Cybersecurity wordt minder vrijblijvend

Datalekken, hacks en met ransomware versleutelde bestanden die pas na betaling van losgeld worden vrijgegeven. Er komt heel wat af op bedrijven en organisaties op het gebied van cybersecurity. Het is belangrijk dat zij voldoende digitaal weerbaar zijn om dreigingen het hoofd te kunnen bieden en dat zij weten wat te doen als het toch mis gaat. Met de komst van nieuwe EU wet- en regelgeving wordt het op orde hebben van de 'cyberhygiëne' een stuk minder vrijblijvend, zo bleek tijdens het seminar 'Help we zijn gehackt, wat nu?', dat eind maart werd georganiseerd door SVDC in Zeist. Bestuurders kunnen straks zelfs tijdelijk uit hun functie worden gezet en persoonlijk aansprakelijk worden gesteld.

Hackers wisten in 2019 toegang te krijgen tot het netwerk van de gemeente Lochem. Een aantal computersystemen was niet meer toegankelijk door ransomware. De aanvallers hadden gegevens gestolen en eisten losgeld. Een deel van de dienstverlening lag plat. Zo konden er tijdelijk geen paspoorten worden aangevraagd of verhuizingen worden doorgegeven. "De criminelen bleken al maanden toegang te hebben tot het netwerk. In korte tijd moesten beslissingen worden genomen, terwijl nog onzeker was welke systemen precies geraakt waren. Konden mensen wel trouwen of uitkeringen uitbetaald worden? Op dat moment hebben we echt in de afgrond gekeken", vertelde burgemeester Sebastiaan van 't Erve aan het begin van het seminar in een videoboodschap. Er werd een uitgebreid onderzoek gestart en direct begonnen met het herstel van systemen. "Wat zou het voor de gemeente betekenen als we wekenlang niet over onze systemen konden beschikken? Wees transparant en communiceer wat er is gebeurd en welke handelingsperspectieven er zijn. Hoe groot de paniek achter de schermen ook is, je hebt maar één kans om je te positioneren. Vertel wat je weet en wat je niet weet."

Cybersecuritystrategie Het kabinet presenteerde in oktober vorig jaar de Cybersecuritystrategie 2022-2028. De verantwoordelijkheid voor digitale veiligheid wordt steeds meer verplaatst van eindgebruikers (zoals burgers en het MKB) naar de overheid en specifieke sectoren. De meest volwassen en bepalende organisaties dragen de zwaarste verantwoordelijkheden. Het Nationaal Cybersecurity Centrum, Digital Trust Center en het Cyber Security Incident Response Team for Digital Service Providers worden samengevoegd tot het nationale Cyber Security Incident Response Team. Deze nieuwe organisatie voorziet vitale en niet-vitale organisaties, overheden en burgers van informatie over (dreigende) cyberincidenten. In het digitale ecosysteem moet niet langer één organisatie of individu de zwakste schakel kunnen zijn. Het MKB en burgers worden 'ontzorgd' door verantwoordelijkheden voor de veiligheid van digitale producten en diensten grotendeels bij hen weg te nemen en neer te leggen bij de overheid, producenten en dienstverleners. Voor de overheid zullen stevige wettelijke eisen voor veiligheid en toezicht op naleving daarvan worden ingericht. Het kabinet streeft naar publiek-private samenwerking waar dat kan. Uitgangspunt voor private partijen is dat samenwerking vrijwillig is, maar zeker niet vrijblijvend.

Voorbereiding Dat cybercrime geen nieuw fenomeen is, illustreerde Eric Luiijf van Luiijf Consultancy aan de hand van een nieuwsbericht uit De Telegraaf in 1977 over chantage om gegevens uit een computer. "Begin jaren zeventig werden al bankrekeningen elektronisch geplunderd. In 1985 werd een PTT-systeem gekraakt door studenten en in 1988 lag het internet plat door de Robert Morris jr. worm. De eerste aanval met ransomware vond plaats in 1989, de eerste phishingaanval in 1995 en de eerste DDoS-aanval drie jaar later. Jaarlijks worden één op de vijf bedrijven slachtoffer van een cyberaanval. Ondanks ruim 46 jaar voorbereidingstijd en talloze waarschuwingen door de overheid en deskundigen. De nieuwe strategie betekent dat organisaties moeten werken aan zelfbescherming en kijken naar hun ecosysteem met essentiële partners, zoals leveranciers." Meerdere richtlijnen helpen bij het inrichten van cybersecurity, zoals de Baseline Informatiebeveiliging Overheid (BIO), NEN 7510-1, en -2:2017, NEN 7512:2022 en NEN 7513:2018 voor de zorgsector en ISO/IEC 27001:2022 en ISO/IEC 27002:2022 voor bedrijven. Eric Luiijf: "Werk aan een cyberweerbaar ecosysteem. Volg en acteer tijdig op beveiligingsadviezen en oefen regelmatig op het cyber incident respons plan. Voldoe aan sectorafspraken en convenanten en stel beveiligingseisen aan toeleveranciers en ingehuurde diensten."

