Auteurs: Mr. drs. A.P. Freund is Information Security Consultant en adviseert over informatiebeveiliging en compliance, geeft awareness trainingen en begeleidt crisisoefeningen. Alexander is bereikbaar via a.freund@ictrecht.nl. Mr. R.A. van der Geest is jurist en houdt zich, onder andere, bezig met advisering over nieuwe technologie. Ook is hij deelnemer aan de Nederlandse AI coalitie. Ruben is bereikbaar via r.vandergeest@ictrecht.nl. Beide auteurs werken bij het juridisch adviesbureau ICTRecht te Amsterdam.

Lig jij ook wakker van ransomware?

De afgelopen jaren lijkt het aantal ransomware-aanvallen schrikbarend te zijn toegenomen. Mede door de verstrekkende gevolgen van een aanval bleef de aandacht hiervoor niet alleen beperkt tot de media die door 'security geeks' wordt bijgehouden, maar werd er ook veelvuldig over geschreven in de dagelijkse media. Verschillende ransomware-aanvallen die in Nederland hebben plaatsgevonden, hebben wijze lessen opgeleverd. Zoals de aanval die de gemeente Hof van Twente in december 2020 trof en de aanval waardoor de Universiteit Maastricht in december 2019 werd platgelegd.

De echte kenner zal zich de aanval uit juni 2017 ook nog herinneren waarbij een gedeelte van de Rotterdamse haven werd getroffen. Dit soort aanvallen kunnen grote gevolgen hebben voor de getroffen partijen en het is daarom van belang om meer inzicht te krijgen in ransomware, hoe men zich ertegen kan beschermen en welke wet- en regelgeving relevant is. In dit artikel gaan wij daarom dieper in op wat ransomware eigenlijk is, het wettelijk kader en de relevante meldplichten, hoe men zich hiertegen kan wapenen en of een cyberverzekering mogelijk uitkomst biedt.

Ransomware: wat, hoe en waarom?

Ransomware is te kwalificeren als kwaadaardige software ('malware') die bestanden versleutelt ('encrypt') of de toegang tot een volledig systeem blokkeert. Ook zaken zoals mobiele telefoons, back-ups en gegevens die in de cloud zijn opgeslagen kunnen versleuteld worden door ransomware. Het versleutelde systeem of de bestanden zouden in principe weer bruikbaar moeten zijn nadat deze ontsleuteld ('decrypted') zijn na het betalen van losgeld ('ransom') aan de aanvaller.

Een ransomware-aanval kan uitgevoerd worden doordat deze gebruikmaakt van zwakheden in bepaalde systemen of de gebruikers ervan. De voornaamste oorzaak hiervan betreft software die niet is bijgewerkt met de meest recente software updates of bijvoorbeeld een RDP (` remote desktop protocol') welke niet goed geconfigureerd is of zwakheden bevat. Juist tijdens de coronacrisis gingen mensen meer vanuit huis werken, waardoor zij veelvuldig gebruikmaakten van RDP of ze inlogden op het bedrijfsnetwerk via de privé computer (welke niet altijd zo goed is bijgewerkt als de zakelijke computer). Dit is mede één van de redenen waarom we een flinke toename van ransomware-aanvallen hebben gezien ten tijde van de coronacrisis.

Gesteld kan worden dat het uitvoeren van ransomware-aanvallen een businessmodel is geworden. Er worden flinke bedragen geëist en soms ook betaald, waardoor het een lucratieve praktijk is voor bepaalde groeperingen. Men moet niet versteld staan als een hulpvaardige '*helpdesk*' staat te trappelen om het slachtoffer door het hele proces te loodsen.

Beveiliging

Ransomware kan alleen schade aanrichten als een apparaat geïnfecteerd raakt. De aanvaller moet de ransomware dus op de een of andere manier op apparaten van het doelwit installeren. Dit kan komen door een menselijke fout (de welbekende phishing e-mail) of door een zwak punt in de beveiliging. Beveiliging met betrekking tot ransomware heeft dan ook twee kanten, een organisatorische en een technische kant. De organisatorische kant poogt menselijke fouten te voorkomen en de technische kant tracht het digitaal inbreken in de systemen tegen te gaan.

Er is veel wetgeving die bedrijven verplicht om goede beveiligingsmaatregelen te nemen, denk bijvoorbeeld aan de Algemene verordening gegevensbescherming (AVG) en de Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze verplichting ziet niet alleen op de technische kant, maar ook op de organisatorische kant.

