26 APRIL 2021

WAT KOST EEN RANSOMWARE AANVAL?

Het afgelopen jaar heeft ransomware maar liefst meer dan €10,5 miljard gekost. Ruim 20.000 organisaties hebben een ransomware aanval gemeld. Dat is 40% meer dan het jaar daarvoor. Zorgwekkend is dat het steeds eenvoudiger is om ransomware aanvallen uit te voeren. Cybercriminelen kunnen zonder de nodige skills of enige vorm van kennis met behulp van softwareprogrammatuur ransomware aanvallen uitvoeren. Cybercriminelen kijken niet of een bedrijf interessant genoeg is om te hacken maar zij kijken naar openstaande deuren om een systeem binnen te dringen. Nóg zorgwekkender zijn de totale kosten die een ransomware aanval teweegbrengt. Naast de directe kosten zoals het betalen van losgeld, zijn er ook een hoop indirecte kosten. Denk aan de tijd die het u kost om weer volledig operationeel te zijn na een aanval of misschien wel erger: imagoschade.

Wij zetten de 6 financiële gevolgen voor u op een rij!

1. LOSGELD

U bent slachtoffer geworden van een ransomware aanval? Wat nu? Al uw bestanden zijn versleuteld en niet meer toegankelijk. Op uw computer verschijnt de melding dat uw computer gegijzeld is. Indien u uw computer weer toegankelijk wilt maken, dwingen cybercriminelen u tot een betaling. Vaak in de vorm van Bitcoins. Cybercriminelen kiezen voor een betaling in Bitcoins omdat Bitcoin betalingen geen sporen achterlaten. Een dure kwestie en criminelen hangen een deadline aan de betaling. Niet binnen 48 uur betaald? Dan blijven uw bestanden versleuteld... voor altijd!

Het bedrag wat de criminelen eisen noemen we losgeld. Losgeld is de meest zichtbare kostenpost bij een ransomware aanval en ook een directe kostenpost. Gemiddeld betaalden slachtoffers in 2020 ruim € 200.000 aan losgeld. Dat is twee keer zoveel als in 2019. Experts raden het betalen van losgeld af, het zou criminelen immers aanmoedigen om ransomware-aanvallen te blijven uitvoeren. Gemiddeld ligt een bedrijf ruim twee weken stil na een ransomware aanval. Wat zou u doen? Het kost de organisatie vaak meer geld om stil te staan dan het betalen van losgeld aan hackers. Want naast losgeld zijn er nog een hoop indirecte kosten.

“Gemiddeld betaalden slachtoffers in 2020 ruim €200.000 aan losgeld, twee keer zoveel als in 2019”