Doorpakken Met de Cybersecuritystrategie en EU wet- en regelgeving in aantocht gaat de overheid doorpakken. Eric Luiijf: "De EU Regulation 2022/2554 Digital Operational Resilience Act (DORA) wordt momenteel 'vertaald' naar nationale wet- en regelgeving in alle EU-lidstaten. Dat moet voor 17 oktober 2024 zijn afgerond. Er gaat veel veranderen. Bedrijven en organisaties kunnen straks niet meer onder hun verantwoordelijkheid op het gebied van cybersecurity uit. Dat geldt voor zeer kritieke sectoren zoals energie, vervoer, bankwezen, financiële markt, zorg, drinkwater, digitale infra en overheid. Maar ook voor andere kritieke sectoren zoals post- en koeriersdiensten, afvalstoffenbeheer, de chemische sector, levensmiddelen en digitale aanbieders. Momenteel is nog niet duidelijk wie waar onder gaat vallen. Er zijn straks misschien wel twaalfduizend bedrijven en organisaties die als 'vitaal' zijn aangewezen. Al die organisaties dienen hun cyberhygiëne op orde te hebben met een basisniveau aan cybersecuritymaatregelen. Zij moeten risico's beheersen en aantoonbaar letten op toegepaste hard- en software. Ook moeten zij kunnen bewijzen dat bijvoorbeeld updates tijdig zijn uitgevoerd en over afdoende backups te beschikken."

Paneldiscussie met Sylvia Liem-Bruining, Eric Luiijf, Michel van Eeten en Luuk Rietveld.

Hacks moeten verplicht zo snel mogelijk worden gemeld aan onder andere klanten, opdat ook zij hun risico's kunnen bepalen. Binnen 24 uur moet een (voor)waarschuwing worden verstuurd naar het CSIRT, een bevoegde autoriteit of centraal contactpunt. Eric Luiijf: "De overheid kan straks bestuurders tijdelijk uit hun functie zetten en er kunnen boetes worden opgelegd op basis van de jaaromzet. Bestuurders kunnen persoonlijk aansprakelijk worden gesteld."

Ransomware Cyberincidenten zoals een aanval met ransomware komen altijd ongelegen. Criminelen bereiden zich goed voor en weten dat het juiste tijdstip om toe te slaan de kans op betaling van losgeld vergroot. Daarover kan ROC Mondriaan meepraten. De onderwijsinstelling in de regio Haaglanden met 26 scholen, 255 opleidingen, 19.545 studenten, 2400 medewerkers en een jaaromzet van 203,5 miljoen euro werd in augustus 2021 getroffen door een ransomeware aanval. "Op maandagochtend, een week voor de start van het nieuwe schooljaar, bleek dat we waren gehackt. De aanvallers eisten vier miljoen euro losgeld. Als eerste hebben we direct de servers en systemen op verschillende locaties uitgeschakeld. Letterlijk werden alle stekkers losgetrokken. Van volledig online gingen we naar volledig offline", blikte Sylvia Liem-Bruining, bestuursadviseur en Functionaris Gegevensbescherming bij ROC Mondriaan, terug. "Niemand had nog toegang tot applicaties. Dus geen mail, lesroosters en digitale leermiddelen. Alle hardware was niet meer te gebruiken. Medewerkers moesten hun laptops uitschakelen, omdat onduidelijk was of ook die waren gecompromitteerd. Zelfs de koffiemachines, ook gekoppeld aan het netwerk, waren niet meer beschikbaar. Het maakte voor iedereen duidelijk wat de impact van de hack was." ▸

"De overheid kan straks bestuurders tijdelijk uit hun functie zetten. Bestuurders kunnen persoonlijk aansprakelijk worden gesteld", vertelde Eric Luiijf.