Technische en organisatorische maatregelen

Uiteindelijk kan bijna elk systeem worden gehackt. Dit is een uitgangspunt dat ook in de rechtspraak terugkomt (1). Dat betekent niet dat er niets gedaan kan worden om dit zo moeilijk mogelijk te maken. Er wordt wel verwacht van bedrijven dat zij zich inspannen om het risico zoveel mogelijk te beperken. Zo staat bijvoorbeeld in de AVG de verplichting dat er passende maatregelen genomen dienen te worden. Om te bepalen wat 'passend' is dient rekening gehouden te worden met onder andere de stand van de techniek ('the state-of-the-art') en de verwerking waar het om draait. Hoe groter de risico's, hoe meer beveiligingsmaatregelen verwacht worden.

Minimale beveiligingsmaatregelen in het digitale domein zijn lastiger te definiëren en preciseren dan in de 'analoge wereld'. In de polisvoorwaarden van een fietsverzekering staat vaak duidelijk aangegeven dat er een bepaald type slot nodig is. Bijvoorbeeld een ART 2 goedgekeurd slot in de ANWB-fietsverzekering. In de digitale wereld is dat dus een stuk lastiger. Er zijn wel bepaalde standaarden waaraan bedrijven zich kunnen conformeren, denk aan de ISO27000 serie of de verschillende NEN-normen, maar deze zijn vaak technologieneutraal opgesteld. Technologieneutraal is een uitgangspunt waar juristen dol op zijn, maar waar IT'ers minder blij van worden. Aan de ene kant biedt het ruimte om mee te groeien met de razendsnelle ontwikkelingen in het digitale domein, maar aan de andere kant is het onduidelijk wat er nu precies van een bedrijf verwacht wordt.

Wat betreft organisatorische maatregelen speelt eenzelfde onduidelijkheid, want hoe weet je nu of er inderdaad voldoende is gedaan en of het onderwerp wel voldoende 'leeft' binnen de organisatie en niet alleen een papieren werkelijkheid blijft? In de praktijk wordt dit voornamelijk ondervangen door het personeel te trainen op dit gebied en te zorgen voor alertheid door het creëren van bewustwording over de mogelijke risico's. Een bedrijf met state of the art beveiligingssoftware is nergens wanneer een medewerker een malafide bestand downloadt of op een phishing link klikt. Het is dus uitermate belangrijk om medewerkers te trainen en ze constant te wijzen op mogelijke risico's. Dit kan bijvoorbeeld gedaan worden door medewerkers deel te laten nemen aan cursussen of simulaties, maar ook door ze te voorzien van informatie via een personeelshandboek. Een belangrijke tip is ook, beperk bewustwording niet tot (middle)management maar betrek het hele bedrijf daarbij. Ransomware kan net zo goed een bedrijf binnendringen via de terminal in een pakhuis als via de laptop van de CFO.

Externe partijen

Een bedrijf heeft dus de verantwoordelijkheid om haar beveiliging goed op orde te hebben. Toch is zij niet altijd de enige die daar verantwoordelijk voor is. Veel bedrijven hebben het opzetten en beheren van hun IT-omgeving (gedeeltelijk) uitbesteed aan derde partijen. Deze derde partijen hebben een zorgplicht die van hen onder meer vereist dat ze de beveiliging goed inrichten (2).
De omvang van deze zorgplicht is afhankelijk van de situatie. Wanneer een complete digitale infrastructuur wordt afgenomen, mag er meer verwacht worden van de

leverancier dan wanneer het gaat om slechts het afnemen van een programma voor tekstverwerking. Verder is ook de deskundigheid van de partijen van belang. Een grote mate van deskundigheid bij de leverancier zorgt voor een zwaardere zorgplicht. De deskundigheid van de afnemer wordt ook meegewogen bij het bepalen van de omvang van de zorgplicht (3). Het gaat erom dat de dienstverlening voldoet aan de mate van zorgvuldigheid die van een redelijk handelend en bekwaam IT-deskundige geëist mag worden.

