HC 7, 19-03-2019, Beveiliging

Wat is beveiliging
Het gaat bij beveiliging om de vraag: wie heeft toegang tot wat? Beveiliging is het reguleren van toegang tot bepaalde goederen/zaken (assets), maar kan ook toegang tot een netwerk zijn.

Verschillende contexten
Van wie zijn die assets? Gaat het om individuele gebruikers? De context bepaalt *wat* je beschermt, tegen *wie* je het beschermt en *hoe* je het beschermt (hoe ver ga je?)

- Militair
- Overheid: afhankelijk van de (beschikbaarheid) van informatie
- Bedrijfsleven
- Gebruikers

De overheid kan verder gaan bij de beveiliging tegen bepalen entiteiten, dan jij als individuele gebruiker bij beveiliging tegen bijvoorbeeld je buurman.

Het doel van beveiliging

- *Confidentiality* (vertrouwelijkheid) —> beschermen van de vertrouwelijkheid van de gegevens. Hierbij gaat het erom wie toegang heeft en wie niet. Het gaat dus niet om volledige vertrouwelijkheid. De vertrouwelijkheid ziet erop dat bepaalde informatie niet toegankelijk is voor onbevoegden in verband met privacy.
- *Integrity* (integriteit) —> zorgen dat de gegevens correct zijn. Informatie moet kloppen en kloppend blijven (niet onderweg van zender naar ontvanger veranderen).
- *Availability* (beschikbaarheid) —> toegang tot de informatie op willekeurige momenten. Tegenwoordig gaan we er altijd vanuit dat je toegang hebt, tot bijvoorbeeld nestor, e-mail, onedrive etc. Als er dus een keer een storing is, heeft men meteen een groot probleem. Daarom is de beschikbaarheid van informatie dus erg belangrijk.

Deze doelen worden ook wel CIA genoemd.

Terminologie: van kwetsbaarheid tot schade

- *Kwetsbaarheid* (vulnerability) —> 100 procent beveiligde systemen bestaan niet. Er is dus altijd een kwetsbaarheid in de beveiliging van een systeem. Dit geeft een externe partij de mogelijkheid om zich toegang te verschaffen tot de informatie die niet voor hem bestemd is.
- *Methode*: manier om kwetsbaarheid te misbruiken —> Het is in principe geen probleem dat er een kwetsbaarheid in een systeem zit, dit wordt pas een probleem als iemand deze ontdekt en een technische manier weet om misbruik te maken van die kwetsbaarheid.
- *Dreiging*: het feit dat er een kwetsbaarheid is en een methode om die kwetsbaarheid te misbruiken, betekent niet dat er gevaar dreigt. Er moet een entiteit zijn die schade wil berokkenen, er moet dus dreiging zijn.
- *Aanval*: een uitgevoerde dreiging. Hier hoeft ook nog geen probleem te zijn, want de aanval kan worden afgeslagen.
- *Incident*: een succesvolle aanval. Hierdoor wordt echt schade berokkend.
- *Schade*: veroorzaakt door een incident. Schade kan direct financieel zijn, maar ook indirect (bijvoorbeeld als je fabriek een tijd niet kan draaien).
- *Maatregel*: herstellen van de kwetsbaarheid. Waarschijnlijk zijn er echter nog meer kwetsbaarheden in het systeem.

Actoren
Dit zijn degenen die uiteindelijk echt schade berokkenen. Het type actor wordt bepaald door:

- R: hoeveelheid **R**esources (geld, technische kennis).
- V: mate van **V**astberadenheid (tijd, doorzettingsvermogen).

We onderscheiden de volgende categorieën:

- **Vandaal**. R: laag, V:laag. Het is redelijk makkelijk om je hiertegen te beschermen. Je moet er slechts voor zorgen dat jouw systeem net beter is beveiligd dan andere systemen die ook het doelwit zijn van de aanval van deze vandaal.
- **Activist**. R: laag, V: hoog. Activist heeft specifiek tot doel om jou schade te berokkenen. Zo'n activist zal doorgaan tot het is gelukt, ook al heeft hij misschien niet alle resources.
- **Cybercriminelen**. R: middel, V: middel. De hoeveelheid geld en tijd die het voor hen kost moet het wel waard zijn. Als het niks oplevert, zullen ze er niet mee door gaan.
- **Natie-staten**. R: hoog, V: hoog. Denk aan landen als de V.S. Of Rusland. Deze landen hebben veel resources en de kennis. Ook zullen ze niet loslaten als ze eenmaal iets hebben gevonden waaraan ze schade willen berokkenen.

