Grant Thornton

Blauwdruk voor cyberweerbaarheid

Met sectorinformatie voor bouw, zorg en transport & logistiek

Inhoud

1. Cybercrime is big

‘Huawei luistert via KPN met Mark Rutte mee, met top secret meetings van grote bedrijven – en met wat Chinese dissidenten in Nederland.’ ‘Criminelen ontvreemden klantengegevens bij RDC en kunnen particulieren een hoop schade berokkenen.’ ‘Twee GGD-medewerkers denken slim bij te verdienen met de data van de geteste en geprikte Nederlanders. Zij bieden die online aan.’

Spionage, diefstal en fraude; online is het elke dag raak. En niet één, maar dertien keer! Kijken we naar politiegegevens, dan ging het in 2019 in totaal 4.700 keer mis. Een stijging van 65,6 procent vergeleken met 2018, zo blijkt uit onderzoek van politiedata door Dutch-Tech Magazine. In 2020 meet de Autoriteit Persoonsgegevens een toename van 30 procent van hack-meldingen, gericht op persoonsgegevens. De toezichthouder luidt de noodklok. Het jaar daarvoor was de stijging ook al 25 procent. Verontrustend dus, maar dat is bekend.

4.700

Spionage, diefstal en fraudemeldingen per dag

Tegenwoordig is alles en iedereen ‘connected’. Technologische ontwikkelingen voltrekken zich in rap tempo en bieden bedrijven volop nieuwe kansen. Tijdens de coronacrisis deed Grant Thornton een wereldwijd onderzoek naar wat bedrijven verwachten van de tijd na de crisis. Overduidelijk is dat investeren in technologie naar verwachting gaat toenemen. 36 procent van de EU-bedrijven denkt na de crisis meer gebruik te moeten maken van technologie en digitale transformatie. Ter voorbereiding op het herstel van de markten geeft 28 procent aan een strategie of implementatie te willen voor het gebruik van technologie ter ondersteuning van organisatorisch herstel. Wereldwijd komt deze optie het meest voor. In de tweede helft van 2020 wezen we in onze EU-indexopstelling ook op het feit dat 72 procent van de middelgrote bedrijven in de EU willen groeien om hun investeringen in technologie te behouden. Technologie en digitalisering blijven dus een sterk groeien. Aldus het International Business Report van Grant Thornton.

Kwaadwillenden spelen in op die sterk groeiende digitalisering en maken dat onze samenleving onder een voortdurende cyberdreiging staat. Om als onderneming succesvol te zijn en te blijven is weerbaarheid tegen cyberrisico’s zonder meer van cruciaal belang.

Preventie is niet meer genoeg. Voor goede cyberweerbaarheid werken wij bij Grant Thornton met de volgende principes:

- voorkomen is beter dan genezen;
- bereid je voor op een misser;
- balanceren tussen bescherming en nut;
- inzicht is cruciaal;
- cyberweerbaarheid vereist continuïteit.

Zo werken wij aan oplossingen, waarover wij in hoofdstuk vier meer schrijven. Maar eerst de gevaren: wat zijn de trends op dit moment? Wij behandelen er hier drie.

Operationele techniek is ontdekt als target

Nieuw is de hevigheid waarmee operationele techniek aanvallen te verduren krijgt. Aldus het Operational Security Trends Report van Fortinet. Professionele criminele teams vallen vitale infrastructuren aan, veelal met malware. Zij vinden de zwakke plekken binnen bedrijven. Zo kan bijvoorbeeld de transport-kabelbaan binnen een bloemkwekerij de hele oogst platleggen. Of kijken we landelijk: wij zijn afhankelijk van stroom- en drinkwatervoorziening. Iedere Nederlander

maakt daar gebruik van. Stel je eens voor dat criminelen een middel in ons water kunnen doen: rampzalig! Dus is het cruciaal die voorzieningen te beveiligen tegen aanvallen en schadetechnieken van specialistische hackteams. Dat is niet simpel. Operational technology (OT)-omgevingen zijn anders dan IT-omgevingen. Ze bestaan al langer, zijn moeilijker te vervangen en ze zijn complex. Waar IT en OT elkaar kruisen moet je beheer en autorisatie professioneel opzetten. Minutieus.

