Wat is ransomware?

Ransomware of gijzelsoftware is malware die gebruikt wordt om je bedrijf of organisatie te chanteren. Momenteel komen er twee soorten van ransomware voor.

de encrypteerder. Die gaat bepaalde bestanden of zelfs alle gegevens op je computer – of alle computers binnen je netwerk – versleutelen en ze zo onleesbaar maken.
De blokkeerder zorgt er dan weer voor dat je geen toegang meer hebt tot je gegevens door een digitale blokkade op te werpen.

Eens de malware zijn werk gedaan heeft, krijg je de vraag om een bepaald losgeld te betalen om je bestanden of computer(s) weer te ontgrendelen. Ga je niet in op die eis, dan worden alle gegevens definitief verwijderd.

Hoe werkt ransomware?
Ransomware werkt enkel als de malware op je computer of in je netwerk raakt. Dat gebeurt meestal via bestanden die als bijlage worden meegestuurd bij een e-mail of via een bezoek aan een besmette website.

Eens de malware op je computer geïnstalleerd is, gaat hij meteen gegevens encrypteren of de toegang blokkeren. Je gegevens worden dus niet (meteen) verwijderd, ze worden gewoon onbereikbaar gemaakt. Daarna wordt een proces gestart waarbij losgeld geëist wordt in ruil voor je gegevens. Je hebt meestal maar een beperkte periode om te reageren. Doe je dat niet, zal de malware je gegevens verwijderen.

Wie zit er achter ransomware?
Ransomware is het nieuwste favoriete speeltje van de georganiseerde misdaad. Zij zien er een eenvoudige en veilige manier in om snel geld te verdienen. Dat kan door ofwel zoveel mogelijk bedrijven in één keer te treffen, ofwel door zeer gericht op bepaalde bedrijven te gaan mikken en dan hoge sommen geld te eisen voor hun bedrijfskritische data.
De criminelen kiezen daarbij vaak bewust om het losgeld te ontvangen in bitcoins of een andere virtuele munteenheid om ervoor te zorgen dat het betalingsverkeer moeilijk of niet getraceerd kan worden.

Heb ik kans om besmet te worden met ransomware?
Ja. Elk bedrijf, ongeacht de omvang of de sector, loopt het risico om besmet te worden met ransomware.

Welke bescherming bestaat er tegen ransomware?
Traditionele antivirusoplossingen bieden weinig hulp tegen ransomware. Eens ransomware geïnstalleerd is, zijn antivirusoplossingen ook machteloos. Ze kunnen de malware dan wel nog verwijderen, maar je data ontcijferen of je toestel deblokkeren lukt niet.

Preventie is dan ook de beste oplossing

Wat moet je doen als je besmet bent met ransomware?

A. bidden
B. vloeken en tieren en de schuld steken op de vuile 'sossen'
C. uw advokaat bellen en uw websitebouwer dagvaarden
D. … ?

1. Koppel je toestel los van het internet en je netwerk
Op het moment dat je met ransomware besmet wordt, krijg je daar een melding van, terwijl in de achtergrond het gijzelen van bestanden doorgaat. Koppel daarom meteen je computer los van het netwerk, eventuele externe schijven en het internet. Dat kan door fysiek de kabels uit te trekken of de Wifi-verbinding af te sluiten. Op die manier heeft de ransomware hopelijk te weinig tijd om ook andere toestellen in je netwerk te besmetten of je bestanden in de cloud te gijzelen.

2. Probeer niet meteen een back-up terug te zetten
Probeer niet meteen een back-up terug te zetten. Zolang de ransomware zich op je toestel of in je netwerk bevindt, is de kans reëel dat dan ook de back-up besmet wordt.
Controleer - vanop een veilig toestel! - of bestanden in de cloud of eventuele cloud back-ups ook besmet zijn.

3. Betaal niet
Het antwoord op de belangrijkste vraag is duidelijk: niet betalen! Niet alleen omdat je meteen in het lijstje van makkelijke doelwitten komt, maar ook omdat je nooit zeker weet of je meteen een ontsleutelcode zal ontvangen. Noteer wel alle gegevens die je kan vinden van de hackers (een Bitcoin-adres bijvoorbeeld), want dit is de enige aanwijzing die je eventueel kan doorspelen aan de Computer Crime Unit.

4. Verwijder de ransomware en installeer back-ups
Er bestaan gespecialiseerde oplossingen om ransomware te verwijderen. Er wordt toch aangeraden om alle gegevens op je toestel volledig te verwijderen en je toestel volledig opnieuw te installeren. Enkel op die manier heb je 100% zekerheid dat er geen restant van de ransomware op je toestel achterblijft.
Eens je toestel opnieuw helemaal veilig is, kan je een externe back-up terugplaatsen.

Bescherm je bedrijf tegen ransomware in 6 stappen

Je kan nooit 100% uitsluiten dat je ooit besmet zal raken. Waar je wel voor kan zorgen is dat je het risico zoveel mogelijk beperkt én dat je voorbereid bent om in te grijpen als je toch slachtoffer wordt.

