RANSOMWARE
NEEM MAATREGELEN EN BEREID JE VOOR

- ICT beheer
- Cloud
- Security
- Hardware
- Telefonie

acf bentveld

ICT VOOR NU EN STRAKS

IN DEZE BROCHURE


acf
bentveld

INLEIDING

Ransomware, in het Nederlands ook wel gijzelsoftware, is een computervirus (malware) dat je computer of alle bestanden erop kaapt en deze vervolgens versleuteld zodat ze niet meer toegankelijk zijn. De cybercriminelen achter deze malware proberen jou, of jouw bedrijf, vervolgens losgeld (ransom) te laten betalen om weer toegang te krijgen tot de versleutelde bestanden. Vaak eisen deze cybercriminelen betaling door middel van Bitcoins (digitale munteenheid). Betaal je niet, dan heb je geen toegang meer tot je bestanden. Ook komt het wel voor dat de bestanden online worden geplaatst zodat anderen jouw bestanden (met misschien wel vertrouwelijke gegevens) vrij kunnen downloaden. Bevatten jouw bestanden belangrijke of vertrouwelijke gegevens, dan zou dit zomaar een methode kunnen zijn om je toch over te halen om het losgeld te gaan betalen.

Ransomware is uitgegroeid tot de grootste online bedreiging voor het bedrijfsleven en zeker ook voor het Midden- en Klein Bedrijf (Mkb). Een succesvolle ransomware-aanval kan niet alleen jouw toegang tot bestanden beperken, maar ook de algehele bedrijfsvoering lamleggen. Klanten kunnen wellicht geen orders meer plaatsen, facturen worden niet meer verstuurd en het uitbetalen van salarissen is ook niet meer mogelijk. Daarnaast kan een geslaagde ransomware aanval zorgen voor reputatieschade wanneer je klanten horen dat jouw bedrijfsnetwerk gegijzeld is en hun gegevens mogelijk op straat liggen. Steeds meer bedrijven en organisaties zijn zich gelukkig bewust van deze onlinebedreigingen.

Maar welke maatregelen moet je nou nemen om echt goed beschermd te zijn tegen cybercriminaliteit in het algemeen en ransomware in het bijzonder?

In deze ransomwaregids hopen wij je meer inzicht te geven.

HOE WERKT EEN RANSOMWARE AANVAL?

Laten we eerst eens gaan kijken hoe een gemiddelde ransomware aanval verloopt. Een ransomware aanval doorloopt eigenlijk altijd een aantal fasen waarin de cybercrimineel in stappen toewerkt naar zijn/haar doel: losgeld! Er zijn verschillende modellen die het proces van een cyberaanval beschrijven. In deze ransomwaregids behandelen we het model van het Computer Emergency Response Team (CERT) uit Nieuw-Zeeland.

DIT MODEL BESTAAT UIT DRIE FASEN

Fase 1
Initiële toegang

Een Cybercrimineel gebruikt verschillende methodes om toegang te verkrijgen zoals:

- Phishing
- Raden van accountgegevens
- Misbruik maken van kwetsbaarheden in software
- Versturen van malware via malafide e-mailbijlagen
- Configuratiefouten

Fase 2
Consolidatie en voorbereiding

De Cybercrimineel beweegt zich binnen de omgeving van de organisatie om:

- Volledige toegang te krijgen tot alle systemen binnen de organisatie
- Gevoelige en/of financiële informatie te achterhalen
- Te achterhalen waarmee het slachtoffer kan worden gechanteerd

Fase 3
Impact op doelwit

De Cybercrimineel gaat over tot actie om de uiteindelijke doelen te bereiken:

- Wegsluizen van informatie en/of data
- Versleutelen en/of verwijderen van originele data
- Verwijderen van back-ups
- De financiële afhandeling – het losgeld

Bovenstaand schema is een gefingeerd voorbeeld van een geslaagde ransomware aanval

Gericht aanvallen versus schieten met hagel

Het is goed je te realiseren dat de meeste Mkb-bedrijven geen doelwit zijn van cybercriminelen. Je kunt er dan dus ook vanuit gaan dat een ransomware aanval niet specifiek gericht is op jouw bedrijf. Door gebruik te maken van grootschalige phishingcampagnes of geautomatiseerde bruteforceaanvallen (pogingen om wachtwoorden te kraken) komen ze jouw bedrijf of medewerkers van jouw bedrijf toevallig tegen. Slecht beveiligde accounts van medewerkers of een medewerker die informatie achterlaat op een website welke is toegestuurd door een cybercrimineel (phishing) zijn voor een groot deel de oorzaak van ransomware aanvallen in het Mkb.

Het Mkb heeft dus voornamelijk te maken met ‘schieten met hagel’.

