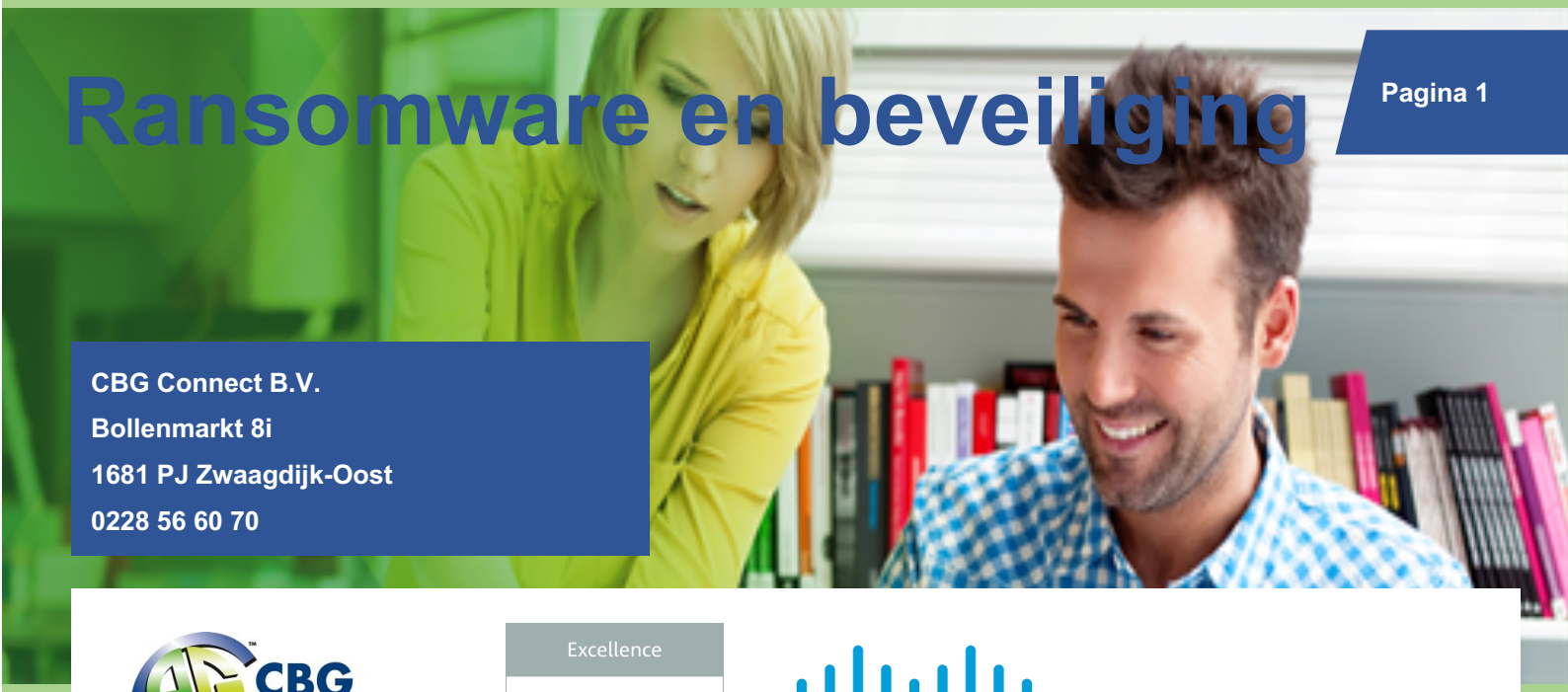
Ransomware en beveiliging



CBG Connect B.V.
Bollenmarkt 8i
1681 PJ Zwaagdijk-Oost
0228 56 60 70

CBG connect
Uw ICT Partner

Excellence
platina business partner kpn

cisco kaspersky

1. Dit is ransomware
2. Verklein het risico op besmetting
3. Hardnekkige plaag voor bedrijfsleven
4. Impact van een besmetting
5. Hoe komt infectie tot stand
6. Blik op de toekomst
7. Totaal aanpak maximale weerbaarheid
8. De menselijke factor
9. Stappenplan voor maatregelen
10. CBG Connect als securitypartner

Experts publiceren regelmatig whitepapers waarin actuele onderwerpen worden besproken.