Aanvallen via de bedrijfsketen nemen toe

Steeds vaker hacken cybercriminelen via leveranciers en zakenpartners hun eindtargets. Heel geraffineerd – en gevaarlijk. Hackers dringen binnen bij slechts één leverancier en maken gevoelige informatie van duizenden organisaties buit. Het zijn bijvoorbeeld leveranciers of adviseurs, die toegang moeten hebben tot een bedrijfsnetwerk van hun klanten om hun werk te doen. Hackers kunnen via die toegang informatie stelen of het netwerk gijzelen om er dan losgeld voor te vragen.

Praktijk: de terminal hack

De wereldwijde hack die in 2017 ook een containerterminal in de Rotterdamse haven platlegde, is een bekend voorbeeld hiervan. Een aanval op een buitenlandse ontwikkelaar van boekhoudsoftware was stap één. Een malafide update besmette vervolgens een reeks bedrijven met kwaadaardige software. Netwerken gingen down tot er losgeld was betaald.

Targets met veel contactgegevens

Hackers kiezen leveranciers met veel contacten uit, om daar in te breken. Zijn de contactgegevens eenmaal binnen, dan kunnen zij rustig lucratieve targets uitkiezen. Zoals bij de hack op SolarWinds. De hackers hadden al lang toegang tot de systemen van deze softwareleverancier. Uiteindelijk besmetten de hackers Microsoft, het Amerikaanse ministerie van defensie – en 18.000 andere bedrijven. Bescherming van de keten is lastig. Eigenlijk zou elk bedrijf uitgebreid de cyberveiligheid van zijn leveranciers moeten testen, maar in de praktijk is dat niet haalbaar. Als bedrijven snel hacks detecteren en de hacks in de keten bekendmaken zou dat de schade – en dus het succes van deze hackers – inperken.

Veel meer thuiswerken: kwetsbaar moment

Thuiswerken neemt een vlucht. Sommige bedrijven werken al jarenlang op afstand en schalen gewoon de thuiswerkoplossingen die zij hebben op. Maar voor veel ondernemingen is het nieuw. Zij zijn er niet op voorbereid en staan voor de uitdaging snel een infrastructuur aan te leggen voor het thuiswerken. En wat altijd geldt, geldt ook nu: security staat of valt met een goede basis. Die basis is bij omschakelmomenten naar thuiswerken soms te snel en te makkelijk gelegd. Cybercriminelen profiteren hiervan. Een gevaarbewuste, defensieve houding van alle medewerkers is dus nodig.

> "Cybercriminaliteit is een wereldwijde bedreiging die iedere besluitvormer aangaat, zowel op bedrijfs- als nationaal niveau. Volgens het World Economic Forum Global Risks Report 2020, zullen cyberaanvallen in de komende 10 jaar het op één na grootste risico voor bedrijven worden."
>
> **World Economic Forum; Partnership against Cybercrime report 2020**

2. Cyberdreiging in de bouw, zorg en transport & logistiek

2.1 Bouw digitaliseren

In de bouwsector versnelt de digitalisering. Dat komt voor de bouw op het juiste moment. De sector staat voor de enorme maatschappelijke opgave om 75 duizend woningen per jaar te bouwen. En bovendien om 30 tot 50 duizend woningen te verduurzamen. Keerzijde is dat cybercrime de sector daardoor harder kan raken. Steeds vaker maken leden van Bouwend Nederland melding van computercriminaliteit. Aandacht voor cybersecurity groeit.

Dreiging bouw groter en groter

Het aantal aanvallen op industriële controlesystemen is sinds 2016 met 110 procent is toegenomen. Dat blijkt uit gegevens van IBM Managed Security Services (MSS). Zij verwachten dat de dreiging van aanvallen explosief zal toenemen de komende jaren. In Nederland meldt Bouwend Nederland dat in 2018 maar liefst 28 procent van de bedrijven in de bouw te maken had met één of meer cyberincidenten.

Drie kritieke bouwfasen

Met name in het voortraject, tijdens de fasen van aanbesteding, bij installatie en bij ingebruikname is er voor cybercriminelen interessante informatie te halen. Zelfs als een bouwbedrijf zijn eigen zaakjes goed op orde heeft, kan er in de bouwfase nog informatie weglekken via onderaannemers of zzp'ers. Maar een menselijke fout van eigen medewerkers is ook zó gemaakt. Bijvoorbeeld in de fase van ingebruikname kwamen recent de gegevens van meer dan 1.000 woningzoekenden op straat, inclusief financiële gegevens. Een medewerker van

een bouwbedrijf had per ongeluk een Excel-bestand met die gegevens meegestuurd naar alle geïnteresseerden.