Grotere organisaties zijn veel vaker een gericht doelwit. Hier is immers over het algemeen veel meer geld te halen. Grote organisaties hebben daarentegen wel meer budget (voor cybersecurity) en daardoor (vaak) een betere beveiliging. Grote organisaties hebben veelal meer middelen om hogere losgeldbetalingen te doen en lopen over het algemeen ook meer omzet mis wanneer de bedrijfsvoering langere tijd stil ligt. Voor Cybercriminelen is het dus echt een zakelijke (lees commerciële) afweging: hoeveel tijd en middelen gaan we inzetten om dit specifieke bedrijf aan te vallen en hoeveel zou het kunnen opleveren?

RANSOMWARETREND

Bedrijven worden steeds vaker door verschillende ransomwaregroepen kort na elkaar aangevallen met verschillende vormen van ransomware. Gevolg kan zijn dat data meerdere malen wordt versleuteld wat herstel nog veel complexer maakt en er meerdere malen losgeld wordt geëist.

DE EVOLUTIE VAN RANSOMWARE

De term Ransomware horen we pas de afgelopen jaren veelvuldig. Dit wordt mede veroorzaakt doordat grote en bekende organisaties worden geraakt. Deze organisaties zijn dan enkele dagen of soms zelfs enkele weken niet in bedrijf waardoor andere organisaties of consumenten er last van hebben.

Ransomware in het nieuws

Denk bijvoorbeeld aan de ransomware aanval bij de Mediamarkt waardoor er alleen nog maar producten die fysiek in de winkels stonden konden worden verkocht. Afhalen en retourneren van producten was niet meer mogelijk. Lees meer over het verloop van deze ransomware aanval en de onderhandelingen met de cybercriminelen op de website van RTLnieuws. Ook de 'Kaashack' is een bekend voorbeeld van ransomware die de afgelopen jaren het nieuws heeft gehaald. Door een geslaagde ransomware aanval bij een leverancier van onder andere Albert Heijn lag er dagenlang geen kaas in de schappen van de supermarkten.

Dit soort aanvallen komen in het nieuws en daardoor lijkt ransomware iets te zijn van de afgelopen jaren. Toch verscheen in 2011 al de 'politie-ransomware' waarbij aanvallers computers op slot zetten en een politielogo in beeld brachten met de melding dat er kinderporno was gevonden. Er werd een 'boete' in rekening gebracht die online kon worden betaald. De computer kon echter heel eenvoudig worden hersteld omdat de bestanden niet echt versleuteld waren.

ER WORDT CONTINU GEKEKEN MET WELKE METHODES ZE HET MAKKELIJKST GELD VERDIENEN

Bloeiende business

Sinds 2011 zijn de cybercriminelen echter flink geprofessionaliseerd. De malware is veel effectiever en ongelooflijk veel sneller geworden. De aanvalstactieken zijn gigantisch uitgebreid en veel geavanceerder geworden. Cybercriminelen zijn constant aan het experimenteren met welke methodes ze de meeste opbrengst behalen. Vragen ze bijvoorbeeld meer of minder losgeld, is er wel of geen mogelijkheid tot onderhandelen en is er wel of geen persoonlijk contact. Er wordt continu gekeken met welke methodes ze het makkelijkst geld verdienen.

Cybercriminaliteit is een bloeiende business waar ontzettend veel geld wordt verdiend. Met professionele ondersteuning en service proberen de cybercriminelen hun slachtoffers optimaal te helpen om ze zodoende over te halen tot betaling van losgeld. Ging het in het verleden nog over tientjes aan losgeld, tegenwoordig eisen de cybercriminelen (natuurlijk afhankelijk van het slachtoffer) zomaar tientallen miljoenen euro's aan losgeld.

Ontwikkeling

De ontwikkeling van ransomware is dus de afgelopen jaren erg snel gegaan. Maar uit recente onderzoeken en verschillende aanvallen blijkt wel dat de ontwikkeling nog steeds doorgaat. Verschillende branches worden aangewezen als branches met een hoger risico. Zo zijn IT-leveranciers tegenwoordig een favoriet doelwit en zijn er signalen dat cybercriminelen zich richten op land- en tuinbouw.

Dit zijn dan dus meer gerichte aanvallen op specifieke bedrijven en sectoren, maar de verwachting is dat het 'schieten met hagel' ook gewoon zal blijven bestaan en dat daardoor Mkb-bedrijven nog steeds doelwit blijven van ransomware-bendes.

DE KOSTEN VAN EEN GESLAAGDE RANSOMWARE AANVAL

Een geslaagde ransomware aanval kost geld en in veel gevallen heel veel geld. Uiteraard variëren deze kosten en zijn ze onder andere afhankelijk van de grootte en het soort bedrijf dat is aangevallen. Daarnaast speelt het ook een rol of het getroffen bedrijf kan terugvallen op een recente back-up en hoeveel tijd het kost om deze back-up weer terug te zetten. Met welke kosten dien je als Mkb-ondernemer nu rekening te houden?