Deze informatie wordt gemaakt om ervaring en expertise te delen en om u te inspireren en te laten zien wat er allemaal mogelijk is.

Bron: KPN

Dit is ransomware

Ransomware is een vorm van schadelijke software die data of systemen van slachtoffers gijzelt. Het woord ransomware is een samenstelling van ‘ransom’ (losgeld) en ‘malware’ (kwaadaardige software). Cybercriminelen gebruiken ransomware om mensen te chanteren via internet.

Er zijn talloze soorten ransomware. De meeste varianten versleutelen de bestanden op een apparaat, maar er zijn ook varianten die het apparaat zelf vergrendelen. Slachtoffers krijgen na besmetting instructies om losgeld te betalen. Meestal gaat het dan om losgeldbedragen in de vorm van bitcoins.

De aanvallers beloven na betaling een speciale tool beschikbaar te stellen waarmee de versleuteling ongedaan kan worden gemaakt, al zijn dat soms loze woorden. Bij veel ransomwarevarianten is zo’n tool de enige manier om weer toegang te krijgen tot versleutelde bestanden of het apparaat.

“Bescherm uw organisatie tegen ransomware en maak de weg vrij voor een weerbare organisatie”

Verklein het risico op besmetting

Twee soorten hackers

Grofweg zijn hackers onder te verdelen in twee groepen. Een deel van hen heeft uiteenlopende motieven, zoals het stelen van intellectueel eigendom, het dwarszitten van een politieke vijand of het verdrijven van de tijd (script kiddies). Er zijn echter ook hackers die puur en alleen uit zijn op financieel gewin. Voor die groep waren banking trojans voorheen het ‘weapon of choice’, maar de laatste jaren hebben criminelen hun aandacht verlegd naar ransomware.

De opkomst van ransomware is ook bij securitybedrijven en overheden niet onopgemerkt gebleven. Met initiatieven als ‘No More Ransom’ proberen zij een vuist te vormen tegen ransomware. De eerste resultaten zijn hoopgevend: in zes maanden tijd ontsleutelde de politie in samenwerking met securitybedrijven de bestanden van zo’n 75.000 slachtoffers. Toch is dit slechts een druppel op een gloeiende plaat. Zo verschijnen er continu nieuwe ransomwarevarianten, in een veel hoger tempo dan enkele jaren geleden.

“Ransomware is een van de grootste digitale bedreigingen voor het Nederlands bedrijfsleven.”

Holistische benadering

Een wondermiddel tegen ransomware bestaat niet. Alleen met een holistische benadering van security, waarbij rekening wordt gehouden met de mensen, de processen en de technologie, kunnen organisaties hun weerbaarheid verhogen. Deze totaalaanpak begint altijd met een risicoanalyse. Welke data of systemen moeten 24/7 beschikbaar zijn? Zijn onze back-ups van goede kwaliteit en testen we dit regelmatig? Hoe zit het met het patchbeleid en het securitybewustzijn van onze werknemers?

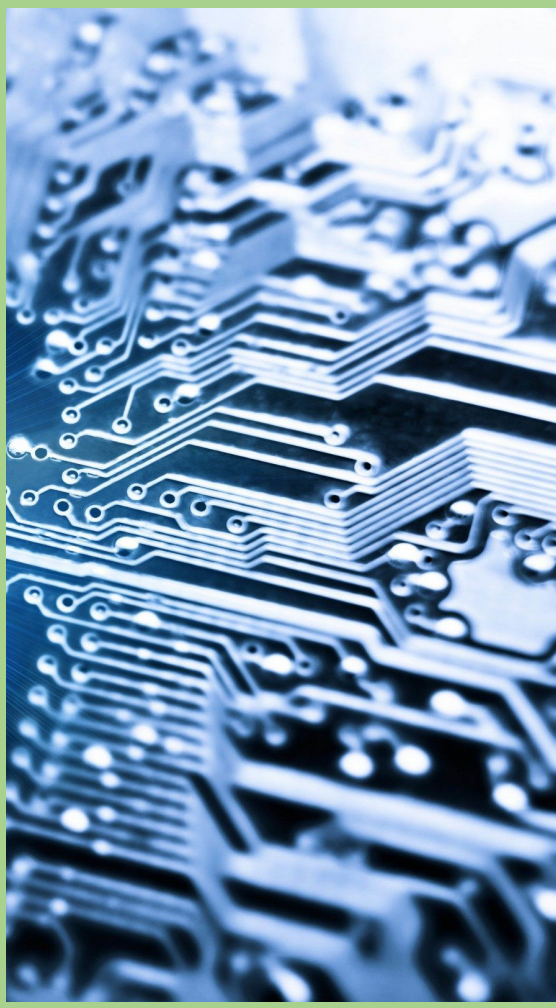
“Zowel mensen en processen als de technologie spelen een belangrijke rol.”