Zo omvangrijk kan de zorgplicht zijn

De zorgplicht kan in sommige gevallen erg omvangrijk zijn, zo blijkt onder meer uit een uitspraak van de rechtbank Amsterdam uit 2018. In deze zaak ging het om een IT-leverancier die de gehele IT-infrastructuur voor diens klant zou verzorgen. Het ging hier om een 'totaalpakket'. De leverancier had aan de klant aangegeven dat er bepaalde beveiligingsmaatregelen genomen dienden te worden, maar de klant wilde dit uitdrukkelijk niet. Hierdoor was de IT-infrastructuur onvoldoende beveiligd.
De rechtbank oordeelde dat de leverancier niet zomaar akkoord had mogen gaan met de wens van de klant. De leverancier had in dit geval de opdracht moeten weigeren, alternatieven moeten aandragen of minstens meerdere malen (schriftelijk) moeten waarschuwen voor de risico's. Deze waarschuwing moet de klant in staat stellen de risico's te begrijpen en er moet duidelijk zijn welke stappen de klant dient te nemen om de risico's te mitigeren. De leverancier had dit niet gedaan en was daarom voor een deel van de schade aansprakelijk.

De aansprakelijkheid van de leverancier, in de in het kader genoemde uitspraak, kwam mede door het ontbreken van duidelijke afspraken. In de overeenkomst werd enkel gesproken over een 'totaalpakket', de wens van de klant om bepaalde beveiligingsmaatregelen niet in te voeren werd niet schriftelijk vastgelegd. Het is dus van belang, zowel voor de leverancier als de klant, om deze afspraken goed vast te leggen.

Uit de rechtspraak blijkt echter wel dat de grondregel is: als er geen specifieke afspraken over beveiliging worden gemaakt, dan dient de leverancier de beveiliging te regelen (4). In de praktijk worden vaak wel duidelijke afspraken gemaakt of wordt de aansprakelijkheid (gedeeltelijk) uitgesloten. Dit neemt niet weg dat IT-leveranciers wel degelijk een zorgplicht hebben.
Bij het inschakelen van een IT-leverancier om een 'totaalpakket' af te nemen mag dan ook verwacht worden dat de beveiliging goed geregeld wordt en dat eventuele gaten of zwakke punten in de beveiliging door de leverancier worden opgepakt en anders duidelijk gemeld worden (5).

Meldplicht

Een andere verantwoordelijkheid die een bedrijf heeft, is het melden van het beveiligingsincident. Er bestaan verschillende meldplichten, maar de bekendste meldplicht is waarschijnlijk die uit de AVG. Dit is ook de meldplicht die voor vrijwel alle partijen geldt. Er zijn echter ook andere, sectorspecifieke, meldplichten.
De reden voor deze hoeveelheid aan meldplichten is mede dat een succesvolle ransomware-aanval in veel gevallen zorgt voor een onderbreking van de dienstverlening. Veel sectorale wetgeving kent een meldplicht in het geval de dienstverlening onderbroken wordt. Denk bijvoorbeeld aan het uitvallen van een communicatienetwerk of een nutsvoorziening. Het gevolg is dat een ransomware-aanval dan ook gemeld dient te worden.
Hier wordt eerst de meldplicht uit de AVG behandeld, vervolgens enkele sectorspecifieke meldplichten en als laatste nog aangifte bij de politie.

AVG

Wanneer blijkt dat er persoonsgegevens betrokken zijn bij het beveiligingsincident komt de AVG om de hoek kijken. De AVG noemt een dergelijk beveiligingsincident een 'inbreuk in verband met persoonsgegevens'. In de volksmond wordt dit vaak een datalek genoemd. Mogelijk moet een datalek gemeld worden bij de Autoriteit Persoonsgegevens (AP) en betrokkenen. Of je dient te melden is afhankelijk van de situatie.

De eerste stap om te bepalen wat er dient te gebeuren, is het vaststellen van de rolverdeling. Er zijn in dit verband twee smaken: je verwerkt de gegevens voor jezelf of voor

De verwerkingsverantwoordelijke is verantwoordelijk voor het melden van een datalek. Als je verwerker bent, hoef je alleen het (mogelijke) datalek te melden bij de verwerkingsverantwoordelijke.