Kosten voor verlies van productiviteit

Wanneer je bedrijf wordt geraakt door een ransomware aanval dan ligt je bedrijf stil of kan in elk geval het kantoorpersoneel niet meer aan het werk. In veel gevallen zien we echter dat productie afdelingen ook volledig afhankelijk zijn van de ICT-infrastructuur. We kunnen dus wel stellen dat in de meeste gevallen de bedrijfsvoering compleet stil komt te liggen. Hoe lang deze periode duurt (en wat het bedrijf dit dus in totaal gaat kosten) is afhankelijk van het feit of er een back-up beschikbaar is, hoe snel deze kan worden teruggezet en natuurlijk hoe recent deze back-up daadwerkelijk is. Hoe snel kun je als bedrijf herstellen van een cyberincident?

Kosten voor externe hulp

Onderhoud je zelf je ICT-omgeving of heb je hiervoor een partner? Zijn er vertrouwelijke gegevens buit gemaakt of weet je dat niet zeker? Veel Mkb-bedrijven besteden de ondersteuning en het onderhoud van hun ICT-omgeving uit aan een externe ICT-partner. In veel gevallen zal een geslaagde ransomware aanval geen onderdeel uitmaken van een onderhoudscontract en zullen de werkzaamheden van de ICT-partner worden doorbelast. xIn veel sectoren wordt er gewerkt met vertrouwelijke gegevens.

Als bedrijf of organisatie wil je dan ook weten of er inderdaad vertrouwelijke gegevens zijn gelekt en natuurlijk ook hoe de cybercriminelen zijn binnengekomen. In dit soort gevallen komt een forensische onderzoeker of incident response-team om de hoek kijken, vaak ‘dure jongens’. Gespecialiseerde bedrijven met veel kennis en kunde die de doorloop van een ransomware aanval vaak volledig kunnen reconstrueren. Dit zodat jij als eigenaar van je bedrijf duidelijk hebt wat er is buit gemaakt en hoe de cybercriminelen te werk zijn gegaan.

Kosten voor (tijdelijk) extra personeel

(Langdurig) verlies van productiviteit moet weer ingehaald worden en veel bedrijven hebben daar niet standaard de mensen voor beschikbaar. Je productiviteit weer op orde brengen, maar vooral de opgelopen achterstand weer inhalen kan zorgen voor hoge kosten.

Kosten voor extra beveiligingssoftware of hardware

In sommige gevallen blijkt een bedrijf onvoldoende beveiligd. Een ransomware aanval wil je niet nog een keer meemaken, dus investeren in betere beveiliging zal dan ook één van de stappen zijn die je als organisatie zal gaan nemen.

32% VAN DE MKB-BEDRIJVEN HEEFT AFGELOPEN JAAR TE MAKEN GEHAD MET EEN CYBERSECURITY INCIDENT

Betalen van losgeld

Hoewel het wordt afgeraden hebben sommige bedrijf gewoon geen keuze, ze moeten losgeld betalen. De back-up was ook versleuteld of heeft de afgelopen maanden gewoon niet goed gewerkt. Om dan je data terug te krijgen kun je wachten totdat de decryptie-sleutels voor “jouw” ransomware beschikbaar komen of ervoor kiezen met de cybercriminelen in onderhandeling te gaan om vervolgens over te gaan tot betalen van losgeld. Deze bedragen variëren van enkele tienduizenden euro’s tot vele miljoenen, dit is uiteraard afhankelijk van de grootte en het soort bedrijf dat is getroffen. Het betalen van losgeld biedt echter geen garantie dat je de data ook daadwerkelijk terugkrijgt of dat je enkele weken/maanden later niet alsnog een keer wordt aangevallen door dezelfde ransomwarebende.

Kosten voor het verliezen van klanten of reputatieschade

Hoe kijken jouw relaties naar jouw bedrijf wanneer je bent geraakt door een ransomware aanval? Welke gegevens zijn buit gemaakt en welke hinder ondervinden jouw klanten hiervan? Geen bedrijf is 100% veilig tegen ransomware en het kan ook echt ieder bedrijf overkomen, maar klanten kunnen het vertrouwen in jouw bedrijf verliezen waardoor ze besluiten om met een concurrent in zee te gaan.

Wat zeggen de onderzoekers?