1. Zorg dat je medewerkers alert zijn

De meeste ransomware-besmettingen gebeuren via medewerkers die een bestand openen via een mail of een malafide website bezoeken. Vroeger kon je dat soort mails en websites van mijlenver onderscheiden dankzij krakkemikkig Nederlands, weinig aan de verbeelding overlatende bestandsnamen of rare URL's. Maar net als bij phishing gebeurt dat vandaag heel wat gerichter en professioneler.

Geef uw medewerkers een viertal basisregels mee en blijf erop hameren:

1. Open geen bijlages in mails van onbekenden
2. Wees wantrouwig tegenover bijlages in mails van bekenden
3. Kijk altijd naar de échte URL van een link voor je erop klikt
4. Geef nooit wachtwoorden door via telefoon, mail of chat

2. Zorg ervoor dat al je software up-to-date is

Ransomware maakt gebruik van lekken in software om zichzelf te installeren en zijn werk te doen. Wanneer je besturingssysteem of andere software verouderd is of niet meer ondersteund wordt, is de kans op dat soort lekken een flink stuk groter.

3. Installeer nieuwe security patches meteen

Hackers zijn er als de kippen bij om misbruik te maken van net ontdekte lekken. Wanneer een leverancier security patches uitbrengt om gekende problemen te verhelpen, zorg dan dat je die meteen installeert. Niet alleen voor je software, maar ook voor je server en je online oplossingen (ERP, CRM, CMS, enz.).

4. Zorg voor degelijke beveiligingsoplossingen

Een antiviruspakket mag dan geen echte oplossing bieden voor ransomware, goede beveiliging op meerdere niveaus is dat wel. Denk daarbij aan fysieke beveiliging, netwerkbeveiliging, beveiligde verbindingen, malwarebescherming, enz.

5. Beveilig toegang van op afstand

Via Remote Desktop toepassingen is het mogelijk om op afstand op bepaalde servers of computers in te loggen. Het is een toegang die door hackers steeds vaker gebruikt wordt om ransomware een bedrijf binnen te smokkelen. Ofwel door wachtwoorden te stelen, ofwel door via een brute force-aanval de meest zwakke wachtwoorden te kraken

6. Maak externe back-ups en zorg dat ze werken

Een goede back-up is de beste bescherming tegen ransomware. Zelfs als je toch besmet raakt, verlies je geen gegevens. Zorg er wel altijd voor dat het gaat om externe back-ups. Een back-up die gewoon mee in je netwerk zit, wordt logischerwijs ook mee besmet door ransomware. En wordt dus nutteloos.

Als je een externe back-up hebt, kan je gewoon de ransomware van je systeem verwijderen en daarna de back-up terugplaatsen. Twee dingen zijn daarbij belangrijk:
dat je weet welk Recovery Point Objective (RPO) je wil én dat je zeker bent dat je back-ups ook effectief werken.
Het Recovery Point Objective (RPO) bepaalt hoeveel gegevens je maximaal kwijt wil. Hoe vaak je voor een herstelpunt moet kiezen, met andere woorden. Als je maximaal 4 uur werk kwijt wil zijn, moet je om de 4 uur een veilige back-up maken van je gegevens. Zorg er ook voor dat je niet alleen de laatste back-up bewaard, maar ook nog een aantal eerdere versies. Zo ben je zeker dat je effectief kan teruggaan tot het moment voor de infectie.

Ransomware-as-a-Service… nog gevaarlijker dan ransomware

Ransomware blijkt een erg efficiënte vorm van afpersing te zijn voor de georganiseerde misdaad. En als een bepaalde techniek of oplossing om geld te verdienen succesvol is, mag je er donder op zeggen dat misdadigers die gaan optimaliseren en perfectioneren.
Dat betekent dat we ons binnen de kortste keren zullen mogen verwachten aan ransomware-as-a-service.

Het “as-a-service”-model wordt immers steeds populairder bij de georganiseerde misdaad. Hackers werken vandaag steeds vaker op bestelling. Ze leveren ransomware op maat en rekenen een commissie op de uiteindelijke opbrengst.
Dat is veiliger, want er is een tussenpersoon. Maar het is vooral een stuk winstgevender, want het succes van ransomware wordt bepaald door de kans dat die ook effectief geïnstalleerd raakt.

Zwakke plekken in je bedrijf?
Door het binnensmokkelen van ransomware uit te besteden aan een partij die jou goed kent (een zakelijke concurrent, een boze ex-werknemer, iemand die snel en makkelijk geld wil verdienen, een lokale misdadiger, enz.), wordt de kans op succes een stuk groter. Stel je maar even voor dat een werknemer een mailtje krijgt met een zogezegde flitsboete. Als het iemand is die regelmatig geflitst wordt, is kans groot dat hij de bijgevoegde “flitsfoto” opent.

Het succes van ransomware wordt vooral bepaald door de kennis over jouw bedrijf en jouw medewerkers. Door in te spelen op gekende zwakke plekken is de kans op succes een flink stuk groter. Hoe goed je je medewerkers ook voorlicht, hoe goed je beveiliging ook is.

Preventie: kleinste kost, grootste zekerheid

Kies daarom resoluut voor goede preventie. Het blijft de kleinste kost voor de grootste zekerheid. Want ransomware is een reëel risico voor elk bedrijf. En met ransomware-as-aservice wordt het écht maar een kwestie van tijd voor ook jij gegijzeld wordt…