Voorbeelden

De Morris Worm (1988)

Dit is een van de eerste virussen die op het internet de ronde deed. Een computer die op de een of andere manier slachtoffer is geworden van een aanval, wordt geïnfecteerd. Omdat het systeem is verbonden met een netwerk, kan het via daar andere systemen ook infecteren. Dat gaat als volgt.

1. Via het netwerk kan het systeem erachter komen welke soort systemen nog meer verbonden zijn met het netwerk. Vervolgens kan het systeem een aanval doen om zwakheden te testen.
2. Het systeem doet een aanvraag naar het hoofdprogramma; van welk systeem maakt de computer gebruik? Dit antwoord wordt teruggestuurd. Daardoor weet het systeem waar de zwakheden zitten.
3. De worm (het virus) kan worden verstuurd.

Free WiFi access point

Als je een keer bent verbonden met een netwerk, maakt jouw computer de volgende keer weer automatisch daarmee verbinding. Als je dit dus hebt gedaan bij een free-WiFi netwerk, maakt jouw computer telkens automatisch verbinding met vrije wifi-netwerken. Omdat die verbinding niet beschermd is, kan een kwaadwillende hacker meekijken met al dit draadloze netwerkverkeer. De enige manier om dit te voorkomen, is om te kijken of de websites die je bezoekt, gebruik maken van een beveiligde verbinding.

Kraken beveiliging: WW II

In de Tweede Wereldoorlog werd de Duitse Enigma gekraakt. Toen werd dus de beveiliging gekraakt. Tegenwoordig is dat niet meer te doen, daarom worden vaak de apparaten waarmee wordt verzonden en ontvangen, gekraakt (telefoon, computer).

Distributed Denial of Service attack

Als maar voldoende computers tegelijk verbinding proberen te maken met een bepaalde server en allemaal tegelijk een 'bericht' sturen naar een website, dan krijgt de server het moeilijk en kunnen minder bezoekers bij de website. Een hacker bewerkstelligt dit door een groot aantal computers op een netwerk te infecteren met een virus en deze allemaal tegelijk een bericht laten sturen naar een bepaalde server. Zo kan de hacker ervoor zorgen dat een website platligt. Om een goede aanval uit te kunnen voeren, is het handig om computers te infecteren die een hele goede netwerkverbinding hebben en dus veel berichten tegelijk kunnen versturen. Deze zijn wel lastiger te infecteren dan computers met een minder goede verbinding.

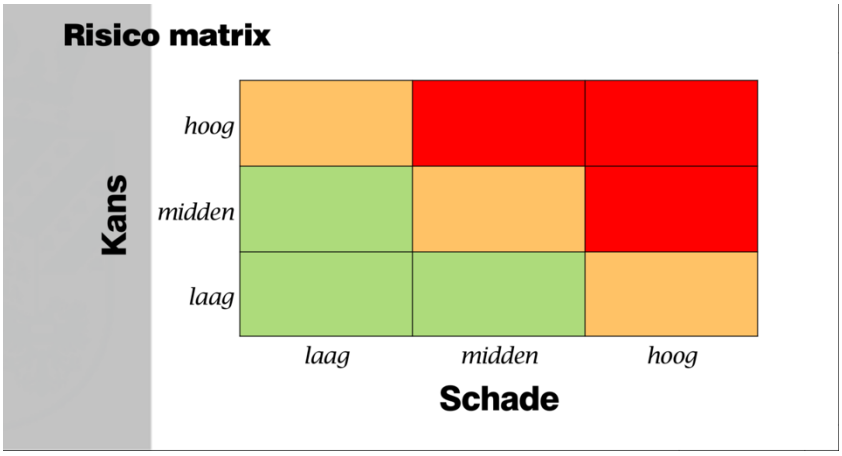
Risico analyse

Hoe kan je je systeem goed genoeg beveiligen? Daar is een risico analyse voor bedoeld. Daarmee probeer je op een iets hoger abstractieniveau naar de beveiliging van je systemen te kijken. Bij de risico analyse wordt van het volgende uitgegaan:

Risico = kans x schade

Het risico wordt groter, naarmate de kans op een probleem groter wordt. Het risico wordt ook groter naarmate de schade, die voortvloeit uit een niet goed beveiligd systeem, groter is. Je kan nooit exact de

kans of de schade uitdrukken, daarom wordt hierbij geschat of de kans of schade hoog, midden of laag is. Hierbij is het van belang om aan de juiste mensen te vragen om dit in te schatten. De kans is te bepalen door een inhoudelijke expert en de schade door een proces verantwoordelijke.



Netwerkbeveiliging

Beveiligde verbindingen: TLS, SSH

Beveiligde verbinding zorgt ervoor dat je zeker weet dat het de juiste website is waar je mee communiceert. Als je je gebruikersnaam en wachtwoord invoert, kan niemand meekijken en die achterhalen. Ook worden beveiligde verbindingen gebruikt om transacties te doen en dat deze juist overkomen. Dus als je 100 euro wil overmaken, dat iemand er niet stiekem een 0 aan toevoegt.

