Inleiding IT-recht - HC 7A, 05-01-21, IT-beveiliging

Actualiteit

In het huidige tijdperk is er sprake van onder andere hacken, DDoS-aanvallen en phising-fraude. Op deze, en meer, gebieden komt de IT-beveiliging aan bod.

Context in IT-recht

IT-beveiliging is begonnen als computer security. Hierbij gaat men ervan uit dat het apparaat beschermd wordt en dat het doel is om hier enkel de juiste mensen bij te laten. Vervolgens moet er overgegaan worden naar information security. Hierbij moet juist de informatie op het apparaat beschermd worden. Dit moet omdat het steeds normaler is dat computers verbonden zijn met netwerken en dat juist de informatie hierbij beschermd moet zijn.

Bij de overheid, die vanaf het begin veel registers heeft gehad, is veel budget gegeven voor de beveiliging. Dit betreft dan het staatsrecht, maar ook het internationaal recht omdat hier geheime informatie is die beschermd moet worden tegen derden waarbij de staatsveiligheid ook is gediend. Daarnaast komt het bedrijfsleven ook aan bod bij de beveiliging, omdat hier ook veel kennis geheimgehouden moet worden (contracten, intellectueel eigendomsrecht en geheimhoudingsovereenkomsten hebben dit ook als doel). Dit betreft naast de kennis ook vaak de diensten die beschikbaar moeten zijn en blijven. Een belangrijk aspect is dat enkel de bevoegde werknemers bij bepaalde informatie te komen, want anders kunnen werknemers informatie zien waar zij helemaal niet bij horen te komen. Tot slot hebben ook particulieren belang bij IT-beveiliging, maar zij hebben hier minder geld voor waardoor zij zich in een moeilijk beschermbare positie bevinden. Bij de gegevensbescherming zal hier dan de bedoeling zijn dat normen worden opgelegd dat andere actoren niet alles met jouw gegevens kunnen doen. Hier zal dan bijvoorbeeld eerst toestemming gegeven moeten worden en kan aansprakelijkheid bij misbruik in het leven komen.

Functies IT-beveiliging

IT-beveiliging heeft sinds oudsher meerdere functies, welke samen de **CIA-triad** worden genoemd. Confidentiality (vertrouwelijkheid), Integrity (integriteit) en Availability (beschikbaarheid).

<u>Beschikbaarheid</u>
Gegevens moeten op het juiste moment voorhanden zijn. Hierbij zijn DDoS-aanvallen een mooi voorbeeld van, omdat deze de beschikbaarheid kunnen verstoren. Hiermee wordt de IT-beveiliging mooi uitgelegd, want deze is van belang om de DDoS-aanvallen tegen te kunnen gaan om de beschikbaarheid te handhaven. Tegenwoordig zitten niet enkel computers op netwerken maar betreffen dit ook dingen die we dagelijks gebruiken (denk aan wasmachines, auto's, telefoons). Een van de problemen van deze 'internet of things' is dat beveiliging van deze apparaten niet enorm deugdelijk is, waardoor deze vatbaar zijn voor indringing van buitenaf.

Om te kijken naar de wet en DDoS-aanvallen kijkt men voornamelijk naar het wetboek van Strafrecht (zie bijvoorbeeld artikel 138b lid 1 jo. 2 Sr). Daarnaast kan het ook vanuit het privaatrecht worden behandeld. Denk hierbij aan de artikelen 6:74 jo. 6:75 BW, aangezien DDoS-aanvallen overmacht kunnen veroorzaken. Wanneer de voorzorgsmaatregelen mochten worden verwacht maar deze niet zijn vervuld, dan is er sprake van schuld. Hierbij kan men denken aan updates die niet zijn uitgevoerd.

De beschikbaarheid kan ook contractueel worden vastgelegd in situaties. Denk hierbiij bijvoorbeeld aan Saas, waarbij een servicelevel agreement een bepaalde uptime kan verzekeren. Daarnaast kan vastgelegd worden wat geldt als overmacht en wat er gebeurt als er niet wordt nagekomen.

