Ransomware-ready?
Een e-book over ransomware

Een e-book voor zakelijk Nederland

kpn. Het netwerk van Nederland

Inleiding

Ransomware is uitgegroeid tot de grootste bedreiging voor het bedrijfsleven. Steeds meer organisaties zijn zich bewust van de risico's. Maar hoe vertaalt u dat bewustzijn naar een betere beveiliging? Welke maatregelen hebben prioriteit?

Een effectieve verdediging tegen ransomware bestaat uit een combinatie van technische en organisatorische maatregelen. In dit e-book vertellen we u hoe zo'n verdediging eruit kan zien. Dat doen we aan de hand van drie fictieve bedrijven:

Slagerij Hoek
is een kleine slagerszaak in een populaire volksbuurt. Met drie fulltimers en een handjevol parttimers verkoopt Slagerij Hoek zes dagen per week de beste vleesspecialiteiten. De slager maakt slechts beperkt gebruik van IT-voorzieningen, bijvoorbeeld voor het kassa- en voorraadsysteem en de financiële administratie.

Hogerop Trainingen
is een middelgrote zakelijke dienstverlener. Hogerop Trainingen verzorgt een breed scala aan opleidingen en trainingen. Het bedrijf heeft een eigen online trainingsportaal en doet veel aan online marketing. De ruim honderd medewerkers werken de helft van de tijd thuis. Hogerop Trainingen is dus sterk afhankelijk van IT.

Ultimate Home Store
behoort tot de grootste retailers van Europa. Het assortiment bestaat uit interieurproducten en elektronica van A-merken die het bedrijf tegen lage prijzen aanbiedt. In Nederland heeft Ultimate Home Store acht filialen. IT loopt als een rode draad door de hele bedrijfsvoering: van HR en logistiek tot marketing en klantenservice.

Deze drie bedrijven vertegenwoordigen verschillende lagen van het Nederlandse bedrijfsleven. Elk met een andere focus én een ander budget voor cybersecurity. Welke maatregelen treffen deze bedrijven? En hoe pakken deze keuzes uit in de praktijk? Daarbij onderscheiden we drie concrete fases: voor, tijdens en na een ransomware-aanval.

Na het lezen van dit e-book weet u hoe een solide beveiliging tegen ransomware eruitziet.

‘Ransomware is een lucratieve business met veel slachtoffers’

Inhoud

Ransomware grijpt om zich heen

Ransomware kost de Nederlandse samenleving jaarlijks vele miljoenen euro's. In dit hoofdstuk schetsen we de aard en omvang van dit probleem.

Gijzelsoftware vindt zijn oorsprong in de jaren 80. De eerste ransomware-aanvallen waren technisch niet verfijnd en vonden slechts sporadisch plaats. Pas in het nieuwe millennium kreeg ransomware echt voet aan de grond. Dit hangt samen met de komst van cryptovaluta zoals de bitcoin. Cybercriminelen kregen hiermee een niet-traceerbare methode om het losgeld te innen. Zo ontstond de moderne ransomware-aanval, waarbij malware bestanden versleutelt en de aanvallers vervolgens een bedrag in cryptovaluta eisen. Inmiddels is ransomware uitgegroeid tot een professionele miljardenindustrie, gerund door criminele groeperingen. En daar horen professionele verdienmodellen bij zoals ransomware-as-a-service (RaaS). Hierbij voeren de ontwikkelaars van de ransomware zelf geen aanvallen uit, maar laten ze dit over aan partners die een deel van de opbrengst krijgen. Zo verkleinen de ontwikkelaars het risico om zelf gepakt te worden. Het is een lucratieve business waar iedereen van profiteert.

Impact van een aanval

Een lucratieve business met veel slachtoffers. Volgens beveiligingsbedrijf Sophos werd in 2021 twee derde van de bedrijven wereldwijd aangevallen met ransomware. De geëiste losgeldbedragen variëren van een paar duizend euro tot vele miljoenen. Maar het losgeld is slechts een fractie van de totale kosten. Vaak gaat er werk verloren. Ook kan het weken duren voordat een bedrijf weer volledig operationeel is. Dat leidt tot productiviteitsverlies, misgelopen inkomsten en reputatieschade.

Het betalen van losgeld biedt overigens geen enkele garantie dat u weer toegang krijgt tot de gegijzelde gegevens. Niet voor niets adviseert de politie om nooit te betalen, ook omdat u daarmee de kas van de aanvallers spekt. De afweging tussen wel en niet betalen is echter vaak lastig te maken. Bovendien gijzelen veel moderne ransomwarevarianten de data niet alleen, maar dreigen ze deze ook openbaar te maken als het losgeld niet wordt betaald. Dit wordt double extortion (dubbele afpersing) genoemd.

Plaag voor het bedrijfsleven

Alle seinen staan op rood. Volgens de Nationaal Coördinator Terrorismebestrijding & Veiligheid (NCTV) brengt ransomware zelfs de nationale veiligheid in gevaar. In het Cybersecuritybeeld Nederland waarschuwt de instantie onder andere voor ransomware-aanvallen op de vitale infrastructuur. Ook wordt RaaS een plaag voor het mkb genoemd. Door een doorgaans lage tot beperkte weerbaarheid is het mkb voor ransomware-aanvallers een makkelijke prooi.