Slimme gebouwen nóg slimmer beveiligen
Het wordt dan ook steeds belangrijker voor facility managers om risico's effectief te beheersen. Gebouwbeheerders zijn zich meer bewust van de invloed van digitalisering op de cyberbeveiliging van een gebouw. Met de opkomst van slimme gebouwen zijn nogal wat apparaten en systemen aangesloten op het internet. Bediening op afstand of met voice, online weersvoorspellingen naar de binnenklimaatregelaar, slimme meters worden afgelezen… handig – maar ook te kraken en daarmee direct een risico. Het zal niet de eerste keer zijn dat een organisatie het risico van IOT in het bedrijfsnetwerk onvoldoende aandacht geeft en daardoor slachtoffer wordt van een cyberincident. Security en facility managers werken dus vaker samen met hun IT-collega's en collega's van de operationele technologie (OT) om naast de fysieke ook de cyberbeveiliging te verbeteren.

Trends voor cyberbeveiliging gebouwen

- Het aantal cyberaanvallen op gebouwen zal waarschijnlijk toenemen als ze steeds meer met technologie worden uitgerust. Dus zijn er grotere risico's voor data, reputatie en mensen.
- Cybersecurity wordt voor OT een belangrijk onderdeel binnen veiligheid en beveiliging voor veel bedrijven. De digitalisering en de onderlinge verbondenheid van systemen maken bedrijven kwetsbaarder voor cyberaanvallen.
- Er zal meer vraag komen naar een nieuw soort beveiligingsprofessional, die de overlapping van OT en IT overziet.
- Een wereldwijde standaard voor cyberbeveiliging zal naar verwachting in alle bedrijfstakken een topprioriteit worden, dus ook in de bouwsector.

2.2 Cybersecurity in de zorg van cruciaal belang

In deze sector kunnen de gevolgen van cybercriminaliteit direct effect hebben op de gezondheid van zorgvragers. Een betrouwbare IT-security is dus onmisbaar. Zeker gezien de dreigingen. Artsen en medisch personeel krijgen volledige toegang tot medische gegevens en achtergrondinformatie van zorgvragers. Een must voor een snelle en juiste diagnose. De hoeveelheid informatie die de zorgsector bewaart, maakt het echter een belangrijk en winstgevend doelwit voor criminelen. We behandelen hier de cyberbedreigingen van dit moment.

Cybersecurity dreigingen voor de gezondheidszorg
Internet of Medical Things
De wereldwijde markt van Internet of Medical Things (IoMT) neemt alleen maar toe. Dus de cyberdreigingen stijgen helaas ook. In Nederland staan al bijna vier miljoen medische apparaten met elkaar in verbinding. Zij slaan de medische gegevens van de zorgvrager op. Dat is een groot beveiligingsrisico en is dus een grote verantwoordelijkheid van de zorginstanties die ze moeten beheren.

Ransomware aanvallen
Ziekenhuizen zijn een aantrekkelijk doelwit van ransomware aanvallen. De cybercriminelen besmetten de systemen en netwerken, maken zo bestanden onbereikbaar en vragen losgeld voor zij die weer vrijgeven. De aanvallen zijn steeds gerichter en beter gepland. Ook kan privacy schade substantieel zijn als de hackers binnendringen en de gegevens van zorgvragers buitmaken of gijzelen.

DDoS aanval

Gevaar is er ook voor een system overload via een DDoS aanval. DDoS staat voor Distributed Denial of Service. Eén server wordt massaal aangesproken en vertraagt of werkt zelfs helemaal niet meer. Dit kan voor zorginstellingen en ziekenhuizen op elke afdeling grote gevolgen hebben. Het kan zelfs levensbedreigend zijn voor zorgvragers.

Datalek: verlies of diefstal

Privacy schade door verlies of diefstal van informatiedragers als laptops, telefoons en USB-sticks. Het is één van de meest voorkomende cybersecurity dreigingen. Het verlies van kritische data kan grote operationele en financiële gevolgen hebben. Uiteraard kan het verlies of diefstal in de zorg leiden tot pijnlijke privacy schade, met als gevolg ernstige imagoschade voor de zorginstelling. En mogelijke persoonlijke schade voor de individuen wiens persoonsgegevens deel uitmaken van het incident.