Er zijn talloze maatregelen die bijdragen aan een betere bescherming tegen ransomware, maar in de praktijk speelt het beschikbare budget ook een rol. Dit betekent dat business-, ICT- en securitymanagers prioriteiten moeten stellen, zowel voor de korte als de lange termijn. In deze whitepaper helpen we u bij het maken van de juiste afwegingen.

Hardnekkige plaag voor bedrijfsleven

Groeiend probleem

Alle seinen staan op rood. In juli 2016 meldde beveiligingsbedrijf Kaspersky al dat het aantal met ransomware aangevallen gebruikers met 550 procent was gestegen ten opzichte van een jaar eerder. Sindsdien heeft de wildgroei van ransomware stevig doorgezet. Zo rapporteerde cyber- securitybedrijf Check Point begin 2017 dat het aantal aanvallen wereldwijd in de tweede helft van 2016 verdubbeld is in vergelijking met een jaar daarvoor.



Ook in Nederland heeft ransomware stevig voet aan de grond gekregen. Symantec becijferde dat ons land op de vierde plaats staat op de lijst van landen met de meeste ransomware-infecties. In 5 procent van de gevallen wordt een Nederlandse computer besmet. Alleen de Verenigde Staten (31 procent), Japan en Italië (beide 8 procent) blijven Nederland voor. Een verklaring is dat Nederlanders kapitaalkrachtig genoeg zijn om veel geld te betalen voor hun bestanden. De hoge digitaliseringsgraad speelt ook een rol.

Lage kosten, hoge winsten

Het businessmodel achter ransomware is even simpel als effectief. Organisaties hebben tegenwoordig steeds meer waardevolle data in handen, bijvoorbeeld concurrentiegevoelige informatie, klantdatabases of patiëntgegevens. Data waar zij vaak bereid zijn voor te betalen en die nodig zijn voor de bedrijfscontinuïteit. Dit maakt ransomware een lucratieve business.

Uit een schatting van de FBI blijkt dat cybercriminelen in 2016 een miljard dollar aan losgeld binnenhaalden met ransomware. Succesvolle varianten als CryptoWall en Locky leveren tientallen miljoenen euro's op. Tegelijkertijd zijn de kosten voor de ontwikkeling en verspreiding van ransomware beperkt. Deze rekensom verklaart waarom dagelijks vele duizenden aanvallen plaatsvinden. Naar schatting wordt elke 40 seconden een bedrijf aangevallen met ransomware en elke 10 seconden een consument.

Geen branche is veilig

Een van de populairste doelwitten is de overheid. In Nederland zijn al diverse gemeenten getroffen. Ook het onderwijs en de gezondheidszorg hebben veel last van ransomware. Zo werden in 2016 enkele Duitse ziekenhuizen gedwongen offline te werken na een besmetting. Ze weigerden het losgeld te betalen en vielen tijdelijk terug op telefoon, fax en pen en papier.

Het is slechts een greep uit de vele incidenten in binnen- en buitenland. De realiteit is dat geen branche veilig is voor ransomware. De maakindustrie, de energiesector, de retail: elke organisatie die waardevolle data bezit of afhankelijk is van computersystemen loopt een verhoogd risico.

"Afgelopen jaren heeft ransomware zich als een olievlek verspreid over de wereld. Nederland is hierop geen uitzondering".

"In Nederland, dat vooroploopt in digitalisering, komen relatief veel besmettingen tot stand".