Sebastiaan van 't Erve, burgemeester van Lochem: "We hebben echt in de afgrond gekeken."

“De mens is niet de zwakste, maar de laatste schakel”, stelde Michel van Eeten (TU Delft).

Sylvia Liem-Bruining (ROC Mondriaan): “Van volledig online gingen we naar volledig offline.”

Het crisis management team kwam bij elkaar en er werd een team met experts ingehuurd. Sylvia Liem-Bruining: “Het model crisismanagement plan was niet specifiek toegespitst op IT. ROC Mondriaan is ontstaan uit meerdere fusies en daarbij zijn ook verschillende netwerken samengegaan. We waren al enige tijd bezig met de transitie van eigen servers naar de cloud en er werden regelmatig pentesten uitgevoerd. Het idee was dat we alles goed op de rit hadden. Niet iedereen had een goed gevoel bij de cloud, omdat het veiliger lijkt om alle data op eigen servers op te slaan. Maar juist die eigen ‘kokosnoot’ was aangevallen. De indringers hadden een klein gaatje gevonden en eenmaal binnen hadden zij de aanval kunnen uitrollen om uiteindelijk toe te slaan.”

Belangen afwegen Volgens de bestuursadviseur is de eerste week na een aanval cruciaal. “Het nieuws lekt toch naar buiten, dus je kunt maar beter zelf openheid geven door snel en duidelijk te communiceren. Voor ons was duidelijk dat we het losgeld niet zouden betalen. Daarbij moesten verschillende belangen worden afgewogen: zorgen voor continuïteit versus het beschermen van persoonsgegevens. De aanvallers dreigden data te publiceren als betaling zou uitblijven. Maar betalen zou als publiek gefinancierde organisatie hoe dan ook moeilijk zijn geweest. Overheidsgeld is bestemd voor onderwijs, niet voor het betalen van losgeld.”
Als Functionaris Gegevensbescherming maakte Sylvia Liem-Bruining een eerste, voorlopige melding van de datadiefstal bij de Autoriteit Persoonsgegevens. “Zij hebben ons in die hectische periode niet op de huid gezeten, we ontvingen niet direct een reactie. Daarnaast moesten we alle leveranciers met wie we verwerkersovereenkomsten hebben afgesloten op de hoogte stellen.” Het expertteam concludeerde dat de servers en systemen van ROC Mondriaan van meet af aan opnieuw moesten worden opgebouwd. “Voor ons stond continuïteit op de eerste plaats en de keuze om het geëiste losgeld niet te betalen had consequenties. Het opbouwen van een nieuw netwerk heeft uiteindelijk meer gekost dan die vier miljoen euro. Of we achteraf dan toch beter hadden kunnen betalen? Kijkend als boekhouder zou je misschien zeggen van wel, maar als onderwijsinstelling niet. We wilden het verdienmodel van de criminelen niet in stand houden. Medewerkers zijn zich nu bewuster van de risico’s. Als organisatie moet je goed nadenken wie er verantwoordelijk is voor welke data en niet meer gegevens opslaan dan strikt noodzakelijk. Realiseer je voortdurend wat je kunt kwijtraken en leg niet alles vast. Meld bijvoorbeeld alleen dat een docent niet kan lesgeven, zonder uit te leggen waarom. Belangrijk is ook te realiseren dat je niet alles alleen kunt. Een aanval gebeurt vaak in het weekend of tijdens een schoolvakantie. Zorg voor een team met externe deskundigen waar je altijd op kunt terugvallen.”