Menselijke fouten

Ongeveer 80 procent van de fouten op het gebied van privacygevoelige informatie wordt veroorzaakt door menselijk gedrag. Terwijl veel aandacht uitgaat naar de technische kant van cyberveiligheid, is nog veel winst te boeken aan de menselijke kant. Bewustwording en gedragsverandering verhogen de cruciale cyberweerbaarheid.

2.3 Transport & logistiek: hoge dreiging cybercriminaliteit

Verschillende incidenten in de afgelopen jaren laten zien dat ook transport & logistiek sector een interessant doelwit is voor hackers. Ruim 40 procent van de bedrijven in de logistieke sector heeft al eens te maken gehad met een vorm van cybercriminaliteit. Onderzoek vertelt ons dat dit de komende jaren alleen maar toeneemt.

Haventerminals vielen stil

Wij weten nog goed hoe in 2017 twee grote containerterminals stilvielen na een wereldwijde cyberaanval met ransomware. De impact was enorm. Het duurde tien dagen voordat APM haar eerste systemen weer actief had. Het duurde nog weken voordat alle systemen weer konden draaien en schepen gelost en geladen konden worden – want dat gaat volledig geautomatiseerd. Totale schade voor Maersk: 300 miljoen dollar. Dat was het ook eerdergenoemde besefmoment. Het was de start van grote investeringen in cybersecurity in de logistieke sector. De urgentie lijkt er vier jaar later weer wat af te zijn. Alert blijven is een must. Het kan letterlijk morgen weer gebeuren.

Digitalisering is topprioriteit in supply chain

Digitalisering is voor bedrijven in de logistieke keten van groot belang. Digitale documentuitwisseling, online boekingsplatformen, automatisch orders inschieten, digitale planning en afhandeling van de transacties, tot en met het laden en lossen van schepen, vrachtwagens en logistieke centra. Dit is ondenkbaar zonder IT-ondersteuning. Technologische enablers als Kunstmatige Intelligentie, clouds, 5G en big data-analyses versterken ook in de toekomst de supply chain. Het verzamelen en delen van real time gegevens om efficiëntie en zichtbaarheid te stimuleren is essentieel voor de veerkracht en duurzaamheid in de supply chains.

Domino-effect

Digitalisering scheelt veel banen en menselijke fouten. Maar het maakt bedrijven ook extra kwetsbaar voor cybercriminaliteit. Door de complexiteit van logistieke ketens heeft een cyberincident al snel niet alleen impact op de eigen onderneming, maar op alle ketenspelers: een domino-effect. Actief risicobeheer is dan ook erg belangrijk. Bedrijven werken aan preventie, maar moeten zich ook goed voorbereiden. Hoe gaan zij reageren bij een incident? Hoe handelen zij het af? Hoe beperken zij de schade. Want de vraag is niet of, maar wanneer dat incident ook uw organisatie treft.

3. Cybercrime vormen

Hacking, ransomware, phishing, fraude; hoe zien die vormen van cybercrime er vandaag uit - in cijfers? En wat zijn de gevolgen?

Hacks

Bij hacks zien ruim zes op de tien organisaties imagoschade voor hun organisatie als het grootste gevolg van een hack. Dit blijkt uit onderzoek van Orange Cyberdefense onder 515 Nederlandse beleidsmakers in management en ICT. Het verlies van data volgt met 56,1 procent, dan het niet kunnen voldoen aan wet- en regelgeving (41,4 procent) en het verlies van de controle over de IT-infrastructuur (34,2 procent).

Ransomware

Elke 14 seconden incasseert ergens op de wereld een bedrijf een ransomware-aanval. Deze vorm van cyberafpersing was gericht op consumenten, maar volgens het Internet Security Threat Report van Symantec richt inmiddels 81 procent van de ransomware aanvallen zich op bedrijven. Migiel de Wit-Beets, partner Cyber risk services bij Grant Thornton: 'Ransomware is één van de meest voorkomende cyberaanvallen die we in ons vakgebied tegenkomen. Nieuw is simpel gezegd de geavanceerde uitvoering. Ransomware is nu vaker een opgebouwde, strategische campagne. Minder 'hit and hope'-achtig. Ze verslaan soms zelfs de grootste bedrijfsverdedigingen.'

