Bedrijfscontinuïteit en cybercrime

RendementOnline

Door redactie FA Rendement

29 september 2021 | 6 minuten

Meer nog dan vroeger kunnen ondernemingen niet meer zonder slimme technologie. De techbedrijven zullen als grote winnaars uit de coronacrisis komen. Nog meer dan voorheen zullen zij een claim leggen op onze data. Als onze gegevens al niet gehackt worden door internetcriminelen... Zeker voor de financiële afdeling is cybercrime en datamanagement een van de grootste uitdagingen om te beheersen. Waar moet u op letten?

Als u en uw collega's het internet gebruiken om financiële zaken te delen of dashboards te presenteren, wisselt de computer continu informatie uit met andere partijen op het web. Gebeurt dit niet op een veilige manier, dan ligt een hack op de loer. En zo'n ongeluk zit in een klein hoekje.

Wat moet u in zo'n crisissituatie dan wel en niet doen? En beter nog: wat kunt u doen om niet in zo'n situatie terecht te komen zodat bedrijfscontinuïteit gegarandeerd is?

Betaal nooit losgeld bij een hack

Stelt u zich voor dat uw collega op maandagochtend facturen wil verwerken. Tot haar grote schrik krijgt zij een foutmelding en ze kan niet in het systeem. Zij meldt dit voorval bij de manager en die gaat op onderzoek uit. De manager opent zijn mail en ziet daar een losgeldbrief.

Het blijkt dat het systeem is gehackt en de hacker eist miljoenen euro's voor de gestolen persoonsgegevens die op de facturen stonden of anders zal het systeem geblokkeerd blijven en komen de persoonsgegevens op straat te liggen.

> **U heeft meer opties dan het betalen van losgeld**

Het advies is in deze situatie: betaal nooit losgeld. Er is namelijk geen garantie dat uw onderneming de controle over de systemen terugkrijgt nadat u de hacker het losgeld heeft betaald. Ook weerhoudt het de hacker er niet van om de persoonsgegevens te houden nadat uw onderneming hem betaald heeft en deze alsnog te verkopen.

Verder is het voor de hacker en zijn netwerk duidelijk dat u te chanteren bent als u het losgeld betaalt. Dit kan mogelijk leiden tot een herhaling in de toekomst.

Blokkeer de accounts

U heeft meer opties dan het betalen van losgeld. Als de bron van het lek bekend is, kunt u de accounts blokkeren die de dief gebruikt om uw onderneming te hacken. Om snel te ontdekken wat de bron van het lek is, moet u logbestanden aanmaken waarin bestandswijzigingen, transfers en eventueel de gebruikers bijgehouden worden.

Op die manier verzamelt u automatisch informatie, die u kunt raadplegen om de bron te ontdekken. Zolang u nog toegang heeft tot een deel van het systeem, kunt u ook de data verplaatsen naar een veiligere locatie of de indringer isoleren van buitenaf.

Leg de systemen stil

Als u geen toegang meer heeft tot het systeem, moet u alle systemen stilleggen. Samen met de procesverantwoordelijken kijkt u naar de waarschijnlijke impact van het uitvallen van een proces en wat de gevolgschade zou zijn. Dit doet u zowel tijdens een cyberaanval als na afloop als het niet tijdig

opgemerkt is.

De gevolgschade kan bestaan uit financiële schade, reputatieschade, schade aan werknemers, leveranciers en relaties, juridische gevolgen of een impact op strategische doelen van uw onderneming. Aan de hand van de informatie die u verkrijgt uit deze analyse stelt u een herstellingstijdsdoel vast en bepaalt u hoeveel gegevens er verloren mogen gaan. In deze situatie ligt uw onderneming stil. Dat wilt u natuurlijk voorkomen.

> ## Zet in goede tijden het thema cybercrime hoog op de agenda

Zet cybercrime op de agenda

Dus is het eerste wat u moet doen is het thema cybercrime in goede tijden hoog op de agenda zetten. Zeker nu al een aantal jaar op rij uit cijfers blijkt dat financieel-economische criminaliteit fors toeneemt. Daaronder valt bedrijfsspionage door bijvoorbeeld meekijken via netwerken, fraude en hacken.

Zorg ervoor dat de risicoanalyse of het bedrijfscontinuïteitsplan geen lijvig, onleesbaar of onbruikbaar document wordt. Dan is het up-to-date houden geen lastige en tijdrovende klus en bent u goed voorbereid op het onverwachte.

Belang van een veilig netwerk

Om te voorkomen dat u met hackers te maken krijgt, is een veilig netwerk noodzakelijk. Gelukkig wordt het belang van een goed beveiligd netwerk steeds duidelijker. Veel (grote) ondernemingen maken tegenwoordig gebruik van een gespecialiseerde zakelijke VPN-oplossing om het bedrijfsnetwerk te beveiligen.

Maar niet alle ondernemingen zijn groot genoeg om het afsluiten van een zakelijke VPN-verbinding betaalbaar of rendabel te maken. Maakt uw onderneming gebruik van een VPN-verbinding, dan wordt er een versleutelde verbinding gecreëerd tussen de (thuis)computer en de rest van het internet.

Een goede VPN-verbinding is dus van groot belang: een haperende internetconnectie brengt de bedrijfscontinuïteit van uw onderneming én een veilige gegevensuitwisseling in gevaar.

Verbinding thuis en VPN

Waar de meeste mensen al weten dat ze een verbinding met een openbaar netwerk moeten beveiligen met een VPN, geldt dat zeker ook voor de internetverbinding en wifi thuis. Deze verbinding thuis is namelijk niet standaard versleuteld en uw onderneming loopt daardoor het risico dat hackers data kunnen onderscheppen of malware kunnen injecteren. Ook is het risico groot dat hackers de internetverbinding afluisteren, waarbij ze bedrijfs- of persoonsgegevens buitmaken.