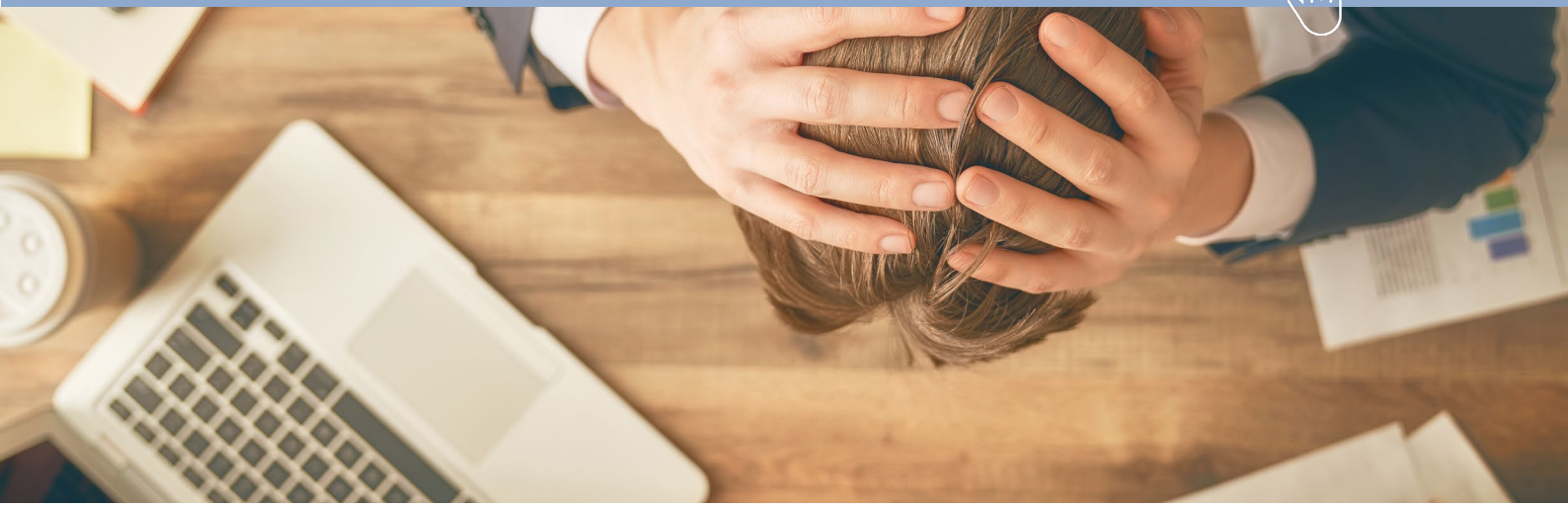
2. DOWNTIME

Met downtime bedoelen we de operationele verstoringen die veroorzaakt zijn door een ransomware aanval. Na een ransomware aanval ligt de complete bedrijfsvoering plat. Een ransomware aanval zorgt voor een gemiddelde downtime van 12 dagen! Reken maar uit wat het u kost als u 12 dagen geen omzet kunt maken... Downtime is daarom een enorme, indirecte kostenpost en vaak vele malen schadelijker dan directe kosten zoals losgeld.

Het bepalen van de exacte kosten van downtime is lastig, omdat downtime uiteenlopende effecten kan hebben bij bedrijven. Downtime kostte in het MKB naar schatting gemiddeld €130.000. Dit is een stijging van meer dan 200% ten opzichte van het gemiddelde van €43.200 in het jaar daarvoor! Dat bedrag is ruim 20 keer hoger dan het gemiddelde bedrag dat hackers van het MKB als losgeld eisten (€5.500).

Downtime kost dus veel geld. Ondanks dat het niet direct zichtbaar is, is een schatting snel gemaakt; **12 dagen geen omzet maar wel 12 dagen vaste lasten!** Daarom is een continuïteitsplan van belang. Heeft u goede afspraken met uw ICT partner? Weet u hoe lang het duurt voordat uw back-up is teruggezet? Weet u zeker dat u beschikt over de laatste antivirus technieken? Of kunt u deze vragen niet met zekerheid beantwoorden? Zorg voor goede afspraken met uw ICT partner rondom de continuïteit van uw bedrijf.

Wilt u een op maat gemaakt plan om uw bedrijfscontinuïteit te waarborgen? **Klik hier!**



3. IMAGOSCHADE

Een andere indirecte en bijzonder vervelende kostenpost; **imagoschade**! Slachtoffers van ransomware verliezen direct een deel of de gehele toegang tot systemen. Het bedienen van klanten stopt hier... klanten zullen ontevreden zijn en zullen opzoek gaan naar de oorzaak. Dit is het moment dat een organisatie moet laten weten dat zij slachtoffer zijn geworden van een ransomware aanval. De buitenwereld weet daardoor dat het criminelen gelukt is om uw organisatie binnen te dringen.

Dit soort publicatie resulteert vaak in een hoop ophef en afkeuring bij de klanten, partners en andere betrokkenen. Het dataherstel na een ransomware aanval is wellicht nog relatief snel te herstellen maar het terugwinnen van vertrouwen bij uw klanten is veel lastiger. Soms is de relatie zelfs niet meer te herstellen wanneer een klant weet dat zijn gegevens 'op straat' zijn komen te liggen.