Ransomware kan aanzienlijke gevolgen hebben voor bedrijven. In 2020 haalden hacks bij Toll Holdings en Travelex de krantenkoppen. Zij waren doelwit van een Mailto-ransomware. Door de aanval werden ongeveer 1.000 systemen gecompromitteerd, waardoor Toll offline moest. De wereldwijde dienstverlening werd verstoord. De gebeurtenis veroorzaakte ook een aanzienlijke managementoverhead. Het afhandelen van het incident en het beheren van het bedrijf zonder de kern-IT-systemen en -processen waren razend ingewikkeld en ingrijpend. Zo heeft Toll bijvoorbeeld het personeel in de contactcentra uitgebreid om de klantenservice te ondersteunen.

Phishing

De huidige phishing-aanvallen spelen in op corona en het toegenomen werkmailverkeer. De phishing-campagnes bieden mensen gezondheidsrichtlijnen, quarantaine- en infectie-updates. Dit zal de komende tijd alleen maar toenemen. Het Australian Cyber Security Centre (ACSC) meldde bijvoorbeeld een phishing scam die beweerde advies te geven over lokale COVID-19-testfaciliteiten. Cybercriminelen profiteren ook van de vele thuiswerkers. Bijvoorbeeld met aanvallen waarin zij bedrijfsrichtlijnen en -procedures, human resources-correspondentie en IT-problemen vervalsen. Deze dreiging van phishing-campagnes die officiële zakelijke communicatie nabootsen, neemt waarschijnlijk toe. De combinatie met ransomware komt veel voor. Na infectie van de systemen via phishing vragen aanvallers meestal losgeld.

Top 10 succesvolste phishing e-mails begin 2021

KnowBe4 onderzocht in het eerste kwartaal van 2021 tienduizenden onderwerpregels van e-mails uit gesimuleerde phishing-campagnes. Het bedrijf beoordeelde ook onderwerpregels van reguliere e-mails die gebruikers hebben ontvangen en aan hun IT-afdelingen hebben gemeld als verdacht.

Dit is de top 10 van onderwerpregels van succesvolle phishing e-mails uit onderzoek van KnowBe4. De phishing-mails zijn door KnowBe4 gesimuleerd.

1. **Password Check Required Immediately**
2. **Revised Vacation & Sick Time Policy**
3. **COVID-19 Remote Work Policy Update**
4. **COVID-19 Vaccine Interest Survey**
5. **Important: Dress Code Changes**
6. **Scheduled Server Maintenance — No Internet Access**
7. **De-activation of [[email]] in Process**
8. **Test of the [[company name]] Emergency Notification System**
9. **Scanned image from MX2310U[[domain]]**
10. **Recent Activity Report**

Kijken we naar alle verzonden en gerapporteerde echte phishing e-mails, dan komen deze 10 het meest voor:

1. **Microsoft 365: Scheduled Server Backup**
2. **IT: IT-Help Ticket Survey Invitation**
3. **Warning: Your E-mail account has just sent 260 E-mails**
4. **Amazon Prime: Action required – Card on file has been declined**
5. **License Update**
6. **Google: Take action to secure your compromised passwords**
7. **Apple: Prize winner! We need your confirmation**
8. **Zoom: You missed a Zoom meeting**
9. **HR: Your payroll details need updating**
10. **Facebook: Important message regarding your Facebook profile**

Fraude

De gemiddelde onderneming verliest jaarlijks 5 procent van haar inkomsten aan fraude. Het gemiddeld verlies is 108 duizend euro per geval. Dit eist een tol in geld van de onderneming, maar kan ook de cultuur en reputatie beschadigen. Het kan gaan om externe cyberfraude en datadiefstal door criminelen. Maar ook interne fraude komt veel voor; medewerkers die data, geld of bijvoorbeeld hardware ontvreemden, of corruptie plegen.

CEO-fraude nu ook bij kleinere bedrijven

Medewerkers van de financiële administratie kunnen ook in ingenieus opgezette vallen trappen: CEO-fraude. Een controller krijgt een e-mail van zijn CEO of CFO, met de opdracht een fors bedrag over te maken. De criminelen doen vooronderzoek. Zij halen gegevens van social media om overtuigende mails te kunnen schrijven. CEO-fraude begon bij grote bedrijven. De administrateur werkt dan bijvoorbeeld bij een dochteronderneming of een buitenlands filiaal van een multinational en kent de CEO niet persoonlijk. Tegenwoordig zijn ook kleinere ondernemingen, stichtingen en verenigingen slachtoffer van deze vorm van oplichting, meldt de fraude helpdesk in maart 2021.