een andere partij. Wanneer je zelf het doel en de middelen van de verwerking kiest, dan ben je *verwerkingsverantwoordelijke*. Wanneer je enkel de gegevens verwerkt voor een andere partij (je levert bijvoorbeeld een hostingdienst) dan ben je de *verwerker*. Dit onderscheid is van belang omdat de *verwerkingsverantwoordelijke* verantwoordelijk is voor het melden van het datalek. Als je verwerker bent hoef je alleen het (mogelijke) datalek te melden bij de verwerkingsverantwoordelijke. Hoe dit precies dient te gebeuren en hoelang je hiervoor hebt, hangt af van de afspraken die gemaakt zijn in de verwerkersovereenkomst. Dit kan dus per verwerkingsverantwoordelijke verschillen. Wanneer je bijvoorbeeld verwerkt voor honderd klanten en je sluit met elk van hen een verwerkersovereenkomst die zij zelf aanleveren, dan kunnen de afspraken flink verschillen. In het geval je het slachtoffer bent van ransomware kan het zijn dat je bij al die honderd klanten moet aangeven dat er een datalek is geweest. Het is dus van belang dat je de verschillende afspraken en termijnen duidelijk hebt, want het kan nare gevolgen hebben als je hierin fouten maakt. Bij het afhandelen van het datalek zelf dien je de verwerkingsverantwoordelijke bij te staan voor zover dat redelijk is ten opzichte van de verhouding.

Stel dat je verantwoordelijke bent, dan moet je gaan kijken of en bij wie je moet melden. In sommige gevallen dient enkel gemeld te worden bij de AP en in andere gevallen bij zowel de AP als ook bij de betrokkenen. Als er géén risico voor de betrokkenen is, hoeft een datalek niet gemeld te worden. Van welke situatie er ook sprake is, het incident dient in ieder geval intern geregistreerd te worden.

Bij wie er precies gemeld dient te worden is dus afhankelijk van de impact van het datalek. Een datalek dat een risico inhoudt voor de rechten en vrijheden van natuurlijke personen dient bij de AP gemeld te worden. Deze mededeling bij de AP dient zonder onredelijke vertraging en uiterlijk 72 uur na het ontdekken van het datalek te geschieden. Deze termijn geldt alleen voor de verwerkingsverantwoordelijke. Wanneer het datalek bij een verwerker heeft plaatsgevonden, vangt de termijn van 72 uur pas aan op het moment dat de verwerker het datalek heeft medegedeeld aan de verwerkingsverantwoordelijke. Dus als is afgesproken dat de verwerker het datalek moet mededelen binnen 24 uur, dan is er dus een totale termijn van 96 uur. Houd de termijn van 72 uur goed in de gaten. Het te laat melden leverde Booking.com een boete van 475.000 euro op! (6)

Wanneer er precies sprake is van een risico voor de rechten en vrijheden van natuurlijke personen is niet altijd duidelijk. Als het bijvoorbeeld gaat om ransomware waar enkel de gegevens gegijzeld worden (en deze dus niet inzichtelijk zijn voor de hacker) en er is een back-up beschikbaar, dan is er mogelijk geen risico voor de betrokkenen. De bedrijfsvoering kan immers doorgaan en er zijn geen persoonlijke gegevens gelekt. In het geval dat er sprake is van dubbele afpersing (`double extortion') is dit een ander verhaal. Bij double extortion worden niet alleen de gegevens gegijzeld, maar wordt er ook nog gedreigd om de gegevens openbaar te maken. De gegevens kunnen immers openbaar gemaakt worden en dat is een risico voor betrokkenen.

Het melden van een datalek betekent niet dat u direct een boete ontvangt. Er wordt slechts naar een klein deel van de gemelde datalekken onderzoek gedaan en het kan ook nog zijn dat het datalek niet ernstig genoeg is om een boete op te leveren. Als de melding al wordt behandeld, vindt er dus ook nog een afweging plaats. Het kan zijn dat de AP het naast zich neerlegt of enkel een waarschuwing geeft. Als een dergelijk datalek niet gemeld zou zijn, dan kan er alsnog een boete volgen voor het niet melden. Dit kan flink in de papieren lopen.

Naast de AP kan het ook zijn dat een datalek gemeld moet worden aan de betrokkenen, dit zijn de personen wiens persoonsgegevens betrokken zijn bij het beveiligingsincident. Deze toets is anders dan bij het melden aan de AP. Er moet namelijk gemeld worden aan de betrokkene wanneer het waarschijnlijk is dat het datalek een hoog risico inhoudt voor diens rechten en vrijheden. Bij de AP gaat het dus om elk risico en bij de betrokkenen om een hoog risico.