Zwakste schakel Mensen kiezen ‘zwakke’ wachtwoorden die eenvoudig zijn te raden door hackers. Ook klikken ze maar al te gemakkelijk op links in phishingmails. Updates voor bekende kwetsbaarheden worden niet geïnstalleerd omdat de gebruiker dat te tijdrovend vindt. Met alle gevolgen vandien. Waarom vallen bedrijven en organisaties telkens weer ten prooi aan kwetsbaarheden? Zeker als zij toch bekend zouden moeten zijn met de risico’s? De conclusie is dan al snel dat de mens de zwakste schakel is in de beveiligingsketen. Maar is die aanname terecht? Michel van Eeten, hoogleraar Bestuurskunde/Governance Cybersecurity aan de TU Delft, vond van niet.
“Er zijn twee terugkerende oorzaken voor cyberincidenten: kwetsbaarheden waarvoor patches niet worden geïnstalleerd en menselijke fouten zoals klikken op een link of trappen in een babbeltruc. Waarom lijkt hiervoor geen oplossing te vinden? Bij verreweg de meeste hacks worden geen geavanceerde technieken of zeroday software kwetsbaarheden toegepast. Het draait meestal om bekende kwetsbaarheden waarvoor al maanden een patch beschikbaar is. Waarom patchen bedrijven en organisaties dan niet? Tussen 2017 en 2020 zijn ruim 48.000 kwetsbaarheden gepubliceerd, waarvan twaalfduizend gelden als ‘kritiek’. Het is niet haalbaar om alles te patchen. Je zou dan dagelijks tientallen patches moeten evalueren en uitrollen over je hele infrastructuur en daarvoor ontbreekt de menskracht. Slechts een heel klein percentage van de kwetsbaarheden wordt daadwerkelijk aangevallen. Dus patchen organisaties niet alles, ironisch genoeg omdat het te risicovol is om alles te patchen. Het gevolg is dat alle organisaties ongepatchte kwetsbaarheden hebben.”

Wachtwoorden Een aanval kan beginnen doordat een medewerker klikt op een link in een phishingmail. Als dat gebeurt door iemand met beheerdersrechten, maken aanvallers daar dankbaar gebruik van. Bedrijven en organisaties sturen medewerkers naar trainingen om hen bewuster te maken van cyberrisico’s. Tegen ‘domme’ gebruikers is volgens Van Eeten echter geen kruid gewassen. “De mens is niet de zwakste, maar de laatste schakel. Als de security faalt wanneer een gebruiker een fout maakt, dan heb je geen security. We geven gebruikers allerlei adviezen en vervolgens leren we ze elke dag om die adviezen te negeren. Mededelingen spreken elkaar tegen. Gebruikers krijgen te horen dat er nooit per mail wordt gevraagd naar hun wachtwoord, maar ontvangen daarna een interne evaluatie in hun mailbox waarvoor zijn moeten inloggen met hun wachtwoord. Ze krijgen zoveel verschillende adviezen dat niemand deze allemaal kan onthouden of uitvoeren. Er worden volkomen onrealistische eisen gesteld aan gebruikers. Als mensen wordt verteld dat zij beveiligingsadviezen soms moeten negeren, moet je niet verbaasd zijn als ze het ook bij andere mails gaan doen.”

Luuk Rietveld (Northwave): “Een aanval met ransomware is vergelijkbaar met een digitale hartaanval.”

Het gebruik van hoofdletters, specifieke karakters en cijfers en een minimum lengte. Iedereen kent wel de vereisten die worden gesteld aan wachtwoorden. Passwords moet dikwijls periodiek worden gewijzigd en/of kunnen alleen handmatig worden ingevoerd. Dergelijk wachtwoordbeleid verlaagt volgens Van Eeten de veiligheid. “Niemand kan dergelijke wachtwoorden onthouden. Gebruikers gaan wachtwoorden sneller hergebruiken. Als zij een wachtwoord moeten aanpassen, wordt er gewoon een uitroepteken achter geplaatst of wordt 2022 veranderd in 2023. Maar vormen de wachtwoorden wel het probleem? Het moet niet mogelijk zijn om honderd pogingen te doen om een wachtwoord in te voeren. Zorg ervoor dat in zo’n geval een account (tijdelijk) wordt geblokkeerd. Accounts worden niet overgenomen doordat hackers makkelijke wachtwoorden raden. Het beleid lokt ook veel resets van accounts uit, die weer misbruikt kunnen worden. Mensen gebruiken vaak wachtwoorden op verschillende plekken, waardoor kwetsbaarheden ontstaan. Verschuif middelen van auditing en compliance naar veerkracht en improvisatie. Investeer in effectieve mechanismen voor herstel. Blijf niet hangen in achterhaald beleid, zoals het eisen van ‘sterke’ wachtwoorden.”