Impact van een besmetting

Downtime

Uit onderzoek van Intermedia blijkt dat downtime de grootste kostenpost is bij een besmetting. Ruim zeven op de tien ondervraagde bedrijven konden twee of meer dagen niet bij hun data. Voor een derde was dat zelfs vijf of meer dagen het geval. Downtime kan onder meer leiden tot gemiste inkomsten, ontevreden klanten en een lagere productiviteit van werknemers.

Gegevensverlies

Als de versleutelde bestanden niet meer kunnen worden hersteld, bent u de inhoud voorgoed kwijt. Dit is extra schadelijk als de ransomware waardevolle informatie heeft versleuteld, zoals intellectueel eigendom. Maar zelfs als de schade meevalt omdat er regelmatig goede back-ups worden gemaakt, is de kans groot dat uren of zelfs dagen werk verloren zijn gegaan.

Boetes

Als de ransomware bestanden heeft versleuteld waarin persoons-gegevens staan, geldt dit volgens de Autoriteit Persoonsgegevens als een datalek. Het niet melden van een datalek kan u op een forse boete komen te staan. Door de Algemene Verordening Gegevensbescherming, die vanaf 25 mei 2018 de Wet bescherming persoonsgegevens vervangt, stijgen de boetes flink.

Reputatieschade

Wanneer een besmetting met ransomware of datalek in het nieuws komt, is reputatieschade niet uitgesloten. Ook downtime en de daarmee gepaard gaande problemen, zoals (online) diensten die langere tijd niet beschikbaar zijn, kunnen voor een flinke deuk in de reputatie zorgen.

Losgeld

Bijna bij alle varianten wordt er bij de gebruiker om losgeld gevraagd. Dit gebeurt meestal in bitcoins, die cyber- criminelen anoniem kunnen innen. Wij adviseren organisaties het losgeld nooit te betalen. Daarmee houden zij het systeem in stand en er is geen garantie dat de cybercriminelen doen wat ze beloven. Bovendien komen betalende slachtoffers op een lijst terecht met doelwitten die af te persen zijn.

Hoe komt infectie tot stand

Er zijn uitzonderingen, maar de meeste ransomware maakt gebruik van Phishing of Exploit kits om een systeem te besmetten. Veel moderne ransomwarevarianten versleutelen tientallen typen bestanden van het slachtoffer, zowel op het device zelf, alsook op externe harde schijven en netwerklocaties. Een relatief nieuwe trend is dat steeds vaker ook back-ups versleuteld worden.

Phishing

Met behulp van social engineering (het misleiden van mensen) worden doelwitten – dat kunnen ook uw medewerkers zijn – verleid om een bijlage te openen of op een link te klikken van een schadelijke website. Meer dan 90 procent van de phishingmails bevat een vorm van ransomware. Malafide links en bestanden worden ook via bijvoorbeeld social media en berichtenapps verspreid. Er is nu zelfs een variant die slachtoffers de optie geeft om het losgeld te betalen door twee contacten te besmetten.

Exploit kits

Dit is code die systemen afspeurt op kwetsbaarheden in software en ze vervolgens gebruikt om malware te installeren. Zodra gebruikers een besmette website bezoeken of een website met kwaadaardige reclame (malvertising) bekijken, worden ze op de achtergrond doorgestuurd naar de website van de aanvaller waar de exploit kit wordt gehost. Exploit kits vinden meestal wel een ingang als de software op een apparaat niet regelmatig wordt bijgewerkt.

“Phishing en Exploit kits worden het meest gebruikt bij ransomware.”

“Nieuwe trend is dat steeds vaker ook back-ups versleuteld worden.”

Blik op de toekomst

Windows en Android worden al jaren geplaagd door ransomware. Dit is deels te verklaren door het feit dat deze besturingssystemen veruit het grootste marktaandeel hebben, respectievelijk op desktop/laptop en op mobiele apparaten. Hoe meer doelwitten er zijn, hoe groter de potentiële opbrengst. Met name bij Android speelt ook de gebrekkige beveiliging een rol. Zelfs smart-TV's die op Android draaien, kunnen gekaapt worden.