Er is in ieder geval sprake van een hoog risico als het gaat om *bijzondere persoonsgegevens*. Bijzondere persoonsgegevens zijn gegevens over de gezondheid van mensen, maar ook gegevens die iets zeggen over de politieke voorkeur, het ras of de religie van een persoon. Vaak wordt er door bedrijven te snel over dit punt heen gestapt, als het gaat om bijzondere persoonsgegevens denkt men vaak eerst aan zorginstellingen en gebedshuizen. Niets is minder waar. Veel bedrijven verwerken bijzondere persoonsgegevens. Denk bijvoorbeeld aan een concertzaal die tickets op naam zet en ook tickets voor mensen met een handicap verkoopt. Een ander voorbeeld is de personeelsregistratie waarin misschien verzuimgegevens zijn opgenomen.

Wanneer het niet gaat om bijzondere persoonsgegevens moet het datalek alsnog gemeld worden wanneer de aard van de getroffen gegevens of de aard van het incident maakt dat er een concreet risico voor betrokkenen kan ontstaan. Denk bijvoorbeeld aan een gehackte mailbox, dit brengt het risico met zich mee dat betrokkenen slachtoffer worden van phishing-mails. Een ander voorbeeld betreft financiële gegevens die gebruikt kunnen worden om geld te stelen van betrokkenen.

In het geval dat melden aan betrokkenen niet verplicht is, dient ook stil te worden gestaan bij de vraag of melden aan betrokkenen gewenst is. Er is altijd een kans dat het nieuws van het datalek naar buiten komt. Dan kan het soms beter zijn om dat nieuws voor te zijn en de betrokkenen zelf in te lichten.

Overige meldplichten

Naast de meldplicht uit de AVG kennen verschillende sectoren ook nog andere meldplichten. Dit artikel is te kort om al die meldplichten uitgebreid te behandelen, maar we hebben er een paar op een rijtje gezet om een beeld te schetsen van de verscheidenheid aan meldplichten die bestaat.

In de **financiële sector** is er een meldplicht op basis van de Wet op het financieel toezicht (Wft). Voor banken geldt dat als het beveiligingsincident een ernstig gevaar vormt voor de integere bedrijfsvoering, dit gemeld moet worden aan de toezichthouder. Afhankelijk van wat voor een soort instelling het betreft moet dit bij de Nederlandsche Bank of de Autoriteit Financiële Markten gebeuren. Net als in de AVG kent deze meldplicht ook een interne registratieplicht. Deze registratieplicht komt overeen met de interne registratie die verplicht is op grond van de AVG en hoeft dus niet apart geregistreerd te worden. Let hierbij op dat zowel aan de vereisten van de Wft als aan de vereisten van de AVG wordt voldaan.
De **Telecommunicatiewet** kent twee meldplichten. Deze meldplichten gelden voor aanbieders van elektronische communicatiediensten zoals telecomproviders. De eerste is een meldplicht die vergelijkbaar is met die uit de AVG. Bij een persoonsgegevens gerelateerd beveiligingsincident moet dit gemeld worden bij de Autoriteit Persoonsgegevens, als dit incident nadelige gevolgen kan hebben voor de betrokkenen. Ook dient het incident gemeld te worden aan de betrokkenen als het voor die betrokkenen waarschijnlijk ongunstige gevolgen kan hebben. Dit laatste lijkt een lagere drempel dan in de AVG is opgenomen (er staat namelijk niet dat het moet gaan om een hoog risico), maar in de overwegingen van de Richtlijn burgerrechten worden voorbeelden genoemd die aansluiten bij een hoog risico geval uit de AVG.

Naast deze AVG-gelijkende meldplicht kent de Telecommunicatiewet nog een tweede meldplicht. Deze meldplicht voor aanbieders van elektronische communicatiediensten heeft betrekking op beveiligingsincidenten die

aanzienlijke gevolgen hebben voor het functioneren van hun netwerken of diensten. Als er sprake is van een dergelijk incident dan dienen zij dit ook te melden, deze melding vindt plaats bij het Agentschap Telecom.

Ook de Wbni kent een meldplicht. Deze wet, die haar oorsprong vindt in Europese wetgeving, is gericht op **digitale dienstverleners**. Een digitale dienstverlener dient een verstoring van de dienstverlening te melden aan de bevoegde autoriteit en het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP). Het gaat hier enkel om dienstverleners die een essentiële dienst verlenen of diensten die te kwalificeren zijn als online-marktplaats, onlinezoekmachine of Cloud computerdienst (7).