Een **DDoS-aanval** werkt door middel van iemand die achter zijn computer zit met de beschikking over een controller. Deze controller zet malware uit (kwaadaardige (stukjes) software) op niet beveiligde computers. Door deze software kunnen deze niet goed beveiligde computers de opdracht krijgen om verzoeken naar het slachtoffer te doen. Het doel is niet om in te breken maar puur om het netwerk, door de vele verzoeken, te belasten waardoor deze zichzelf uitgeschakeld. Gaat dit lang door, dan kan het gevolg zijn dat het slachtoffer enorm lang de tijd nodig heeft om zichzelf weer te herpakken.

Integriteit, vertrouwelijkheid
Bij de SolarWinds-hack zijn veel accounts geraakt. Hierbij hebben derden informatie gezien die ze niet aanging en is de beveiliging van accounts dus doorbroken. Ook kan het zijn dat dingen van partij naar partij gestuurd worden en men probeert hiertussen te komen om de informatie in te zien (man in the middle – attack). Men probeert de informatie als zodanig te versleutelen zodat wanneer iemand de informatie in handen krijgt deze niks aan de inhoud heeft. Dit gebeurde in bijvoorbeeld de EncroChat-hack. Hierbij gebruikt men dus de encryptie van berichten(verkeer).

Wanneer gesproken wordt over de vertrouwelijkheid van accounts dan wil men dat deze beveiligd zijn. Bij de beveiliging kan het best gebruik gemaakt worden van een wachtwoordmanager. Bij essentiële organisaties wordt steeds vaker gebruik gemaakt van multi-factor authenticatie (combinaties van iets wat je kent, iets wat je bent en iets wat je hebt). Deze beveiliging wordt niet enkel technisch gereguleerd maar ook in het strafrecht door bijvoorbeeld artikel 138ab Sr (computervredebreuk). Vanuit de AVG is de bescherming van de persoonsgegevens ook weer een zaak van de beveiliging. De verwerkingsverantwoordelijke heeft hierbij ook de plichten om passende technische organisatorische maatregelen treffen blijkens artikel 32 AVG.

In het berichtenverkeer moet men dan ook het onderscheid maken tussen enerzijds de beveiliging van de toegang tot een account en anderzijds de beveiliging van het berichtenverkeer (denk hierbij aan de end-to-end encryptie).

De encryptie van berichten kunnen met de eenvoudige symmetrische versleuteling. Daarnaast bestaat ook de asymmetrische versleuteling. Deze laatste versleuteling gaat softwarematig, waarbij het ook goed mogelijk is dat een derde partij is (trusted third party). Deze software zal public keys registreren, identiteit verifiëren, private sleutels aanmaken en certificaten ter bevestiging van de authenticatie aanmaken. Bij de asymmetrische versleuteling kan het zijn dat deze automatisch is ingeschakeld, wat voor het berichtenverkeer absolute beveiliging levert. Dit houdt dit niet in dat de metadata (wanneer wordt ingelogd, met wie en waarvandaan) beschermd is. Daarnaast kan de telefoon ook gestolen/gehackt worden en kan het zijn dat de justitie toch een sleutel heeft en hier dus bij kan komen.

De juridische functie van encryptie is in de eIDAS-verordening te vinden. Denk hiernaast aan de elektronische handtekening (artikel 7:932 BW) en de elektronisch aangetekende bezorging, omkering van de bewijslast.

Handhaving van recht
Voor de handhaving zijn specifieke toepassingen van de IT voor beveiliging van IE-beschermde producten. Een voorbeeld hiervan is de Sony rootkit.

IT-beveiliging en internet governance
In college 1A is ingegaan op de theorie van Lessig. Hij stelde dat het rondom internet (überhaupt het gehele recht) te beperkt is dat de juridische positie van een persoon of organisatie, enkel door wetten

en contracten, kan worden bepaald. Het is wel belangrijk, maar het is niet bepalend. Naast het recht nemen ook sociale normen en marktwerking een rol in de bepaling van ons gedrag.