TESORION

Een ransomware-aanval doorsta je alleen met een goede **recoverystrategie**. Die begint met een veilige back-up. Maar om de **schade te beperken** heb je een compleet bedrijfscontinuïteitsplan nodig.

Een ransomware-aanval kost gemiddeld zo'n 827 duizend euro. Veel bedrijven gaan er failliet door. En ze komen steeds vaker voor. Ransomware versleutelt je bestanden waardoor je er niet meer bij kunt. Vaak gaat het om een groot deel van je data. Ook back-ups worden tegenwoordig aangevallen door deze vorm van malware. Verwijderen van ransomware is werk voor experts. En zelfs als er losgeld wordt betaald, krijgen organisaties zelden meer dan een deel van hun data terug. De meeste zijn alles kwijt.

Op een dag gebeurt het: er vindt een ransomware-aanval plaats in jouw organisatie. Geen paniek, gelukkig heb je een goede back-up! Je IT'ers gaan meteen aan de slag om hem terug te zetten. Maar tot hun schrik zien ze dat er niets meer op de server staat: de aanvallers hebben de back-up gewist … Nu sta je echt met lege handen.

Maak een plan en test

Als er niet meer gewerkt kan worden, vallen de inkomsten weg maar de kosten niet. De directie moet dus echt zorgen voor een solide recovery-strategie.

Die begint met veilige back-ups die je ook echt kunt terugzetten. Ook voor je gegevens in de cloud, want de providers doen dat niet automatisch! Maar ook de beste backup is nooit up-to-date. En wat doe je als de back-up is gewist of aangetast?

Cloudopslag is geen garantie

Ook in de cloud zijn je data niet veilig voor een ransomware-aanval. Wil je een back-up? Dan moet je daar zelf werk van maken. De cloud-aanbieders doen dat niet automatisch. Neem de cloud dus op in je continuïteitsplan. Kijk goed wat de mogelijkheden zijn. Waar liggen de verantwoordelijkheden?

En ook hier geldt, net als bij een brandoefening: test geregeld of alles ook écht werkt zodat je kan blijven werken.

Beveilig je back-ups

Steeds vaker valt ransomware ook de back-up aan. In de praktijk blijkt dan ook dat je de back-up alleen kunt beschermen als hij in een geïsoleerde omgeving staat. Bovendien moet het onmogelijk zijn om hem te wijzigen. Dat moet je ook laten monitoren.

Een goed uitgangspunt is de 3-2-1-regel. Daarbij heb je drie versies van je bedrijfsdata: de werkversie en twee back-ups. Ze moeten op twee verschillende media staan, met één kopie op een andere fysieke locatie.

TESORION

Fokkerstraat 4
3833 LD Leusden

T: +31 33 456 3663
E: sales@tesorion.com

www.tesorion.com

Tesorion 7 checklist

De basis op orde. Waar begin je als jij je wilt wapenen tegen cybercriminelen?

1. Maak **medewerkers** weerbaar
We weten dat we niet op dat linkje moeten klikken. Ook weten we dat we niet zomaar geld moeten overmaken. Toch letten we niet altijd even goed op en trappen we er misschien allemaal wel eens in.

2. Splits je **netwerk** op in **compartimenten**
Segmenteer je netwerk. Zie het als brandwerende compartimenten. Wanneer er brand in een bepaald deel is kan je de branddeur sluiten en gaat niet het hele pand verloren.

3. Beveilig apparaten, e-mail en social media
We werken overal waar we willen. E-mail is in veel organisaties het belangrijkste communicatiemedium. Daarom wil je direct kunnen ingrijpen op apparaten die vreemd gedrag vertonen of zijn geïnfecteerd.

4. Versleutel belangrijke data
Data is het nieuwe goud, waarom beschermen we het dan niet net zo? Zorg dat je belangrijke data versleuteld bewaart, zodat wanneer data op straat komt te liggen deze niet toegankelijk is voor derden.

5. Maak betrouwbare **back-ups**
Het maken van back-ups lijkt een open deur. Back-ups zijn belangrijk, zo niet essentieel, om binnen afzienbare tijd (deels) verder te kunnen werken in geval van bijvoorbeeld ransomware.

6. Regel **toegang** tot bedrijfsmiddelen
Alle medewerkers hebben ongetwijfeld een eigen gebruikersnaam en wachtwoord. Waarschijnlijk heb je ook al sterke authenticatie ingeschakeld. Alleen een wachtwoord is niet veilig genoeg.

7. Houd je software en apparaten **up-to-date**
Overal zit tegenwoordig software in. Er zijn legio voorbeelden van software die kwetsbaarheden bevatten. Juist hierdoor kunnen cybercriminelen binnenkomen. Kortom: hoe ga jij om met deze updates?

24/7 actief
180+ experts
500+ klanten
1.000+ sensoren
4+ mln beschermde apparaten
100% Europees

ISO/IEC 27001 Information Security Management · NEN 7510 Information Security in Healthcare · EUROPOL The No More Ransom Project · EC3 European Cybercrime Centre