Voor partijen die opereren in de **zorgsector** zijn er ook verschillende meldplichten, zo is er een meldplicht opgenomen in de Wet kwaliteit, klachten en geschillen zorg (Wkkgz). Een zorgaanbieder moet op grond van de Wkkgz iedere calamiteit binnen de instelling melden die betrekking heeft op de kwaliteit van de zorg en die tot de dood van een cliënt of een ernstig schadelijk gevolg voor een cliënt heeft geleid. Deze melding dient te worden gedaan bij de Inspectie Gezondheidszorg en Jeugd.
Naast deze specifieke meldplichten zijn er nog vele andere, kleinere meldplichten te noemen. Vaak zijn deze meldplichten van toepassing omdat een ransomware-aanval zorgt voor het wegvallen van een dienst of omdat door het incident de dienst nadelige gevolgen kan hebben voor burgers en/of de leefomgeving. Neem bijvoorbeeld het wegvallen van communicatiediensten zoals hiervoor besproken. Andere voorbeelden zijn bijvoorbeeld het melden van een (beveiligings)incident met betrekking tot het gastransportnet waardoor nadelige gevolgen zijn ontstaan voor mens of het milieu.

Aangifte

Het plaatsen van ransomware is strafbaar. Welke delictsom-schrijving het best past, verschilt per geval, maar het zou bijvoorbeeld om computervredebreuk of opzettelijke computersabotage kunnen gaan (8). Ook afpersing is een

Veel bedrijven verwerken bijzondere persoonsgegevens. Denk bijvoorbeeld aan een concertzaal die tickets op naam zet en ook tickets voor mensen met een handicap verkoopt.

mogelijkheid (9). Naast het melden aan één of meerdere instanties is het dus ook mogelijk om aangifte te doen bij de politie.

Hoewel dit niet verplicht is, is dit wel aan te raden. In het geval de dader gepakt wordt, kan een slachtoffer zich immers voegen in de strafzaak om zo schadevergoeding te krijgen. Verder is het van belang om de verschillende ransomware-aanvallen en de hoeveelheid daarvan in kaart te kunnen brengen. Op die manier kunnen de autoriteiten hun aanpak van cybercriminaliteit verbeteren.

Hoe je wapenen tegen een ransomware-aanval?

Risico's met betrekking tot de bedrijfsvoering zijn in de praktijk niet honderd procent uit te sluiten. Wanneer je maatregelen wilt nemen tegen ransomware-aanvallen of maatregelen die de impact van een ransomware-aanval beperken, is het daarom voldoende om op zoek te gaan naar maatregelen die passend zijn, rekening houdend met de stand van de techniek.

We zien dat veel partijen worstelen met dit vraagstuk, omdat het voor hen lastig is om in te schatten wat nu 'passend' is en wat 'state-of-the-art' inhoudt. Het kan helpen om hierbij op zoek te gaan naar *best practices* die gemeengoed zijn in een bepaalde industrie en waarover consensus bestaat.

De grote hoeveelheid aan ransomware-aanvallen heeft er ook voor gezorgd dat er binnen de 'security community' meer inzicht is ontstaan over welke maatregelen het meest effectief zijn om de impact van een aanval te beperken.
Een eerste belangrijk punt betreft het creëren van awareness bij het bestuur, de leidinggevenden en het overige personeel. Juist de menselijke factor zorgt voor een zwakste schakel en door awareness training kan dit aangepakt worden.

Daarnaast is het van belang om te zorgen voor een goed updatebeleid en patchmanagement. De besturingssystemen en software dienen zo goed mogelijk bijgewerkt te zijn om te voorkomen dat zwakke plekken hierin worden uitgebuit.

Netwerksegmentatie betreft een volgend aandachtspunt dat de impact van een ransomware-aanval kan beperken. Door bepaalde gedeeltes te scheiden of los te koppelen, kan voorkomen worden dat in een keer het volledige bedrijf wordt platgelegd.