De ernst van de situatie blijkt ook uit de vele ransomware-incidenten in Nederland die de afgelopen jaren het nieuws haalden. Van de gemeente Hof van Twente en Universiteit Maastricht tot het ROC Mondriaan, RTL Nieuws en de 'kaas-hack' bij logistiek bedrijf Bakker: geen sector lijkt veilig en de schade is vaak enorm. Bovendien is dit nog maar het topje van de ijsberg. Veel getroffen bedrijven zijn niet transparant over een aanval, bijvoorbeeld omdat ze vrezen voor imagoschade. Toch is er reden voor optimisme. Bedrijven zijn niet weerloos tegen ransomware. Er zijn allerlei manieren om enerzijds ransomware-aanvallen af te slaan en anderzijds de impact van een incident te beperken. Maar hoe ziet een effectieve beveiliging er dan uit? Daarvoor moeten we eerst begrijpen hoe een ransomware-aanval werkt.

Zo werkt een ransomware-aanval

Een ransomware-aanval bestaat uit verschillende fasen. Daarin werkt de cybercrimineel toe naar zijn doel: het binnenhalen van het losgeld. In dit hoofdstuk kruipen we in de huid van de cybercrimineel.

Er zijn diverse modellen die de opzet van een cyberaanval beschrijven. We lichten er twee uit: de Cyber Kill Chain en een nieuw model van het Computer Emergency Response Team (CERT) van Nieuw-Zeeland.

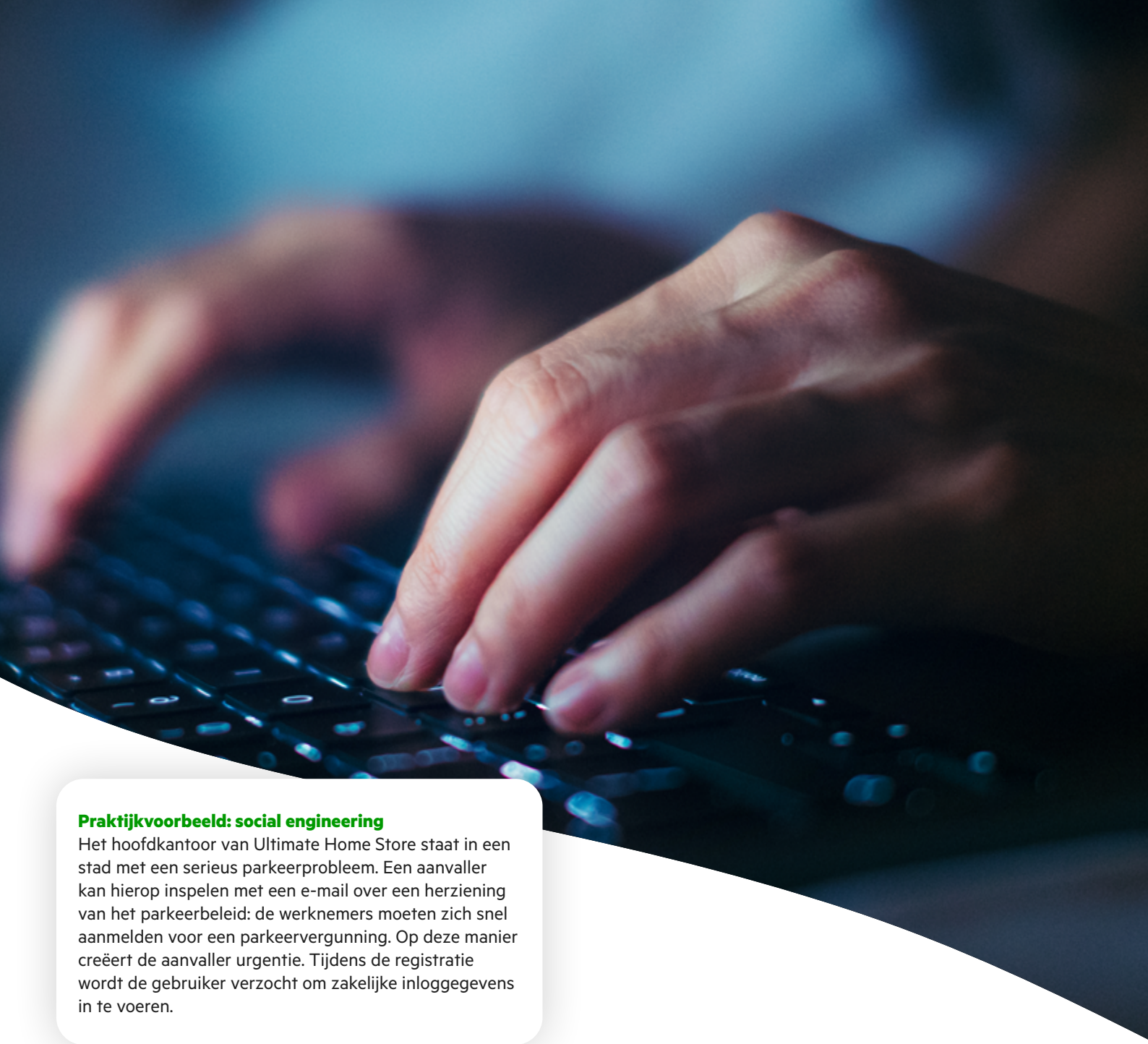
Cyber Kill Chain

De Cyber Kill Chain helpt bedrijven te begrijpen hoe een cyberaanval verloopt en reikt voor elke fase beschermende maatregelen aan. Dit model onderscheidt zeven fases:

Verkenning
Bij een gerichte aanval probeert de aanvaller zoveel mogelijk informatie over het bedrijf te verzamelen om een zwakke plek in de beveiliging te vinden. Wie werken er? Wat is hun functie? Met wie hebben ze contact? Welke systemen zijn in gebruik en hoe zijn die beveiligd? Ook wordt op het darkweb gezocht naar bruikbare informatie zoals inloggegevens.