VPN: Virtual Private Network

De verbinding tussen jouw computer en de VPN provider is beveiligd. Daarom kan niemand deze berichten onderscheppen. Ook krijgt de website die jij bezoekt niet jouw IP-adres te zien, maar die van jouw VPN-provider. Dat is voordelig, omdat IP-adressen vaak iets zeggen over jouw locatie. Veel websites baseren hun aanbod op het land waar je zit. Ten slotte is het voor bedrijven voordelig om gebruik te maken van een VPN. De reden daarvoor is dat als medewerkers thuis werken, je als bedrijf graag wil dat alle communicatie beveiligd is. Voordat medewerkers bij de database van het bedrijf kan, moeten zij dan verbonden zijn met de VPN-provider van hun bedrijf.

Firewall

Als je als bedrijf een eigen bedrijfsnetwerk hebt, wil je ervoor zorgen dat alleen computers die in je bedrijf zitten verbinding met elkaar kunnen maken. Je wil niet dat willekeurige computers buiten het bedrijf verbinding kunnen maken met de computers binnen het bedrijf. Om dit te voorkomen is er het principe van de Firewall. Dit is een virtuele muur tussen het intranet (alle computers binnen het bedrijfsnetwerk) en alle computers op het internet daarbuiten.

De Firewall kijkt naar ieder pakketje en het daaraan gelinkte IP-adres, als er een pakketje binnenkomt van een computer buiten het intranet. Als zo'n pakketje specifiek gericht is aan een IP-adres binnen het intranet, dan komt die niet binnen. Alle pakketjes van buiten die bedoeld zijn voor de webserver, zijn wel toelaatbaar. De server moet van buiten wel bereikbaar zijn. Daarnaast moeten medewerkers die thuis werken ook verbinding kunnen maken met de VPN-server.

Bij Application proxies wordt niet alleen naar de IP-adressen van de pakketjes gekeken, maar ook naar de inhoud. Op basis daarvan kan het pakketje niet betrouwbaar worden geacht. Dit is alleen mogelijk als de data niet versleuteld is.

Intrusion detection systemen (IDS)

Deze systemen monitoren het netwerk verkeer en proberen verdachte patronen te herkennen en te blokkeren.

- **Signature-based:** herkennen verdachte patronen op basis van karakteristieke patronen. Dit is dus op basis van eerdere aanvallen op systemen. Dit kan nieuwe aanvallen dus niet herkennen.
- **Anomalie-gebaseerd:** weten wat 'normaal' netwerk gedrag is en detecteren afwijkingen daarvan. Hierbij laat je het netwerk draaien en kijk je wat het normale gebruik van dit netwerk is (bijvoorbeeld er wordt enkel gebruik gemaakt van het netwerk tussen 9 en 5 en plotseling wordt netwerkverkeer gedetecteerd in de avonduren). Dit systeem kan nieuwe aanvallen wel herkennen. Het kan echter voorkomen dat er een signaal uitgaat dat er iets aan de hand is, terwijl dat niet zo is. Bijvoorbeeld als iemand aan het overwerken is.

Informatiebeveiliging
Hieronder komen twee vormen van informatiebeveiliging aan bod.

Encryptie
Beschikbaarheid van informatie wordt niet beschermd door encryptie. Je kan op verschillende manieren versleutelen:

1. Versleutelen van individuele bestanden. Bij het lezen of schrijven moet het bestand dan worden ontsleuteld en vervolgens weer worden versleuteld. Hierbij is ieder bestand apart versleuteld. Voor ieder bestand moet je een aparte code invoeren voor het activeren van de cryptografische sleutel.
2. Harddisc encryptie. Alle informatie op je harde schijf wordt versleuteld. Het gevolg daarvan is dat je een andere soort beveiliging hebt. Als je computer uitstaat dan is alle informatie op de harde schijf versleuteld, maar als je computer aan is dan heeft je systeem de sleutel om bij alle bestanden te kunnen actief gemaakt. Daardoor kan je systeem bij al je bestanden. De informatie is pas niet meer beschikbaar als je de computer uitschakelt.

Copyright protection
Een derde partij probeert jouw toegang tot jouw eigen informatie te beperken. Bijvoorbeeld als je online een boek hebt gekocht, dan zorgt dat systeem ervoor dat jij op jouw computer hier toegang tot hebt maar dat je hier niet zomaar een kopie van kan maken. Bij encryptie kan je aan iedereen de sleutel geven zodat ook anderen toegang hebben. Dat is dus geen vorm van copyright protection.