Instellingen voor toegangsrechten

Maar er zijn meer aandachtspunten dan alleen het netwerk. Als u files wilt delen die bedrijfsinformatie en persoonsgegevens bevatten, kies dan voor een service die end-to-endcodering biedt. Dit beschermt u tegen externe hackers en voorkomt ook dat de host uw gegevens kan bekijken.

Maak actief gebruik van de mogelijke instellingen voor toegangsrechten. Toegangsrechten kunnen een middel zijn om onbevoegde inzage of bewerking tegen te gaan. Het verschilt sterk per tool in hoeverre u als gebruiker controle heeft over autorisatie (verlenen van toegang) en authenticatie (vaststellen van de identiteit van een persoon).

> **Instrueer werknemers over de visie en principes over toegangsrechten**

Formele procedure

Ga uit van ‘minimale toegang’ door alleen de rechten toe te kennen die minimaal nodig zijn om aan het document gerelateerde taken uit te voeren. Maak zo min mogelijk gebruik van de optie ‘openbaar delen’. Dit betekent dat iedereen met de juiste link de bestanden kan verkrijgen, dus ook een hacker. Instrueer werknemers over de visie en principes over toegangsrechten van uw onderneming door deze vast te leggen in een formele instructie of procedure.

Maak regelmatig back-ups

Door te zorgen voor veilige cloudopslag die tevens regelmatig back-ups maakt, wordt uw onderneming ook beveiligd tegen bijvoorbeeld een ransomwareaanval. Als uw onderneming zowel lokaal als in de cloud regelmatig een back-up maakt is de kans klein dat werk kwijtraakt.

Vooral voor financiële rapporten waar meer mensen tegelijk aan werken is ‘real time editing’ in de cloudhandig. Dit voorkomt dat werknemers bestanden in het wilde weg rondsturen, waardoor problemen rond versiebeheer ontstaan.

Er is bij real time editing maar één juiste versie van een document. Dit betekent dus geen verkeerde samenvoegingen of dubbel werk meer. Elke werknemer van uw onderneming kan te allen tijde beschikken over de meest recente versie van een document. Dat is dus ook als een systeem er tijdelijk mee ophoudt. Een werknemer hoeft nooit meer helemaal opnieuw te beginnen als het systeem uitvalt, omdat hij alle documenten in de digitale cloud opslaat.

Zorg voor goede beveiliging van communicatie via e-mail

Doordat cybercriminelen steeds slimmere technieken gebruiken, is e-mail een belangrijk middel bij sociaal engineering. Via misleidende e-mails proberen de criminelen persoonlijke en bedrijfsgevoelige informatie los te peuteren. Uw bedrijfsgegevens zijn daardoor niet altijd veilig.

Ook lokmails om de gebruiker naar malafide websites te leiden, verschijnen regelmatig in de inbox. De volgende aandachtspunten kunnen van dienst zijn om dat te voorkomen:

- Zijn de e-mailprocedures geheel up-to-date?
- Is iedereen in de onderneming op de hoogte van de risico's en gevaren?
- Is er in de onderneming beleid rondom wel of niet delen van bepaalde gegevens via e-mail, en op welke manieren dat hoort te gebeuren?

Overweeg ProtonMail

Verstuurt uw onderneming veel informatie over de mail? Let dan goed op: e-mail is een risicovol kanaal. Maar er zijn privacyvriendelijke alternatieven te vinden. Een van de bekendste privacyvriendelijke aanbieders is ProtonMail.

Deze aanbieder is gevestigd in Zwitserland dat strenge privacywetten kent, waardoor het onmogelijk is dat privégegevens zonder pardon worden gedeeld met derden. Om een e-mailaccount aan te maken zijn geen persoonsgegevens nodig.

De onderneming houdt daarnaast ook geen logboeken met IP-adressen bij. Hackers kunnen dus onmogelijk e-mailadressen aan personen koppelen. Tevens hanteert de dienst standaard end-to-endencryptie. ProtonMail is open-source en gratis te downloaden.

Dit verdiepingsartikel is geschreven door Andrea Visser en Geoffrey van den Bergh van CRANIUM Nederland, e-mail: nl-info@cranium.eu

Dit is een artikel van de redactie van FA Rendement

FA Rendement is dé informatiebron voor administrateurs, boekhouders, controllers en andere financiële professionals. Wat is er veranderd op het gebied van financieel-administratieve wet- en regelgeving, en hoe kunt u als specialist deze informatie direct in uw dagelijkse werk toepassen? Daarnaast moet u op de hoogte zijn van onder meer de fiscaliteit, automatisering, de loon- en salarisadministratie, sociale voorzieningen, debiteurenbeheer en inkoop.

De onafhankelijke en ervaren redactie van FA Rendement zit bovenop het nieuws en vertelt u als eerste wat de ontwikkelingen zijn. Altijd in heldere taal en met een praktische insteek, zodat u de informatie direct kunt vertalen naar uw eigen werksituatie. FA Rendement is daarnaast multimediaal. De voor uw vakgebied relevante informatie verschijnt:

- ✓ dagelijks op het digitale platform Rendement Online, waar u onder meer het laatste nieuws, checklists, rekentools, maatwerkbrieven en verdiepingsartikelen tot uw beschikking heeft;
- ✓ wekelijks gebundeld in een e-mailnieuwsbrief;
- ✓ maandelijks in het vakblad FA Rendement, boordevol nieuws en achtergrondartikelen, digitaal en op de mat;
- ✓ tweemaandelijks in een handzaam themadossier: een pocketboekje dat iedere editie een complex onderwerp uitdiept.