Bewapening
Daarna breekt de bewapeningsfase aan. Daarbij kiest de aanvaller het juiste aanvalswapen. Dat kan bijvoorbeeld geavanceerde malware zijn die binnenkomt via een kwetsbaarheid in niet-geüpdatete software en de virusscanner omzeilt. Of een phishingmail met als doel het stelen van inloggegevens.

Aflevering
In deze fase probeert de aanvaller het wapen af te leveren. Daarvoor zijn verschillende methoden, zoals een e-mail met een besmette bijlage of een link naar een website die de malware downloadt. Vaak wordt gebruikmaakt van een emotionele trigger waar werknemers gevoelig voor zijn (social engineering).



Praktijkvoorbeeld: social engineering
Het hoofdkantoor van Ultimate Home Store staat in een stad met een serieus parkeerprobleem. Een aanvaller kan hierop inspelen met een e-mail over een herziening van het parkeerbeleid: de werknemers moeten zich snel aanmelden voor een parkeervergunning. Op deze manier creëert de aanvaller urgentie. Tijdens de registratie wordt de gebruiker verzocht om zakelijke inloggegevens in te voeren.

Exploitatie
De schadelijke code wordt uitgevoerd, vaak door een gebruiker. Een medewerker opent bijvoorbeeld de malafide bijlage en downloadt de malware.

Installatie
Meteen daarna kan de aanvaller de malware installeren op het systeem, of speciale software die detectie door securityoplossingen voorkomt.

Controle
Het geïnfecteerde systeem maakt verbinding met een command & control (C&C)-server en wacht op nieuwe instructies. Op deze manier krijgt de aanvaller controle over systemen binnen de organisatie. In deze fase vindt ook een verdere verkenning van het netwerk plaats. Doel is om toegang tot zoveel mogelijk apparaten en systemen te krijgen.

Versleuteling
Nu kan de cybercrimineel zijn doelstelling realiseren: het slachtoffer onder druk zetten om losgeld te betalen. Na het versleutelen en stelen van bedrijfsgegevens en het activeren van de ransomware ontvangt het slachtoffer de betalingsinstructies.

De Cyber Kill Chain heeft niet specifiek betrekking op ransomware-aanvallen. Daarom belichten we hier ook een model van het CERT van Nieuw-Zeeland. Dit model legt op eenvoudige wijze uit hoe een ransomware-aanval werkt.

Fase 1: initiële toegang

De aanvallers zoeken een manier om toegang te krijgen tot het netwerk. De meest gangbare methoden zijn:

- Het verkrijgen van gebruikersnamen en wachtwoorden om in te loggen op computers.
- Het uitbuiten van kwetsbaarheden in systemen die via internet te benaderen zijn.
- Het versturen van malware via malafide e-mailbijlages.

Fase 2: consolidatie en voorbereiding

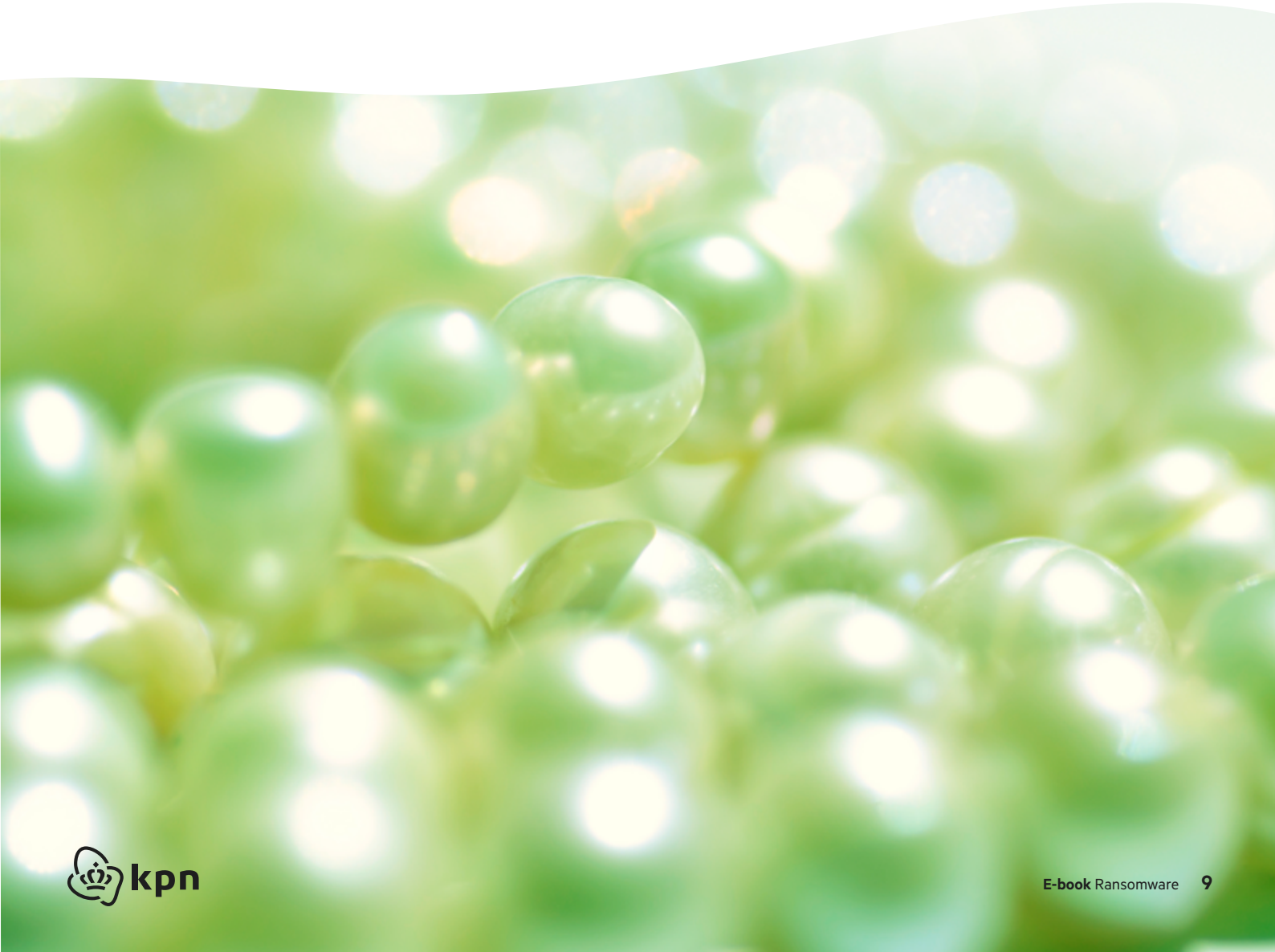
Vanuit het gecompromitteerde systeem probeert de aanvaller met beheerdersrechten toegang te krijgen tot alle computers en apparaten binnen het bedrijf.