Een goede back-upstrategie is cruciaal om goed te kunnen herstellen van een succesvolle ransomware-aanval. Door te zorgen voor offline (of bijvoorbeeld 'read-only') back-ups kunnen systemen hersteld worden na een aanval. Hierbij moet er wel rekening mee worden gehouden dat

aanvallers soms langere tijd in de systemen actief zijn voordat zij 'toeslaan', waardoor er veilige back-ups beschikbaar moeten zijn waarvan met zekerheid gezegd kan worden dat deze niet alsnog succesvol gebruikt kunnen worden voor een nieuwe aanval.

Naast bovenstaande aandachtspunten kan uiteraard aan nog veel meer gedacht worden, zoals bijvoorbeeld een goede monitoring en detectie, het gebruik van anti-malware software, een goed werkend incident management proces en disaster recovery procedure en het analyseren van de leverancierskeketen op mogelijke risico's.

Maar we zijn toch verzekerd?

De toename van het aantal datalekken en cybersecurityincidenten heeft er ook voor gezorgd dat er meer aandacht is voor het afsluiten van een zogenaamde cyberverzekering. Het afsluiten van een verzekering kan ertoe leiden dat er gehandeld wordt volgens de onterechte aanname dat incidenten minder snel zullen plaatsvinden en dat indien ze plaatsvinden er toch wel een uitkering zal volgen vanuit de verzekeraar ('we zijn toch verzekerd…?').
De markt voor cyberverzekeringen is op dit moment volop in ontwikkeling. Onderwerp van debat is of bijvoorbeeld AVG-boetes en vergoedingen voor betaald losgeld, in verband met een ransomware-aanval, wel vergoed kunnen (mogen) worden door verzekeraars. Daarnaast is het van groot belang om de uitsluitingen van de verzekeringspolis te kennen. Zo is in sommige gevallen bijvoorbeeld 'social engineering' specifiek uitgesloten. Terwijl social engineering juist bij het uitvoeren van een ransomware-aanval een grote rol kan spelen (10).

Naast de discussie of het moreel wel juist is om de vergoeding van bepaalde boetes toe te staan, vindt er op het morele vlak ook discussie plaats over de vraag of er bij een ransomware-aanval überhaupt wel betaald moet worden. Er kan immers gesteld worden dat er op deze manier een crimineel businessmodel in stand wordt gehouden. Daarnaast worden verschillende organisaties (deels) gefinancierd door publiek geld. De vraag is of het moreel wel wenselijk is dat gemeenschapsgeld wordt gebruikt voor het betalen van losgeld na een ransomware-aanval.

Het laatste woord hierover is dus zeker nog niet gezegd en de discussie zal nog wel even doorgaan. Hetzelfde geldt helaas ook voor ransomware-aanvallen. Gezien het lucratieve karakter en de vele mogelijke slachtoffers zijn we daar op korte termijn nog niet vanaf. Gelukkig bestaan er genoeg mogelijkheden om je tegen deze aanvallen te verdedigen. En als het dan onverhoopt toch zover is gekomen, dan is het een kwestie van weer opstaan, de juiste meldingen doen en hopen dat de back-ups uitkomst bieden.

Referenties

(1) Hof Arnhem-Leeuwarden 4 september 2018, ECLI:NL:GHARL:2018:7967, r.o. 5.8
(2) Zie bijvoorbeeld: Rb. Amsterdam 18 januari 2017, ECLI:NL:RBAMS:2017:228; en Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124
(3) Hof Amsterdam 14 juli 2020, ECLI:NL:GHAMS:2020:2016
(4) Rb. Overijssel 9 maart 2022, ECLI:NL:RBOVE:2022:717, r.o. 5.6
(5) I.S. Feenstra, annotatie bij Rb. Amsterdam 14 november 2018, ECLI:NL:RBAMS:2018:10124, IR 2020/5
(6) Autoriteit Persoonsgegevens, Boetebesluit Booking.com, 10 december 2020, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_boete_booking.pdf
(7) Artikel 1 Wet beveiliging netwerk- en informatiesystemen, artikel 4, bijlage II en bijlage III van Richtlijn (EU) 2016/1148
(8) Artikel 138ab Wetboek van Strafrecht (computervredebreuk) en artikel 350a Wetboek van Strafrecht (opzettelijke computersabotage)
(9) Artikel 317 Wetboek van Strafrecht
(10) N.M. Brouwer, 'De cyberverzekering: over incident response, boetes en ransomware', Maandblad voor Vermogensrecht 2022/2, p. 64 – 68