Reputatieverlies heeft daarom direct negatieve gevolgen op het behoud van klanten maar ook op toekomstige klandizie of de eventuele beurswaarde van het bedrijf.

"Verzekeraars: imagoschade MKB kost €10.000 tot €100.000 per incident"

4. AANSPRAKELIJKHEID

Tot nu toe heeft u gelezen dat ransomware veel geld kost. **Downtime**, **ontevreden klanten** of zelfs nog erger: **vertrekkende klanten** en **imagoschade**. Een ander gevolg van ransomware is een faillissement. Want naast dat u langere tijd niet operationeel bent en klanten ziet vertrekken, kan het ook nog gebeuren dat u aansprakelijk wordt gesteld.

Volgens de privacywetgeving (AVG) moeten organisaties de persoonsgegevens die ze verwerken goed beveiligen. Als achteraf blijkt dat de beveiliging niet goed in orde was, kunnen gedupeerden een schadeclaim indienen. Ontevreden klanten kunnen juridische stappen zetten om compensatie op te eisen.

5. NEVENSCHADE

Een ander, indirect financieel gevolg van een ransomware aanval is nevenschade. Er ontstaat schade die niet direct is ontstaan uit de cyberaanval zelf maar wel te herleiden is naar de aanval. Zo is er het voorbeeld van een bedrijf dat geïnfecteerd raakten met ransomware, en dacht snel hersteld te zijn. De ICT partner kon de back-ups snel terugzetten, waardoor er geen losgeld betaald hoefden te worden en dankzij een continuïteitsplan was de downtime minimaal. Klanten hebben gelukkig niks gemerkt van de ransomware-aanval. De organisatie dacht er goed vanaf gekomen te zijn. Natuurlijk wel flink geschrokken maar de schade bleek beperkt te zijn. Helaas bleek na enkele weken dat de identiteitsbewijzen van de medewerkers waren gestolen en werden ingezet voor allerlei malafide zaken. De conclusie: vaak staan er meer gevoelige gegevens op onze computers dan dat we denken.

6. DATAVERLIES

Het allerergste van een ransomware aanval is het compleet verliezen van data. In sommige gevallen verliezen bedrijven de complete administratie of andere bedrijfskritische gegevens. Er zijn zelfs voorbeelden van bedrijven die failliet gingen door het verlies van data. Helaas is het betalen van het losgeldbedrag ook geen garantie op het veilig herstellen van de versleutelde data, soms zijn de bestanden niet meer terug te halen of gaan de hackers na uw betaling er vandoor met het losgeld. Het is daarom cruciaal voor uw bedrijf om zeker te zijn van een goede back-up. Uw ICT-partner kan u helpen met het instellen van goede back-ups. Wij adviseren u goede afspraken te maken over het maken van back-ups, wie deze controleert, hoe vaak back-ups gemaakt worden en hoe lang het duurt voordat u uw bestanden terug hebt.

Nog beter is het om naast het hebben van goede back-ups te kunnen beschikken over de juiste kennis waarmee aanvallen voorkomen worden want een ransomware-aanval gaat hoe dan ook gepaard met kosten!

Wij kunnen u helpen met het voorkomen van ransomware-aanvallen. Wij bieden hiervoor diverse oplossingen waaronder Security Awareness trainingen. Door middel van een interactief trainingsplatform maken wij uw medewerkers bewust van de risico's op het gebied van cybercriminaliteit.

Door het creëren van bewustwording vormt u sterkste verdediging tegen cybercriminaliteit. De Human Firewall voorkomt cyberaanvallen en houdt hackers buiten de deur!

Benieuwd hoe u hackers te slim af kunt zijn?

Klik hier voor een vrijblijvend advies op maat of neem contact met ons op.