Fase 3: impact op doelwit

De aanvallers versleutelen en/of stelen de data om zo de bedrijfsvoering te ontregelen. Ook verwijderen ze back-ups, wat het herstel bemoeilijkt. Vervolgens eisen ze losgeld.

Gerichte aanvallen versus 'hagelschieten'

Het is belangrijk te beseffen dat de meeste ransomware-aanvallen niet gericht zijn op een specifiek doelwit. Veel cybercriminelen schieten met hagel, bijvoorbeeld via grootschalige phishingcampagnes of geautomatiseerde pogingen om wachtwoorden te kraken (bruteforce-aanvallen). Met name mkb-partijen worden veelal op deze manier aangevallen.



Grote bedrijven hebben doorgaans meer budget voor securitymaatregelen, en een betere beveiliging. Cybercriminelen moeten dus meer moeite doen om binnen te komen. Bij zo'n gerichte aanval wordt elke fase van de Cyber Kill Chain zorgvuldig afgestemd op het doelwit. Ook wordt de keten vaak meerdere keren doorlopen. De aanvaller komt steeds een stukje dichter bij de waardevolle gegevens en systemen (de 'kroonjuwelen').

Voor cybercriminelen is dit een zakelijke afweging. Bij een interessant doelwit zijn ze bereid om meer tijd en middelen in een aanval te steken. Een groot, kapitaalkrachtig bedrijf kan zich immers ook een hoger losgeldbedrag veroorloven. Ook wordt er meer omzet misgelopen als de bedrijfsvoering platligt, wat een impuls is om snel te betalen.

Hogerop Trainingen
Meerdere werknemers van Hogerop Trainingen ontvangen een e-mail met een aanbod om gratis het nieuwe iPhone-model te testen. De e-mail oogt authentiek, maar wekt ook argwaan. Zo lijkt de tekst letterlijk vertaald uit het Engels, is de e-mail vrij generiek en ziet het e-mailadres van de afzender er rommelig uit. Een van de ontvangers stapt naar de IT-afdeling, die de e-mailfilters aanscherpt en de medewerkers waarschuwt.


‘Een waterdichte beveiliging tegen ransomware bestaat niet. Wel kunt u de kans op een aanval verkleinen en de impact minimaliseren.’

Beperk de impact van ransomware

Cybersecurity is een complex en dynamisch vakgebied. Er zijn honderden maatregelen die bescherming bieden tegen ransomware. Ook zijn er verschillende richtlijnen en best practices voor cybersecurity. Zo is er het NIST-raamwerk dat maatregelen verdeelt over vijf fases: het identificeren van risico's, het beschermen van de IT-infrastructuur, het detecteren van aanvallen, het reageren op incidenten en het herstel. Een ander bekend model is het MITRE ATT&CK-raamwerk, dat maatregelen categoriseert aan de hand van veertien aanvalsfases van.

In dit hoofdstuk maken we voor u de vertaalslag naar de praktijk. We beschrijven de belangrijkste maatregelen vóór, tijdens en na een ransomware-aanval.

Vóór een aanval

Een goede bescherming tegen ransomware begint bij bewustwording. Ransomware is een ernstige bedreiging die elke organisatie serieus zou moeten nemen. Gelukkig heeft IT-security voor het merendeel van de Nederlandse bedrijven prioriteit, zo blijkt uit de Monitor Digitale Transformatie van KPN. Er is een sterke samenhang tussen de omvang van het bedrijf en de mate van urgentie. Hoe groter het bedrijf, hoe meer prioriteit security krijgt en hoe meer maatregelen er zijn genomen.

De Monitor Digitale Transformatie laat evenwel zien dat er nog voldoende uitdagingen zijn op het gebied van cybersecurity. Zo geeft de meerderheid van de bedrijven aan niet goed (genoeg) voorbereid te zijn op een aanval. De helft maakt zich zorgen over de beveiliging van klant- en bedrijfsgegevens. Kennis vormt hierin de grootste bottleneck. Het is voor bedrijven lastig om de juiste IT- en securitykennis binnen te halen.

Fundamentele maatregelen

Een effectieve beveiliging tegen ransomware is geen lappendeken van losse maatregelen maar een continu proces dat door de hele organisatie heen loopt. Met deze tien maatregelen legt u hiervoor het fundament:

Risicoanalyse
Cybersecurity draait om het beschermen van de bedrijfskritische systemen en data. Bij een onderwijsinstelling zijn dat bijvoorbeeld de gegevens van studenten. Een retailer wil voorkomen dat de kassa- en voorraadsystemen door ransomware worden platgelegd. Deze 'kroonjuwelen' vormen het startpunt voor uw assetanalyse. Ook brengt u de voornaamste bedreigingen in kaart. Bepaalt u de impact voor de bedrijfscontinuïteit.