Langzaam maar zeker zien we echter een verschuiving naar andere besturingssystemen. Zo werd in november 2015 de allereerste ransomwarevariant voor Linux ontdekt (Linux.Encoder.1). In maart 2016 maakten onderzoekers bekend dat ze voor het eerst ransomware voor OS X 'in het wild' hadden gespot (KeRanger). Op iOS bleef de dreiging van ransomware vooralsnog beperkt tot een variant die de browser Safari gijzelde.

In theorie is elk apparaat met een internetverbinding kwetsbaar voor malware. De verwachting is dat ontwikkelaars van ransomware zich steeds vaker op IoT-devices zullen richten: van sensoren en machines in fabrieken tot zelfrijdende auto's, slimme huizen en medische apparatuur als pacemakers. Deze apparaten zijn veelal slecht beveiligd en dus eenvoudig te besmetten.

De toekomst

Op het eerste oog is er weinig reden om optimistisch te zijn. Een sentiment dat wordt gedeeld door het Rathenau Instituut. Het onderzoeksinstituut waarschuwde in een rapport dat de Nederlandse overheid en het bedrijfsleven onvoldoende beschermd zijn tegen cyberdreigingen. De onderzoekers schrijven onder meer 'dat het lijkt alsof de top van ransomware nog niet bereikt is en het aantal manifestaties de komende jaren zal toenemen'.

Volgens McAfee verplaatst het strijdtoneel zich naar mobiele apparaten. Omdat deze regelmatig worden geback-upt in de cloud, is mobile ransomware in de basis minder effectief. Clouddata zijn niet onkwetsbaar, maar met een opslagdienst als Dropbox kunt u bestanden herstellen naar een eerdere versie die nog niet besmet is. Daar zitten wel haken en ogen aan, zoals een limiet van 30 dagen voor het terugzetten van vorige bestandsversies.

Ransomware op mobiele apparaten kan evengoed heel vervelend zijn, bijvoorbeeld als het toestel vergrendeld wordt. De kans is bovendien groot dat cybercriminelen nieuwe trucjes bedenken om misbruik te maken van het feit dat vrijwel iedereen een (zakelijke) smartphone of tablet gebruikt.

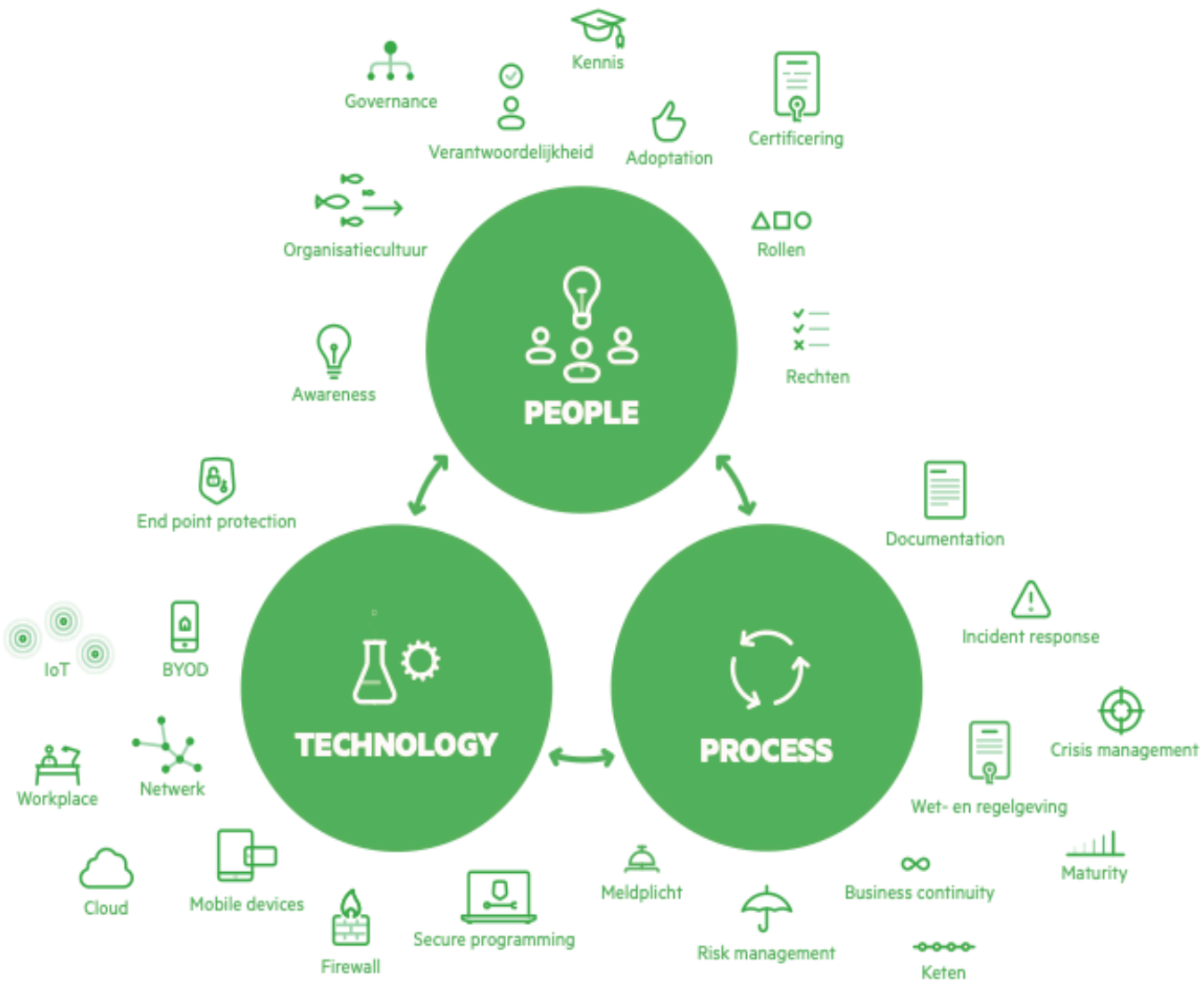
"Het strijdtoneel van ransomware verplaatst zich naar mobiele apparaten, maar is daar in de basis minder effectief door de back-ups in de Cloud."