4. Blauwdruk voor cyberweerbaarheid

Het is dus niet de vraag of, maar wanneer een bedrijf een cyberaanval te verduren krijgt. Realistisch gezien loopt elk bedrijf het risico te worden aangevallen. Hoe vergroot je cyberweerbaarheid? Dat staat of valt bij een goede basis. Alleen dan kun je veiligheid opbouwen en laag voor laag verstevigen.

Hacks

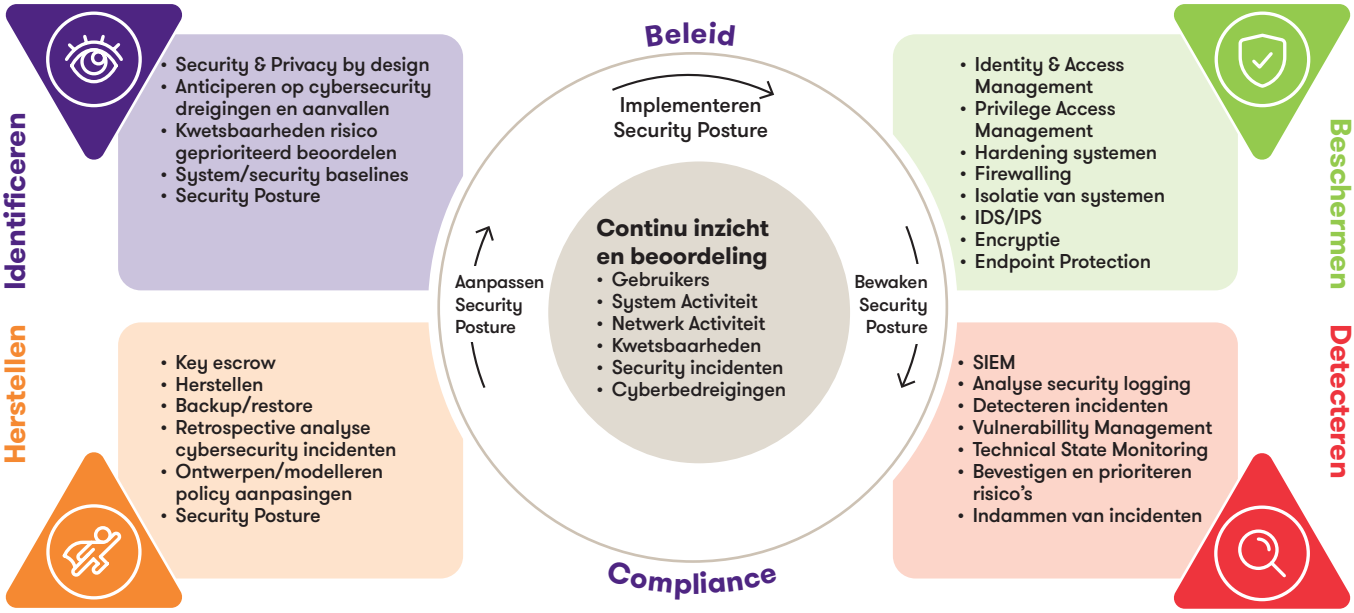
Er is géén snelle manier om een bedrijf cyberweerbaar te maken. Het vergt een grondige aanpak en raakt veel processen. Onze huidige systemen zijn nu eenmaal al gauw een samensmelting van verschillende onderdelen, zoals soft- en hardware en andere, ook externe diensten. Om houvast te houden is het daarom vanzelfsprekend dat organisaties steeds vaker openheid eisen van externe leveranciers. Dan komt de vraag: waar moet je naar vragen? Een grondig intern proces helpt organisaties hun cyberweerbaarheid in te richten op basis van factoren die zij belangrijk vinden. En zo kunnen zij ook hun leveranciers op die cruciale punten toetsen.

En ja, cyberweerbaarheid blijft aandacht vragen om het risico op cyberaanvallen zo klein mogelijk te houden. Het is nooit echt klaar, maar met een goede basisinrichting is de aandacht die het vraagt passend bij het risico. En gelukkig is er malware detectie-software die u waarschuwt bij verdachte acties, zoals onze CyberHunter. Dat scheelt IT-verantwoordelijken een hoop tijd.

Wij pakken het pragmatisch aan. Bij Grant Thornton gaan we uit van deze principes als we werken aan cyberweerbaarheid van onze klanten:

- voorkomen is beter dan genezen;
- bereid je voor op een misser;
- balanceer goed tussen bescherming en nut;
- inzicht is cruciaal;
- cyberweerbaarheid vereist continuïteit.

