerkverkeer en zo proberen verdachte patronen te herkennen en te blokkeren.

- Signature based, herkennen van verdachte patronen op basis van karakteristiek
- Anomalie based, weten wat normaal netwerkgedrag is en elke afwijking daarvan detecteren.

Anders dan een Firewall omdat een Firewall alleen naar individuele pakketjes bekijkt, terwijl een IDS het hele plaatje in de gaten houdt.

Encryptie

- Harddisk encryptie
- De hele externe opslag wordt versleuteld
- Beschermd alleen als de laptop uitstaat omdat er maar één keer een wachtwoord hoeft te worden ingevoerd.
- Denk aan het wachtwoord op je smartphone.
- Versleutelen van individuele bestanden
- Een extra beveiliging op de harddisk encryptie
- Denk aan het beveiligen van je notities in je smartphone, elke keer dat ik een bepaald document open moet ik weer een code invoeren.

Copyright protection

Denk aan e-books, wanneer je een digitaal bestand koopt zit er een privé sleutel in je bestand verwerkt. De aanbieder heeft de publieke sleutel waar informatie in staat over jouw account, doormiddel van dat zogeheten watermerk kan alleen jij als koper dit bestand inzien en wordt het kopiëren van het bestand tegen gegaan.

Systeembeveiliging

Geschiedt in de volgende stappen

- Identificatie, bepalen van iemands identiteit
- Authenticatie, controleren van iemands identiteit
- Authenticiteit, garantie voor de bron van bepaalde informatie

Basisprincipes die hierbij gebruikt worden zijn het volgende

- Something you know, wachtwoorden
- Something you have, een USP
- Something you are, bewijzen dat je iemand bent doordat je een bepaalde sleutel hebt
- Something you do, bepaald gedrag of biometrie

Accescontrol en autorisaties

- Directory, legt per gebruiker voor elk object de bevoegdheden vast
- Accescontrol, legt per object de bevoegdheden van iedere gebruiker vast
- Role based access control, groepeer gebruikers en vervolgens per groep bevoegdheden vaststellen
- Capabilities, bevoegdheden vastleggen in een onvervalsbare token (fietssleutel)