Totaal aanpak maximale weerbaarheid

Er is geen eenduidige oplossing voor ransomware. Het tackelen van deze problematiek begint bij het besef dat technische maatregelen alleen niet genoeg zijn. Een integrale aanpak van security over de 3 assen mensen, processen en technologie en de samenhang van deze 3 assen, bepaalt het succes van de bescherming van uw organisatie.

Veel organisaties worstelen ermee om een effectieve verdedigingsstrategie tegen ransomware te bepalen die bescherming bieden tegen ransomware. Als er al een strategie is, dan is het maar de vraag of die oplossingen u afdoende beschermen tegen de nieuwste ransomwarevarianten. Traditionele beveiligingssoftware vergelijkt malware met een database met bekende varianten, op basis van de unieke 'handtekening' van de malware. Geavanceerde ransomware is echter polymorf, wat betekent dat deze constant van uiterlijk verandert. Dit soort malware laat zich niet detecteren door zo'n 'signature-based' oplossing.

Om polymorfe ransomware aan te pakken, is een oplossing nodig die het 'gedrag' van de malware analyseert met behulp van sandboxingtechnologie (het uitvoeren en analyseren van verdachte code in een afgeschermde virtuele ruimte, zodat deze geen schade kan aanrichten). Het veranderen van uiterlijk heeft dan dus geen enkel effect.



De menselijke factor

Technische maatregelen zijn bovendien slechts één onderdeel van een goede verdediging tegen ransomware. Minstens zo belangrijk is het verhogen van het security bewustzijn van uw werknemers. De mens is vaak de zwakste schakel in de beveiliging. Zelfs als technisch alles dichtgetimmerd is, blijft die menselijke factor onvoorspelbaar.

Elke organisatie heeft mensen in dienst die minder securityminded zijn. Wanneer een van deze werknemers bijvoorbeeld in een phishingaanval trapt of een besmette USB-stick gebruikt, haalt hij of zij toch agressieve ransomware binnen. Awarenesstrainingen helpen bij het tackelen van deze problematiek, maar zelfs een goed getrainde medewerker kan de fout ingaan. Er is maar één moment van onoplettendheid nodig en besmetting is een feit.

Bovenstaand scenario illustreert dat een succesvolle aanpak van ransomware rekening houdt met de mensen, de processen en de technologie. Dit inzicht helpt u om de juiste defensieve maatregelen te selecteren.