Goede cyberweerbaarheid vergt een goed samenspel van maatregelen op het gebied van mensen, processen en technologie. Deze maatregelen delen we op in vijf aandachtsgebieden: identificeren, beschermen, detecteren, herstellen en centraal staat: continu inzicht.



Identificeren

Met identificeren bedoelen we het inzicht verkrijgen in de gegevens die voor uw onderneming van grote waarde zijn, gecombineerd met de technologiesystemen waar die gegevens in zitten. Het kan gaan om digitale gegevens zoals klantgegevens, unieke ontwerpen, productiemethoden, recepturen, productkenmerken. Maar ook de gegevens van medewerkers, de omzet en andere financiële gegevens. Bedrijven inventariseren in deze fase ook de cyberdreigingen, zowel in de buitenwereld als in hun eigen omgeving. Detectiesoftware en scans door derden kunnen helpen bij deze stap. Met deze inzichten kunnen ondernemers beter kiezen in welke maatregelen zij zullen investeren en welke risico's zij accepteren.

Beschermen

Hierbij gaat het om de preventieve maatregelen die ondernemingen treffen om cyberincidenten te voorkomen. Dus de maatregelen waarmee zij de digitale 'kroonjuwelen' van hun onderneming beschermen. Met de waarde van die beschermde zaken, kunnen zij ook de grootte van het risico inschatten en daarmee kijken of hun beveiligingsinvestering in verhouding is. Zo stellen zij een informatiebeveiligingsplan op en tuigen hun digitale risicomanagement op. Daar hoort ook een plan bij hoe te handelen in geval van een cyberaanval: een draaiboek. Zo beperken zij deschade bij een cyberincident. Vaak gaat bescherming ook over de training van medewerkers – bijna altijd de zwakste schakel. Die moeten zich bewust zijn van de risico's; elke dag. En bedrijven die veel met privacygevoelige gegevens werken, kunnen ook nadenken over de gecombineerde functie voor cyberweerbaarheid en privacy binnen het bedrijf: één digitale risicofunctie. Of zij huren een specialist met die skills in.

Een paar aanbevelingen

Cybertraining

Traditionele benaderingen van cybertraining werken niet. Bedrijven zouden kortere, regelmatige trainingsvideo's moeten ontwikkelen en phishing-pogingen moeten simuleren om hun personeel beter op te leiden.

Specialist in huis

Bedrijven moeten hun digitale kwetsbaarheden kunnen identificeren en in kaart te brengen. Als ze medewerkers aannemen met gespecialiseerde cybervaardigheden, vormen die een aanvulling op cyberbeveiligingssoftware. Een andere optie is abonnementen op expertise inhuren – zoals CISO as a Service. Zo kunnen bedrijven hun investering in preventieve software op de juiste gebieden richten.

Cyber verzekering

Alle bedrijven gaan te maken krijgen met een cyberaanval, hoeveel ze ook investeren in preventieve software. Een algemene verzekering dekt mogelijk geen cyberaanvallen. Dus is het slim om een specifieke digitale risicoverzekering te onderzoeken. Een verzekering die zowel cyberaanvallen, als inbreuken op de privacy gevoeligedata dekt. De cyberverzekeringsmarkt is relatief jong. Bedrijven moeten de verzekeraars goed inlichten over hun specifieke kwetsbaarheden. Dan krijgt het risico een goede prijs. En zodra de verzekering is afgesloten, moeten bedrijven wel waakzaam blijven en de algemene voorwaarden naleven. Als ze bijvoorbeeld geen updates installeren, kan de verzekering vervallen. Alertheid blijft cruciaal.

Detecteren

Onder detecteren verstaan we het kunnen detecteren van kwetsbaarheden. Logging van beveiligingsrelevante gebeurtenissen, analyse en monitoring van deze gebeurtenissen spelen hierin een belangrijke rol. Goede detectiemiddelen zijn nodig om vast te stellen of de beschermingsmaatregelen goed werken. Ze zijn ook in staat om vooraf bedachte foutscenario's te signaleren. En detectiemiddelen geven inzicht in afwijkend gedrag in netwerk, systeem of applicatie. Met deze tools - zoals CyberHunter van Grant Thornton – krijgen bedrijven een veilig online dashboard voor de monitoring van hun risico's. Zij hebben daarmee altijd actueel inzicht en kunnen tijdig adequaat optreden bij een incident.