Patches en hardening
Hanteer voor alle hardware en software een strikt patch- en updatebeleid, zodat cruciale beveiligingsupdates zo snel mogelijk geïnstalleerd worden. Zorg er verder voor dat alle systemen veilig geconfigureerd zijn en schakel overbodige functies uit. Dit wordt hardening genoemd. Ook is het belangrijk dat u een goed overzicht heeft van alle IT-systemen. Dan kunt u sneller handelen als er een nieuwe kwetsbaarheid wordt ontdekt.

Toegangsbeheer
Beperk de toegang tot systemen en data, zodat deze afgeschermd zijn van de buitenwereld. Het uitgangspunt van Identity & Access Management (IAM) is: hoe minder toegang, hoe beter. Een werknemer krijgt alleen toegangsrechten die nodig zijn voor werk. Wees extra voorzichtig met het toekennen van beheerdersrechten. Deze accounts zijn zeer interessant voor cybercriminelen en moeten dus ook goed gemonitord worden.

Logging en detectie
Monitoring vormt de basis van de beveiliging. Door logbestanden van bedrijfssystemen bij te houden en afwijkingen te signaleren, kan een ransomware-aanval in een vroegtijdig stadium worden gedetecteerd. Ook maakt logging het makkelijker om te begrijpen hoe een incident kon plaatsvinden en wanneer het is begonnen.

Multifactorauthenticatie
Wachtwoorden zijn inherent onveilig. Ze kunnen onder andere via phishing gestolen worden of op een andere manier op internet belanden. Multifactorauthenticatie (MFA) voorkomt dat een aanvaller kan inloggen met alleen een gebruikersnaam en wachtwoord. De gebruiker moet zijn identiteit ook op een andere manier aantonen, bijvoorbeeld met een sms-code. Het activeren van MFA gaat ongeoorloofde toegang tot bedrijfssystemen tegen.

Macro's uitschakelen
Macro's automatiseren bepaalde taken in kantoorsoftware, maar ze worden ook gebruikt voor het verspreiden van malware. Een veelgebruikte truc is het versturen van een nepfactuur. De gebruiker moet de macro's activeren om de factuur te bekijken, waarna de malware wordt gedownload. IT-beheerders dekken dit risico bijvoorbeeld af door alle macro's standaard uit te schakelen zonder dat de gebruiker dit kan herstellen.

Endpointbeveiliging
Malware komt vaak binnen via malafide bijlages en het onbewust downloaden van bestanden (drive-by downloads). Een extra beveiligingslaag op endpoints zoals laptops en smartphones helpt dit te voorkomen. Een moderne oplossing voor endpointsecurity detecteert zowel bekende als nieuwe malware. Ook stelt u met zo'n oplossing in welke applicaties veilig zijn om te gebruiken. Schadelijke software wordt geblokkeerd.

Back-ups
Misschien wel de belangrijkste maatregel is het maken van meerdere back-ups. Zorg dat u minstens drie kopieën van bedrijfskritische data heeft op verschillende opslagmedia, zoals een externe harde schijf of op tape. Verplaats minstens één back-up naar een andere fysieke locatie of naar de cloud, en zorg voor minstens één offline back-up. Dit wordt de 3-2-1-1-regel genoemd. Test de back-ups ook regelmatig op verschillende manieren. Een recente back-up is essentieel in het geval van een ransomware-aanval.

Netwerksegmentatie
De aanvallers proberen zoveel mogelijk systemen te besmetten voordat ze de ransomware activeren. Daarom is het belangrijk om het netwerk goed te segmenteren. Dit betekent dat het netwerk in meerdere zones wordt verdeeld. Dat doet u bijvoorbeeld met behulp van firewalls. Door deze digitale branddeuren wordt het moeilijker om het gehele netwerk te compromitteren.

Incident-responseplan
Ga ervan uit dat uw bedrijf ooit slachtoffer wordt van ransomware. Belangrijke systemen zijn niet beschikbaar, uw bedrijfsvoering raakt ontregeld en de cybercriminelen eisen een fors geldbedrag. Hoe handelt u dan? Wat is uw beleid ten aanzien van het losgeld? Hoe ziet de herstelprocedure eruit? Hoe communiceert u met klanten en de media? Leg dit vast in een plan en oefen de afspraken regelmatig met verschillende afdelingen.

Tijdens een aanval

Maatregelen zoals MFA en het patchen van kwetsbaarheden maken het vooral moeilijker om in te breken op het netwerk. Maar als een aanvaller écht binnen wil komen, lukt dat meestal wel. Sommige maatregelen zijn dan ook primair gericht op het minimaliseren van de impact. Bijvoorbeeld door een indringer snel te detecteren, verdere verspreiding van de malware te voorkomen en de gegijzelde gegevens te herstellen. Daarbij volgt u de afspraken uit het incident-responseplan.

KPN Security adviseert bedrijven om in het geval van een ransomwarebesmetting eerst de impact in kaart te brengen. Welke data en systemen zijn niet toegankelijk en wat betekent dit voor de bedrijfsvoering? Schakel bij ernstige problemen forensisch specialisten in. Zij kunnen helpen bij de impactanalyse en bij het beperken van de schade. Doe ook altijd aangifte. De politie heeft bepaalde expertise die van pas kan komen. Daarnaast is het belangrijk dat de politie een zo volledig mogelijk beeld heeft van de impact op Nederlandse organisaties.