Voorspellende Maatregelen

Het actief inwinnen van betrouwbare informatie over nieuwe ransomware-varianten, aanvalsmethoden en kwetsbaarheden.

Preventieve Maatregelen

Het regelmatig maken van (externe) back-ups van data, databases en systemen, netwerksegmentatie, een streng patchbeleid en het maken van een incident-responsplan. Maar ook een zorgvuldig beheer van gebruikersrechten, het verhogen en periodiek testen van het securitybewustzijn van werknemers, het testen van back-ups, het optimaliseren van restoretijden en het oefenen van de uitwijkprocedure.

Detectie Maatregelen

Inzetten van securitygateways om malware in uw e-mail en internetverkeer te detecteren en werknemers te ondersteunen die niet in staat zijn om malafide e-mails van echte te onderscheiden, een next-gen firewall met Threat Extraction-functionaliteit voor het scannen van documenten op bedreigingen, Enterprise Mobility Management en Mobile Threat Defense voor respectievelijk het beheer en de beveiliging van mobiele devices en Security Information and Event Monitoring (SIEM) voor netwerkmonitoring.

Respons Maatregelen

Het volgen van de stappen in het incident-responsplan, het isoleren van besmette systemen om grootschalige verspreiding te voorkomen, het inschakelen van forensische hulp om de schade te beperken.

De bescherming tegen ransomware wordt verder bemoeilijkt doordat werknemers steeds vaker hun eigen (mobiele) apparaten gebruiken voor zakelijke doeleinden. Als een apparaat van een medewerker thuis en dus buiten het zicht van de IT-afdeling geïnfecteerd raakt, bijvoorbeeld door het downloaden van een geïnfecteerd bestand, neemt hij of zij de ransomware vervolgens mee naar kantoor.

Een besmetting hoeft geen gigantisch probleem te zijn als er goede back-ups zijn gemaakt. Het testen van back-ups is een belangrijk proces. De kwaliteit van de back-ups en de snelheid van het herstel moeten regelmatig worden getest, anders kan tijdens een aanval blijken dat de back-upfunctionaliteit niet goed werkt. Resultaat: de herstelprocedure duurt veel langer of bestanden zijn verloren. En als er geen incident-responsplan klaarligt, ontbreekt een heldere taakverdeling. Dit levert nog meer vertraging op.

Herstel Maatregelen

Het terugplaatsen van back-ups en het verhuizen naar een uitwijklocatie waar werkzaamheden na een incident snel kunnen worden hervat. Slechts een handvol organisaties heeft de financiële slagkracht om álle maatregelen te nemen. Er moeten dus keuzes gemaakt worden.

Stappenplan voor maatregelen

1. Bepaal wat uw belangrijkste digitale assets zijn
Elke organisatie heeft systemen of data die net even belangrijker zijn dan de rest, bijvoorbeeld omdat ze cruciaal zijn voor de bedrijfsvoering of persoonsgegevens bevatten. Voor een ziekenhuis kunnen dat patiëntgegevens en met internet verbonden medische apparatuur zijn. Een school of universiteit wil voorkomen dat informatie over de leerlingen en studenten verloren gaat.

2. Breng de grootste risico's in kaart
Vervolgens bepaalt u hoe het met de beveiliging van deze 'kroonjuwelen' gesteld is. Welke maatregelen zijn er al genomen om ze te beschermen tegen ransomware? Hoe effectief zijn ze? Welke werknemers hebben toegang tot deze data en systemen? Kan een besmetting zich snel over uw netwerk verspreiden?

3. Stel de investeringsbereidheid vast
Elke maatregel kost geld. Voordat u verantwoorde keuzes kunt maken over de te nemen maatregelen zult u eerst te weten moeten komen hoeveel budget er beschikbaar is.

4. Kies de maatregelen met de hoogste prioriteit
Op basis van uw risicoanalyse en het budget kiest u een aantal maatregelen die eigenlijk geen seconde langer kunnen wachten. De 'basics', zoals goede back-ups met minimale restoretijden, een firewall, een web- en e-mailgateway en antimalware, moeten in ieder geval op orde zijn. Welke maatregelen daarna de hoogste prioriteit hebben, verschilt per organisatie.