Operational Security Trends Report van Fortinet:
Security specialisten combineren met automatisering

De vraag naar managed security services groeit en automatisering van security komt op. De gewilde engineers richten zich op complexe incidenten. De eenvoudige incidenten lost het systeem dan automatisch op. Detectie met kunstmatige intelligentie (KI) wordt steeds geavanceerder. Met de eigen machine learning analyse van het netwerk brengt een KI-systeem afwijkingen en vreemd gedrag snel boven water. Vervolgens treft het automatisch de juiste maatregelen om bijvoorbeeld een lek te dichten.

Drie voordelen van CyberHunter

Continue verbetering van cyberweerbaarheid
Een veilig online dashboard voor de monitoring van uw risico's biedt altijd actueel inzicht.

Houd kwaadaardige aanvallen tegen
Actueel inzicht in kwetsbaarheden en aanvallen op het netwerk, de systemen en applicaties. CyberHunter analyseert met machine learning en kan kwaadaardige aanvallen automatisch blokkeren.

Eenvoudige implementatie van onze sensor
De CyberHunter sensor is eenvoudig te implementeren en heeft geen impact op het netwerk. Ook niet op de snelheid van het netwerk.

Herstellen

De maatregelen die de onderneming treft om te herstellen bij een cybersecurity-incident zijn belangrijk. Het draaiboek daarvoor moet klaarliggen om zo de schade snel te beperken. Naast het acute herstel is een root cause analyse nodig. Daarmee bepaal je of een structurele verbetering van beschermings- of detectiemaatregelen nodig is. Inadequaat herstel maakt de impact van cyberincidenten groter dan noodzakelijk. Belangrijk dus om het goed af te ronden.

Continu inzicht

Cyberweerbaarheid staat of valt met inzicht – continu inzicht. Dat bewaakt de effectiviteit van de cybersecuritymaatregelen van de organisatie. Bouw continu inzicht op. Bijvoorbeeld door altijd de activiteit van het netwerk, gebruikers en systemen te meten en bewaken. Maar ook hoort adequaat inzicht in de kwetsbaarheden, de cybersecurityincidenten en cyberdreigingen hierbij. Met deze inzichten kan je aanpassingen in de cybersecuritymaatregelen implementeren. Je moet altijd scherp blijven.

5. Cyber strategy and compliance van Grant Thornton

Welke cyberdreigingen zijn relevant voor mijn onderneming? Hoe voorkom ik dat er gevoelige informatie over mijn klanten op straat komt te liggen? Welke cybersecurity maatregelen moet ik nu inzetten? Welke regelgeving is eigenlijk voor mij van toepassing? Allemaal goede vragen. Onze dienst Cyber strategy and compliance zorgt voor de antwoorden.

Expertise is de sleutel

Met onze pragmatische Cyberweerbaarheidscheck weten onze klanten snel waar de knelpunten van cybersecurity binnen hun onderneming zitten. Vervolgens definiëren we samen welke maatregelen nodig zijn om de cyberweerbaarheid te vergroten. Zo helpen we organisaties bijvoorbeeld bij het opstellen van hun informatiebeveiligingsplan inclusief een plan hoe te handelen bij een cyberaanval. We kiezen daarbij altijd voor de meest pragmatische oplossing die goed bij de onderneming past. We kunnen natuurlijk ook ondersteunen bij de implementatie van de maatregelen.

Naast strategisch advies helpen we ondernemingen ook te voldoen aan de voortdurend groeiende wet- en regelgeving omtrent privacy (Algemene Verordening Gegevensbescherming) en cybersecurity. Of bijvoorbeeld bij het behalen of behouden van beveiligingscertificaten (zoals ISO27001). Ondernemers hoeven dus geen tijd meer te spenderen om te begrijpen wat alle regels en richtlijnen voor de onderneming betekenen. Wij geven werkbaar advies om aan de wet te voldoen.

- inzicht in risico's waar de onderneming aan blootgesteld is.
- na een cyberaanval is de downtime minimaal.
- zonder zorgen voldoen altijd aan de nieuwste wet-en-regelgeving
- reputatieschade beperken
- certificeringen zonder verdieping in alle regels.

Wilt u meer weten? Neem dan contact op met Migiel de Wit-Beets.

Migiel de Wit-Beets
Partner Cyber risk services
T +31 (0)88 676 91 86
E migiel.de.wit@nl.gt.com

Grant Thornton

www.gt.nl