Onderzoek van Connectwise geeft aan dat wereldwijd 32% van de Mkb-bedrijven afgelopen jaar te maken heeft gehad met een cybersecurity incident. De financiële schade varieert behoorlijk, maar komt gemiddeld uit op ongeveer € 100.000,00. Een geslaagde ransomware aanval levert echter aanzienlijk meer financiële schade op. Onderzoek van onder andere onze securitypartner ESET toont aan dat de gemiddelde kosten voor een geslaagde ransomware aanval voor een Mkb-bedrijf ongeveer € 220.000,00 zijn. In Nederland blijkt dit gemiddelde echter nog hoger te liggen met bedragen rond de € 270.000,00. Dit wordt mede veroorzaakt doordat veel bedrijven in Nederland enorm hebben geïnvesteerd in digitalisering. De conclusie die we hieruit kunnen trekken is dat het een Mkb-bedrijf veel geld en tijd kost om te herstellen van een geslaagde ransomware aanval. In sommige gevallen kan het zelfs het voortbestaan van een bedrijf in gevaar brengen. Uiteindelijk kan geen enkel bedrijf zichzelf 100% beschermen tegen ransomware of andere vormen van cybercriminaliteit. Toch zijn er voldoende maatregelen beschikbaar waarmee je het cybercriminelen verschrikkelijk lastig kunt maken. Daarover vertellen we je in het volgende hoofdstuk meer.


/ ICT voor
nu en straks

RANSOMWARETREND

Data vernietigen in plaats van versleutelen. Gegevens stelen en vervolgens de originele bestanden vernietigen. Dit lijkt een nieuwe ransomware-methode te zijn om zodoende getroffen bedrijven nog verder onder druk te kunnen zetten. Herstel van versleutelde data is immers niet meer mogelijk, de data is er niet meer. Zo hopen cybercriminelen dat meer slachtoffers overgaan tot het betalen van losgeld.

EEN RANSOMWARE AANVAL VOORKOMEN

Eén eenvoudige oplossing om een ransomware aanval te voorkomen is er niet. 100% bescherming tegen een ransomware aanval is er ook niet. Toch is het mogelijk om de kans op een geslaagde ransomware aanval te minimaliseren. Dit kun je realiseren door een samenspel van verschillende maatregelen en het zal je misschien verbazen, niet al deze maatregelen zijn van technische aard.

Een goede cybersecurity-strategie houdt rekening met de driedeling mens, organisatie en techniek waarbij mens en organisatie van evenveel belang zijn als de gebruikte techniek.

Alle mogelijke maatregelen benoemen zal zorgen voor een ontzettend lange whitepaper. Wij hebben ons beperkt tot een gangbare, maar effectieve set aan maatregelen. Bijkomend voordeel van deze set is dat zij ook andere vormen van cybercriminaliteit helpt te voorkomen.

Lees op de volgende pagina de set aan maatregelen.


acf
bentveld

Bewustzijn van medewerkers

Mensen zijn gewoontedieren en de kans dat een medewerker binnen jouw bedrijf op een phishing link klikt, is gewoon aanwezig. Een medewerker van de administratie is er bijvoorbeeld minder op getraind phishing e-mail te herkennen. Zo kun je het bewustzijn van medewerkers verhogen door het (regelmatig laten) geven van een Security Awareness training of door het uitvoeren van phishing simulaties.

Toegangsbeveiliging

Cybercriminelen hebben (meestal) toegang nodig tot accountgegevens van een medewerker om toegang te krijgen tot het bedrijfsnetwerk of de specifieke computer. Door het gebruik van wachtwoordzinnen, verschillende wachtwoorden per account en het toepassen van Multi Factor Authenticatie wordt het voor cybercriminelen haast onmogelijk om wachtwoorden te raden of toegang te krijgen tot het account. Uiteraard is het dan ook van belang dat de medewerkers voldoende uitleg krijgen in het gebruik van Multi Factor Authenticatie.

Updaten maar

Hard- en software up-to-date houden is een zeer belangrijk onderdeel van een goede cybersecurity strategie. Cybercriminelen proberen (helaas regelmatig succesvol) misbruik te maken van lekken in software welke al gedicht hadden kunnen zijn wanneer er op tijd updates geïnstalleerd zouden zijn. Geautomatiseerd patchmanagement zorgt ervoor dat die updates snel, op tijd en geautomatiseerd worden geïnstalleerd. Dit bespaart tijd, maar zorgt vooral voor een up-to-date ICT omgeving.

Positieve securitycultuur

Helaas zien we nog wel eens gebeuren dat een medewerker wordt gestraft (of belachelijk wordt gemaakt) wanneer hij/zij een phishing e-mail aanklikt. Dit noemen ze ook wel ‘naming & shaming’. Vaak resulteert dit erin dat die betreffende medewerker een eventuele volgende keer dat het hem/haar gebeurt niet meer vertelt met verstrekkende gevolgen. Meld een medewerker een security-incident beloon dit meteen. Dit zorgt voor betrokkenheid en een open cultuur waardoor incidenten veel sneller worden opgemerkt.

Endpoint Detection & Response (EDR) (of toch maar XDR?)