Zijn uw werknemers bovengemiddeld vatbaar voor phishingaanvallen? Wellicht is het dan verstandig om te investeren in awarenesstrainingen. Worden binnen uw organisatie veel mobiele apparaten gebruikt? Dan zijn oplossingen voor het beheer en de beveiliging van mobiele devices een logische keuze.

5. Stippel het verdere groeipad uit
Cybersecurity is geen eenmalige oefening. Ransomware ontwikkelt zich continu en uw beveiliging moet daar gelijke tred mee houden. Het loont dus om een groeipad uit te stippelen. Waar wilt u over een jaar staan? Welke maatregelen zijn misschien niet direct cruciaal, maar zou u op de lange termijn wel graag willen treffen

6. Implementeren, testen en optimaliseren
U heeft nu een goed beeld van uw huidige situatie en kunt weloverwogen keuzes maken over de te nemen technische en organisatorische maatregelen. Na de implementatie mag u niet op uw lauweren rusten. Misschien nog wel belangrijker is het testen, evalueren en optimaliseren van de maatregelen. Ook dit is een doorlopend proces.

CBG Connect als securitypartner

Beveiliging is nooit waterdicht. Enig realisme is dus gepast. Een besmetting met ransomware is nooit volledig uitgesloten. Een waterdichte beveiliging moet ook niet het streven zijn. Het gaat erom dat uw organisatie het risico op infectie verkleint en zo goed mogelijk voorbereid is als het onverhoopt toch misgaat. Zo beperkt u de impact en bent u snel weer operationeel.

Cisco Meraki Security

De Meraki Securityoplossing bestaat uit een hardwarecomponent met daarbij een licentie waardoor u toegang krijgt tot alle mogelijke beveiligingsopties van Cisco Meraki Security. De Meraki Securityoplossing wordt beheerd via een Cloudportaal. Via deze omgeving kunnen alle instellingen aangepast worden.

De Cloudportaal is uitgebreid ingericht om de beveiliging van het netwerk op diverse fronten in te stellen. Tevens is de Cloudportal uitgerust met verschillende diagnostische functies die een overzicht geven van alle informatie omtrent het netwerk. Uniek is ook het feit dat mogelijke malware gebeurtenissen onderzocht worden door de rechercheurs van het Talos Team. Mocht er toch sprake zijn van gedownloade malware dan komt hiervan een melding in de Cloudportal en wordt het systeem ook meteen geupdate en dus intelligenter gemaakt. Zo worden toekomstige downloads van de bewuste malware tegen gehouden.

Kaspersky

Al ruim 20 jaar is Kaspersky de erkende expert in de strijd tegen malware en cybercriminaliteit. In 2018 eindigde de producten van Kaspersky in 88 onafhankelijke test, waarin zij beoordeeld werden maar liefst 73 keer op de eerste plaats. Kaspersky biedt voor diverse producten en oplossingen voor Small, Medium en Enterprise organisatie.

Wilt u meer informatie ontvangen over Cisco Meraki Security en/of Kaspersky? Neem dan contact op met een van onze accountmanagers, zij helpen u graag.

CBG Connect verbindt zich alleen aan organisaties die A-Kwaliteit producten en diensten leveren.

CBG Connect is:

- KPN Excellence Business Partner
- Partner Cisco
- Microsoft Partner

CBG Connect levert o.a.

- Connectiviteit KPN ÉÉN
- VoIP KPN ÉÉN
- Mobiel KPN ÉÉN
- Microsoft 365
- Cisco Meraki Securityoplossingen
- CBG Connect servicediensten Connect Secure
- Netwerkbeheer
- Overige IT-ondersteuning

Bron: Voor het samenstellen van deze informatie hebben wij gebruik gemaakt van de informatie van KPN omtrent Ransomware.

De 4 pijlers van CBG Connect:

1. **Toegankelijkheid**
2. **Vertrouwen**
3. **Innovatie**
4. **Groeien**

CBG connect
Uw ICT Partner

CBG Connect
Bollenmarkt 81
1681 PJ Zwaagdijk-Oost
www.cbgconnect.nl
Algemeen telefoonnummer 0228 56 60 70
Team Verkoop: optie 2
Directie:
Johan Schotanus en Manuel Jamin