Zijn bij de ransomware-aanval persoonsgegevens versleuteld? Dan is er sprake van een datalek. De aanvallers hebben namelijk toegang gekregen tot de data om deze te kunnen versleutelen. Mogelijk vormt dit datalek een risico voor de privacy van de betrokken personen. In dat geval moet u het datalek binnen 72 uur melden bij de Autoriteit Persoonsgegevens. Informeer ook altijd de betrokkenen. Lopen zij een ernstig risico? Stel hen dan zo snel mogelijk op de hoogte.

Na een aanval

Een ransomware-aanval werkt nog lange tijd door. Vaak duurt het weken of maanden voordat het bedrijf weer volledig operationeel is. Mogelijk schrikt het incident klanten af, waardoor de omzet achterblijft. Tegelijkertijd zijn er bijkomende kosten zoals het inhuren van forensisch specialisten. Bovendien moet het bedrijf maatregelen treffen om herhaling te voorkomen. Daardoor is er minder geld voor bijvoorbeeld investeringen in de ontwikkeling van nieuwe producten en diensten.

Maar onderschat ook de menselijke impact niet. Zo'n incident is een stressvolle situatie voor alle betrokkenen. Dat geldt misschien nog wel het meest voor de IT-professionals. Mogelijk hebben zij al vele malen voor ransomware gewaarschuwd, maar was er geen budget voor aanvullende beveiligingsmaatregelen. Tijdens het incident werkten ze dag en nacht door om de schade te beperken. En onder de streep worden juist deze mensen alsnog verantwoordelijk gehouden voor de gevolgen.

Toch kan de nasleep van een ransomware-aanval ook positieve effecten hebben. KPN Security geeft een aantal adviezen die hieraan bijdragen:

1. Trek lering uit het incident

Never waste a good crisis. Dat geldt ook voor een ransomware-aanval. Durf kritisch te kijken naar de beveiliging en luister hierbij goed naar de IT-afdeling. Welke maatregelen hadden het moeilijker gemaakt om binnen te komen? Hoe konden de aanvallers zo lang ongemerkt het netwerk verkennen? Hoe verliep het crisismanagement? Waarom lukte het niet om de back-ups te terug te zetten? Zorg ervoor dat deze dialoog constructief verloopt.

2. Scherp de beveiliging verder aan

Gebruik de opgedane inzichten om de beveiliging daadwerkelijk naar een hoger niveau te tillen. Idealiter hanteert u een continu verbeterproces voor cybersecurity, waarbij u de maatregelen regelmatig test en optimaliseert. Zo wordt security onderdeel van het DNA. Wellicht blijkt dat uw bedrijf toch niet voldoende kennis en expertise heeft om dit proces goed in te richten. Schakel hiervoor dan een gespecialiseerde partner in.

3. Wees zo transparant mogelijk

Er rust nog steeds een taboe op ransomware-aanvallen. Veel getroffen bedrijven houden dit angstvallig geheim omdat ze vrezen voor reputatieschade. Dat is zonde, want een incident kan ontzettend leerzaam zijn voor andere bedrijven. Ook klanten en andere stakeholders waarderen openheid van zaken. Gelukkig zijn er steeds meer organisaties die juist transparant zijn over de aanvalsmethode en de keuzes die ze maken.

die ze maken.

Aanpak van cybersecurity: drie scenario's

In dit hoofdstuk brengen we de impact van maatregelen tegen ransomware tot leven. Dat doen we aan de hand van de drie fictieve bedrijven. Zij hebben elk een ander securityniveau.

Slagerij Hoek is nauwelijks bezig met cybersecurity. De eigenaar weet niet wat een ransomware-aanval is. Hij leest in het nieuws wel verhalen over cyberaanvallen, maar ziet Slagerij Hoek niet als een interessant doelwit. 'Bij mij valt niks te halen.'

Praktijkvoorbeeld: laag securityniveau
De eigenaar van Slagerij Hoek ontvangt een factuur van een leverancier die hij niet direct herkent. Geschrokken opent hij de factuur. Opeens gaat het scherm op zwart: 'Your files have been encrypted.' De laptop staat vol met belangrijke bedrijfsdocumenten, zoals de financiële administratie en contracten van werknemers. De slager moet 3500 euro in bitcoins betalen om weer toegang tot de data te krijgen. Back-ups zijn er niet.

De ondernemer staat voor een duivels dilemma. Het losgeldbedrag kan hij eigenlijk niet missen, maar zijn bestanden ook niet. En als hij wel besluit te betalen, is het maar de vraag of de gegevens inderdaad hersteld worden. Een snelle zoektocht op internet geeft hem weinig hoop op een oplossing. De politie neemt de aangifte op, maar kan verder niks voor hem betekenen. En dat allemaal door een relatief simpele truc.

Hogerop Trainingen is zich bewust van de dreiging van ransomware. Cybersecurity is ondergebracht bij IT. Met een beperkt budget heeft het IT-team enkele basismaatregelen genomen. Toch zijn er twijfels of het bedrijf goed voorbereid is op een aanval.

Praktijkvoorbeeld: gemiddeld securityniveau
De IT-manager van Hogerop Trainingen is nog maar net op kantoor als de digitale hel losbarst. De klantenservice krijgt allemaal boze telefoontjes van cursisten en docenten. Het online trainingsportaal en het e-mailsysteem werken niet. Ook ligt de website plat. Al snel blijkt dat vrijwel alle belangrijke bestanden door ransomware zijn versleuteld vanuit een ongebruikt account met beheerdersrechten. De losgeldeis: 70.000 euro in bitcoin.