Een goede antimalware op werkplekken en op servers is natuurlijk van essentieel belang. Antimalware in combinatie met EDR zorgt voor zichtbaarheid en geautomatiseerde respons op endpoints zoals laptops en werkstations. Maar bedrijfsnetwerken van tegenwoordig bestaan uit veel meer dan alleen werkplekken en servers. Denk bijvoorbeeld aan smartphones, maar ook aan machines in je bedrijf welke met het netwerk of zelfs het internet verbonden zijn. XDR (eXtended Detection & Response) wordt ook wel 'Any-Data-Source- detectie genoemd en baseert zich op gegevens en detectie van veel meer producten. Zo kan XDR direct actie ondernemen door bijv. te reageren op detectie in e-mail, netwerk, identiteit van medewerkers en nog veel meer.

Het uitdelen van de juiste rechten en het indelen van het netwerk

Geef medewerkers de rechten die ze nodig hebben voor hun dagelijkse werkzaamheden en niet meer. Zorg voor een gescheiden WIFI netwerk (gasten en intern) en verdeel het netwerk zo mogelijk in verschillende segmenten. Hierdoor wordt het een stuk lastiger om het gehele netwerk te besmetten.

Monitoring

Het monitoren, loggen en analyseren van netwerkverkeer kan ervoor zorgen dat afwijkende activiteiten snel worden gesignaleerd. Hierdoor kan er mogelijk sneller worden opgetreden in geval van een incident.

Back-up (!!!)

Back-up schrijven we hier met drie uitroeptekens en dat is niet voor niets. Een goede, actuele back-up op een externe locatie is van essentieel belang om snel te kunnen herstellen na een geslaagde ransomware aanval. Een ijzersterke back-up strategie is cruciaal voor ieder bedrijf. Zorg in elk geval voor drie kopieën van je data, dat je de back-ups op twee verschillende media opslaat en er in elk geval één kopie op een andere locatie wordt bewaard. Daarnaast zou het nog beter zijn wanneer er vervolgens ook nog één offline back-up beschikbaar is. Wil je nog een stapje verder gaan dan is Disaster Recovery de te nemen stap. Met Disaster Recovery zorg je ervoor dat de bedrijfscontinuïteit zo snel mogelijk wordt hersteld na een calamiteit.
Met als doel: de (economische) impact tot een minimum te beperken.

TOCH SLACHTOFFER GEWORDEN
EN NU?

Niet betalen

De overheid en justitie geven het advies om in elk geval geen losgeld te betalen. Door het betalen van losgeld zorg je ervoor dat de cybercriminelen geld verdienen en houd je dus hun verdienmodel in stand. Daarnaast is er ook niet de garantie dat je ook daadwerkelijk je bestanden terugkrijgt (of deze niet online worden gepubliceerd) wanneer je het losgeld betaald en zijn er verschillende gevallen bekend waarbij betalende slachtoffers enkele weken of maanden later nogmaals slachtoffer werden van dezelfde ransomware(bende). Maar wat moet er dan wel gebeuren?

1. Breng de betrokkenen op de hoogte.

Voordat je zelf ook maar iets gaat doen neem contact op met je ICT-afdeling of ICT-partner. Geef duidelijk aan dat je waarschijnlijk te maken hebt met een ransomware aanval. Het advies hierbij is om vervolgens een gespecialiseerde partij, samen met de ICT-afdeling of ICT-partner, onderzoek te laten doen naar de aanval. De vervolgstappen zullen sowieso samen met de ICT-afdeling of -partner en/ of de gespecialiseerde partij uitgevoerd dienen te worden.

2. Isoleer (zo mogelijk) het getroffen systeem of de getroffen systemen.

Is er één computer binnen het bedrijfsnetwerk besmet isoleer deze dan van de rest van het netwerk door de netwerkverbinding te verbreken. Zet de betreffende PC niet uit.

3. Maak een foto of screenshot van het losgeldbericht.

Wanneer de bestanden op je computer zijn versleuteld dan krijg je vanzelf een bericht in beeld met instructies hoe je contact op moet nemen en vooral natuurlijk hoe je kunt betalen. Maak hiervan altijd een foto en bewaar deze bijvoorbeeld op je smartphone. Je kunt deze later nodig hebben bij een eventuele decryptietool of bij je aangifte.

4. Gebruik antivirus en controleer of je computer vrij is van malware gebruik.

Indien aanwezig, antivirus- of antimalwareprogramma's om de ransomware te verwijderen van je computer of laptop. Mogelijk moet je het systeem opnieuw opstarten in de veilige modus. Door de ransomware te verwijderen (als dit al lukt) krijg je geen toegang tot je bestanden, maar kun je mogelijk wel veilig proberen de originele bestanden te herstellen.