Digitale hartaanval Overheid, onderwijsinstelling, ziekenhuis of winkelketen: een aanval met ransomware kan iedereen overkomen. Aanvallen zijn niet te voorspellen of voorkomen en er bestaat geen basis plan van aanpak waarin praktisch is omschreven wat bedrijven en organisaties kunnen doen als zij gehackt worden. Dat betekent niet dat er helemaal geen voorbereiding mogelijk is. Hoe gaan cybercriminelen te werk? Op welke momenten slaan zij meestal toe? Heeft het zin om met criminelen te onderhandelen over losgeld?
“Een aanval met ransomware is vergelijkbaar met een digitale hartaanval. Het businessmodel ligt volledig plat. Gegevens en bestanden zijn versleuteld. Er kan niets meer worden ingekocht; bestellingen kunnen niet worden verstuurd naar klanten”, zei Luuk Rietveld, Product Lead Cyber Resilience bij Northwave. “Cybercrime heeft overeenkomsten met fysieke inbraken. Criminelen tasten de beveiliging af. Eenmaal binnen zoeken zij de kroonjuwelen. Waar in het pand staat bijvoorbeeld de kluis? Dit patroon is ook bij aanvallen met ransomware te herkennen. In de meeste gevallen worden gelekte of zwakke wachtwoorden, phishingmails of bekende kwetsbaarheden gebruikt om binnen te komen. De aanvallers doorlopen daarna het volledige netwerk. Ze hoppen door de organisatie, zoeken naar accounts met hoge gebruikersrechten zoals een administrator. Waardevolle gegevens worden gekopieerd en daarna versleuteld. Backups worden vernietigd. Dan volgt de eis voor losgeld.”
De criminelen zijn goed georganiseerd. Groepen bestaan uit leden met verschillende specialisaties en rollen. Waar de één is gespecialiseerd in het binnendringen van netwerken of het te koop aanbieden van gestolen wachtwoorden, richt de ander zich op onderhandelen over losgeld. Luuk Rietveld: “Een nieuwe rol is de zogenaamde ‘chaser’. Deze zet druk op het slachtoffer om toch vooral te betalen, bijvoorbeeld door de directie te bellen met dreigementen.” Een goede aanpak van ransomware aanvallen omvat voorbereiden, reageren en herstellen. “Zorg voor inzicht in de kroonjuwelen van de organisatie. Wat is er voor nodig om ze in stand te houden, hoe kun je er mee omgaan als ze verstoord worden? Wie houden zich bezig met incident response en crisismanagement? Welke verantwoordelijkheden zijn er binnen en tussen teams? Wie heeft het mandaat? Spreekt iedereen dezelfde taal? Direct na een aanval komt de IT-afdeling met tal van technische termen die de directie niet veel zullen zeggen. Contact met de aanvallers wordt vaak vermeden, maar er is wel degelijk informatie uit te halen en tijd mee te winnen.”

Paneldiscussie Tijdens de afsluitende paneldiscussie werd door de sprekers en deelnemers onder meer gediscussieerd over het betalen van losgeld om weer toegang te krijgen tot gegevens. “Het is wettelijk verboden te onderhandelen met criminelen”, vertelde Michel van Eeten, die een vergelijking maakte met het terugkopen van gestolen kunst door musea. “Organisaties kunnen baat hebben bij de inzet van professionele onderhandelaren, die kunnen de-escaleren en er allicht voor kunnen zorgen dat er minder losgeld wordt geeist. Pas echter wel op voor partijen die onder één hoedje spelen met de aanvallers, gaan ‘onderhandelen’ en op ‘magische wijze’ de sleutels om data te ontgrendelen verkrijgen.” Luuk Rietveld wees erop dat er ook na betaling geen zekerheid is dat je alle data weer bruikbaar terughebt. “Het dreigement om data te publiceren als je niet betaalt is wel reëel. De criminelen zullen hun verdienmodel niet ondermijnen.” Cyberverzekeringen zijn een groeiende markt en kunnen volgens Eric Luiijf een optie zijn voor bedrijven. “De eisen waaraan moet worden voldaan om een verzekering te kunnen afsluiten worden wel steeds hoger.” De sprekers waren het er over eens dat vooraf duidelijk moet zijn welke schade wordt vergoed. Als de cyberverzekering bijvoorbeeld het inhuren van experts of mogelijk zelfs een bepaald percentage van losgeld dekt, is dat een duidelijke meerwaarde.

■ Robert van Daesdonk
Redactie@beveiliging.nl