Er ontstaat een chaotische situatie. IT probeert de back-ups terug te zetten, maar die zijn ook versleuteld. De directie steggelt over het besluit om wel of niet te betalen. Dan wordt het bedrijf gebeld door een journalist die lucht van de problemen heeft gekregen. Maar de communicatieafdeling mag niks zeggen en is niet voorbereid op dit scenario. Ondertussen blijven de boze cursisten bellen. Een deel vraagt al zijn geld terug.

Ransomware-aanval
Een aanval met een kwaadaardige bijlage zou bij Hogerop Trainingen heel anders verlopen dan bij Slagerij Hoek, want de IT-afdeling heeft macro's voor alle gebruikers uitgeschakeld. Toch wordt Hogerop Trainingen getroffen door ransomware. De aanvallers komen binnen via een kwetsbaarheid in verouderde hardware van een thuiswerker. Omdat de logging en detectie niet goed zijn ingeregeld, kunnen ze zich ongemerkt verspreiden over het netwerk. Net voor de start van het nieuwe semester wordt alles op slot gezet.

Hogerop Trainingen heeft wel maatregelen getroffen om besmetting te voorkomen, maar het patchbeleid bleek toch niet helemaal toereikend. Ook was de zakelijk opleider zoals gevreesd niet goed voorbereid op een ernstig incident. Daardoor duurt het herstel langer dan nodig en verloopt zowel de interne als de externe communicatie ronduit slecht. De reputatieschade wordt nog eens vergroot door een kritisch artikel in de krant.

Ultimate Home Store beschikt over een professioneel securityteam onder leiding van een ervaren CISO. De bescherming tegen ransomware is een topprioriteit. Wel heeft Ultimate Home Store moeite om voldoende IT- en securitykennis aan te trekken.

Van de drie bedrijven heeft Ultimate Home Store zijn beveiliging tegen ransomware het beste op orde. De CISO en zijn team voeren continu risicoanalyses uit en krijgen alle benodigde financiële middelen om de grootste risico's af te dekken. Daardoor zijn nog meer maatregelen mogelijk, zoals frequente security-awarenesstrainingen, een disaster-recoveryoplossing die het herstel bespoedigt en een samenwerking met een securityspecialist voor ondersteuning tijdens een incident.

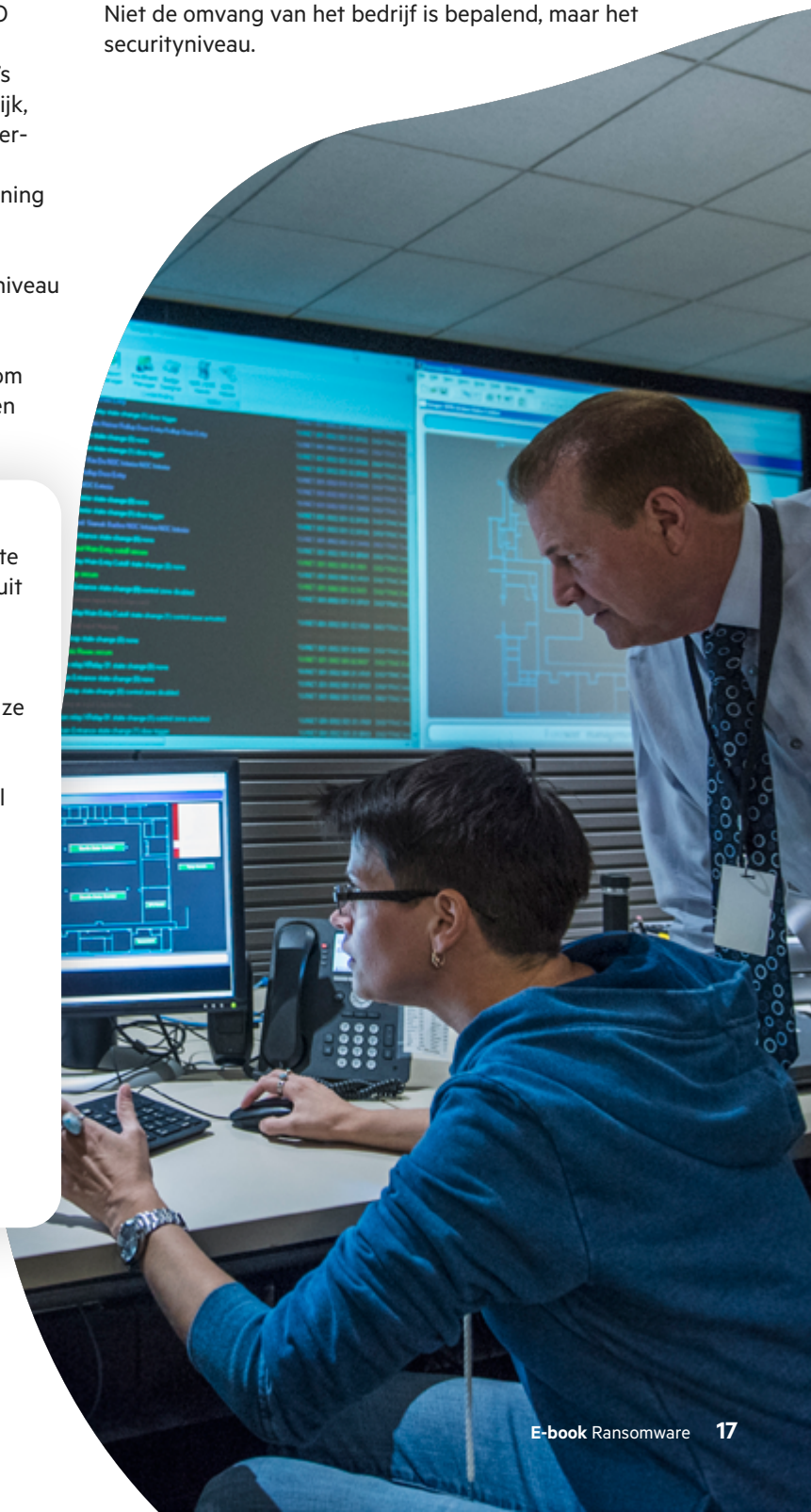
Toch is een ransomware-aanval ook bij dit hoge securityniveau niet uitgesloten. Een nieuwe ransomwarebende zoekt maandenlang naar een gaatje in de beveiliging van Ultimate Home Store. Uiteindelijk lukt het de aanvallers om inloggegevens van een kantoormedewerker te ontfutselen via een gerichte phishingmail.