5. Controleer of ontsleuteling mogelijk is.

Op de website van de Fraudehelpdesk of No More Ransom (wat een samenwerking is tussen onder andere de Politie en Europol) vind je informatie over hoe je bestanden kunt herstellen. Op No More Ransom zijn decryptieprogramma's beschikbaar voor verschillende ransomwarevormen. Er is helaas geen garantie dat deze programma's ook daadwerkelijk werken en voor veel ransomwareversies is helaas geen decryptie beschikbaar.

Op No More Ransom zijn decryptieprogramma's voor ransomware beschikbaar. Regelmatig worden hier nieuwe Decryptors toegevoegd. Maak dus ook een back-up (op bijvoorbeeld een externe harde-schijf) van de versleutelde bestanden. Het kan zomaar zijn dat er over een paar maanden wel een decryptor beschikbaar is zodat je alsnog je bestanden kunt ontsleutelen. Controleer dus ook regelmatig **deze** website voor nieuwe decryptors.

6. Geen decryptie beschikbaar? Dan kun je alleen nog maar terugvallen op een Back-up.

In veel gevallen is een goede back-up de enige manier om toegang te krijgen tot je bestanden. Maak je dagelijks een back-up dan is de hoeveelheid gegevensverlies over het algemeen beperkt. Maak je maar af en toe een back-up dan ga je verder terug in de tijd. Maar dit is nog steeds beter dan helemaal opnieuw te moeten beginnen. Lees op pagina xx hoe je een goede back-up van je gegevens maakt.

7. Goede back-up? Zeker? Dan deze herstellen op een schoon geïnstalleerde machine.

Ben je er zeker van dat er een goede back-up beschikbaar is? Heb je dit bijvoorbeeld getest door de back-up terug te zetten op een andere machine? Dan is het advies om de data niet op de eerder versleutelde computer terug te plaatsen maar hiervoor een nieuw geïnstalleerde machine te gebruiken.

8. Doe aangifte en meld (indien nodig) een datalek.

Aangifte doen na een cyberaanval of ransomware aanval is erg belangrijk. Wanneer er aangifte wordt gedaan heeft de politie, en dan vooral de cybercrime-unit van de politie, inzicht in wat er in Nederland gebeurt, welke ransomware-bendes actief zijn en of er specifieke branches worden aangevallen.

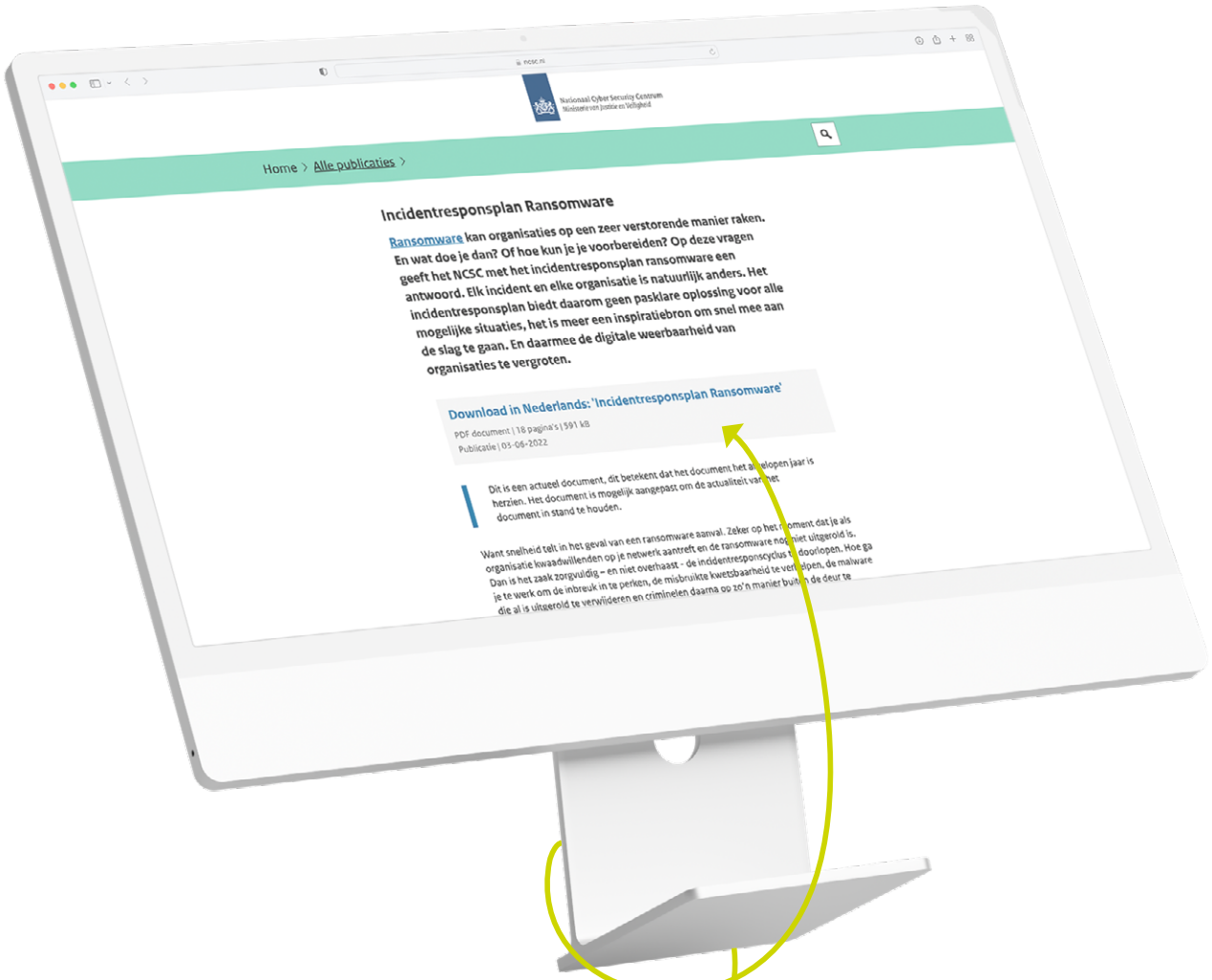
Is er persoonlijke of vertrouwelijke data buitgemaakt? Dan is de kans aanwezig dat er een melding gedaan moet worden bij de Autoriteit Persoonsgegevens.