Praktijkvoorbeeld: hoog securityniveau

Het securityteam acteert op een melding over verdachte activiteit op het netwerk. Er wordt geprobeerd om vanuit het buitenland in te loggen op een bedrijfssysteem. Dankzij MFA mislukt dat. Een maand later slaan de aanvallers alsnog toe, dit keer via een onbekende kwetsbaarheid in een e-mailserver. Van daaruit leggen ze het webwinkelsysteem plat en versleutelen ze een deel van de klantgegevens. Netwerksegmentatie voorkomt een verdere verspreiding van het netwerk. Een speciaal crisisteam volgt een zorgvuldig afgestemd en getest incident-responseplan. Onderdeel van dit plan is het inschakelen van de securitypartner, die forensisch onderzoek uitvoert en extra IT-capaciteit beschikbaar stelt. Tegelijkertijd werkt het eigen IT-team aan het terugzetten van de back-ups. Uit principe wordt nooit losgeld betaald aan cybercriminelen.

Klanten merken dat de website niet bereikbaar is. Via social media stelt de klantenservice hen op de hoogte van een cyberaanval waarbij mogelijk klantgegevens zijn buitgemaakt. De communicatie-afdeling kan ook journalisten hiernaar verwijzen.

Deze drie scenario's illustreren het nut en de noodzaak van beveiligingsmaatregelen. Ze verkleinen de kans op incidenten en beperken de schade als het toch misgaat. Toch is een kanttekening op zijn plaats. Ook een multinational met een enorm securitybudget kan ernstig in de problemen komen door ransomware. En er zijn genoeg kleine ondernemers die wél back-ups maken en in staat zijn om nepmails te herkennen. Niet de omvang van het bedrijf is bepalend, maar het securityniveau.



Slotwoord: neem ransomware serieus

Elk bedrijf kan slachtoffer worden van een ransomware-aanval. Met de juiste maatregelen verkleint u de risico's significant. En als iedere organisatie dit doet, maken we samen een vuist tegen cybercriminaliteit.

De bewustwording rondom ransomware groeit met de dag. Met name de financiële sector heeft de beveiliging prima op orde. Helaas zijn er ook nog steeds bedrijven die ransomware niet serieus nemen. Zo'n aanval is iets dat anderen overkomt. Zelf zijn ze toch geen interessant doelwit. En ze hebben toch niet voor niets een IT-afdeling? Die zorgt er maar voor dat alles gewoon blijft werken. Andere bedrijven besteden hun IT uit aan een partner, met het idee dat deze ook de beveiliging regelt.

Dit zijn kapitale denkfouten. Van persoonsgegevens tot geldbedragen: bij elk bedrijf valt wel iets te halen. De IT-afdeling weet heus wel dat ransomware een groot risico vormt, maar heeft vaak niet de specifieke kennis én de financiële mogelijkheden om de juiste maatregelen te treffen. En zelfs als dat wel het geval is: ransomware gaat iedereen binnen de organisatie aan. Zo kan elke werknemer in een phishingmail trappen. Geen IT-partner kan alle risico's voor u afdekken.

Maatschappelijke verantwoordelijkheid
KPN Security ziet het als zijn maatschappelijke plicht om de digitale weerbaarheid van Nederland te verhogen.
Dat doen we allereerst door onze klanten zo goed mogelijk te beschermen. We bieden inzicht in cyberrisico's en passen de security daarop aan, zonder de bedrijfsvoering te hinderen. Zo creëren we rust en verkleinen we het risico op een ernstig incident. Samen met de klant verhogen we het securityniveau stapsgewijs. En als het toch misgaat? Dan staan we 24/7 klaar met hulp en advies.

Onze missie is Nederland veiliger te maken. Zo organiseert KPN Security meerdere keren per jaar het securityevent NLSecure[ID]. Eens per jaar publiceren we het gratis securitymagazine Cyber Security Perspectives. Op deze manier informeren we bedrijven over het dreigingslandschap en best practices. Verder werken we op diverse manieren samen met overheidsinstanties zoals het Team High Tech Crime van de Nederlandse politie en de FBI. Samen maken we Nederland veiliger.

Uw partner voor cybersecurity
Met dat uitgangspunt is ook dit e-book ontwikkeld. We hopen dat u de inzichten kunt toepassen om uw organisatie weerbaarder te maken tegen ransomware. Heeft u hier hulp bij nodig? Of wilt u graag door een onafhankelijke partij laten toetsen hoe effectief uw beveiliging is? Neem dan geheel vrijblijvend contact met ons op via kpnsecurity@kpn.com.

Meer informatie

Wilt u meer weten over hoe KPN Security u kan helpen bij het voorkomen van ransomware? Neem dan contact op met uw accountmanager of via kpnsecurity@kpn.com

AD-20743/06-22/KRE