9. Niet onbelangrijk – leer van het incident en scherp beveiliging aan.

Never waste a good crisis! Durf kritisch te kijken naar de beveiliging van je bedrijf of het bedrijfsnetwerk. Welke maatregelen had je kunnen nemen die de aanval hadden kunnen voorkomen (of het in elk geval de cybercriminelen een stuk lastiger had gemaakt)? Hoe kan het dat de aanvallers zo lang ongemerkt actief konden zijn? Waarom kon de back-up niet worden teruggezet? Etc etc. Gebruik de verkregen informatie om de beveiliging aan te scherpen. Til de beveiliging naar een hoger niveau.

10. Wees transparant.

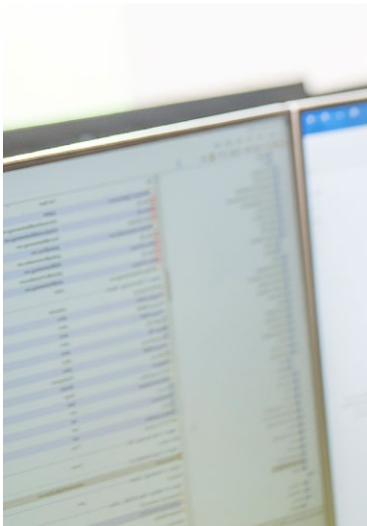
Veel bedrijven kiezen er helaas voor een datalek of cyberaanval stil te houden. Een cyberincident kan echter ontzettend leerzaam zijn voor andere bedrijven en organisaties en gelukkig waarderen klanten openheid van zaken ook gewoon. Uiteraard moet er goed afgewogen worden wat je wel of niet communiceert, maar geef openheid van zaken over het incident.



KLIK HIER OM TE OPENEN!

Incident responseplan

Het is goed om een incident response plan klaar te hebben liggen. Hierin staat onder andere beschreven wat je wel en vooral niet moet doen om schade te beperken of te herstellen. Ook is beschreven met welke partijen, personen of organisaties je contact dient op te nemen. Het doel van een incidentresponseplan is om snel, kalm en adequaat te kunnen reageren op een incident om zodoende schade te beperken en herstelwerkzaamheden te minimaliseren.



HET NCSC HEEFT EEN DOWNLOADBAAR VOORBEELD VAN EEN GOED INCIDENT RESPONSEPLAN OP HUN WEBSITE STAAN

Back-up

Back-up is een cruciaal onderdeel om van een geslaagde ransomware aanval te kunnen herstellen. Zonder back-up valt er immers niets te herstellen. Maar wat is nu een goede back-up? Voor ieder type bedrijf zijn er andere vereisten voor de back-up, maar over het algemeen geldt er voor ieder bedrijf dezelfde basis.

Maak dagelijks een back-up

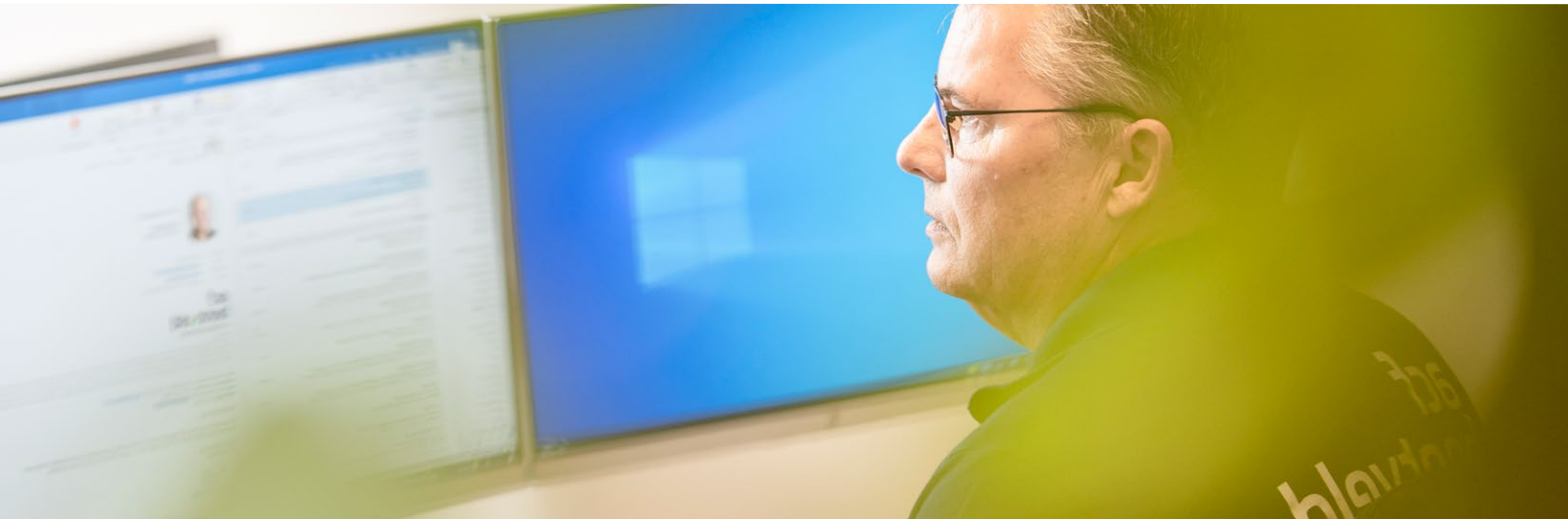
Hoe vaker je een back-up maakt, hoe beter. Maak je dagelijks een back-up dan blijf je actueel en kost het veel minder tijd (en dus geld) om te herstellen na een ransomware aanval.

Maak een back-up op verschillende locaties

Zorg ervoor dat je een back-up maakt op een fysieke locatie en bij voorkeur op een online locatie. Een fysieke locatie (zoals bijvoorbeeld een externe harde-schijf) kan wel vernietigd worden door brand maar is minder vatbaar voor digitale aanvallen. Een online locatie is daarentegen minder vatbaar voor fysieke schade maar is wel vatbaarder voor online aanvallen. Wanneer je beide opties gebruikt ben je dus sowieso zekerder van een goede beschikbare back-up.

Test je back-up regelmatig

Dagelijks een back-up maken is goed maar niet goed genoeg. Je weet pas zeker dat een back-up goed werkt wanneer je deze regelmatig test. Dit doe je door te controleren of er ook daadwerkelijk data op de back-up locatie is opgeslagen. Maar natuurlijk is het nog beter om regelmatig ook eens een set data te herstellen vanuit een back-up.



CONCLUSIE

Een ransomware aanval 100% voorkomen is eigenlijk niet mogelijk. Je kunt als bedrijf, maar ook gewoon als consument, verschillende maatregelen nemen om het de cybercriminelen zo moeilijk mogelijk te maken. Natuurlijk zul je ook maatregelen moeten treffen om zo eenvoudig en snel mogelijk van een incident te kunnen herstellen. Een cybersecurity incident is kostbaar voor een bedrijf, maar door de juiste maatregelen te nemen kun je de schade zo beperkt mogelijk houden.

ICT-beveiliging is niet een instelling of oplossing die je één keer inricht waar vervolgens jaren geen aandacht aan hoeft te worden besteed. Er moet met regelmaat naar worden gekeken en er moeten ook regelmatig aanpassingen worden gedaan. Cybercriminelen zitten niet stil. Jij als bedrijfseigenaar kunt ook niet achteroverleunen en afwachten. Ga met je ICT-partner regelmatig het gesprek aan met ICT-beveiliging als belangrijk onderwerp. Praat erover met je collega's en neem voldoende maatregelen. Want ook hier geldt: voorkomen is echt beter dan genezen.

HULP NODIG?

Bel ons op 0527-858585, kom bij ons langs op Ecopark 63 in Emmeloord of stuur een e-mail naar info@acfbentveld.nl.

Colofon

Dit is een uitgave van ACF Bentveld. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. ACF Bentveld kan daarvoor niet aansprakelijk worden gesteld.