TESORION

Werken je mensen wel veilig? Denk aan al die **laptops** waar ze thuis, of **onderweg** of op een terras mee werken. Vaak vol met gevoelige data. Wat voor risico's loop je daardoor? En hoe kun je ze **effectief beveiligen**?

Je kunt je bedrijfsnetwerk zo veilig maken dat het niet meer gebruikt wordt. Er zijn in de cloud immers tal van alternatieven waarmee je wél fijn kunt communiceren of bestanden delen. Je moet je mensen dus een werkbare omgeving bieden. En zeker weten dat ze die ook echt gebruiken.

Dat is deels een kwestie van techniek. Met Endpoint Protection krijg je grip op die apparaten die altijd en overal bij jouw data kunnen. Zonder dat de gebruikers daar veel last van hebben. Maar even belangrijk is dat je mensen echt betrokken worden bij de inrichting van een veilige netwerkomgeving. Tesorion zorgt ervoor.

Jouw medewerker zit aan de keukentafel te werken. Er moet een presentatie naar iemand worden gestuurd. Helaas weigert het mailprogramma: het bestand is te groot om te mogen versturen via de zakelijke laptop. Geen probleem! Er zijn genoeg gratis tools in de cloud waar het wél mee kan. Maar … zijn jouw bedrijfsgegevens dan wel veilig?

Veilig bestanden delen

Belangrijkste data wil je veilig versturen, dus versleuteld en per e-mail. Iedereen weet immers dat gratis tools in de cloud nooit echt gratis zijn: je betaalt door vertrouwelijkheid en privacy op te geven. Maar wat als je tegen een bestandslimiet aanloopt? Heb je dan veilige alternatieven? Of zijn er toch goede mogelijkheden met e-mail?

Krijg controle met Endpoint Protection

Traditionele virusscanners zijn signature-based: ze herkennen alleen virussen die al zijn ontmaskerd. Endpoint Protection is veel intelligenter. Het kijkt naar de actieve processen van je applicaties, op zoek naar gedrag en technieken die kenmerkend zijn voor cybercriminelen. Zo kunnen zelfs zero-day-aanvallen worden opgemerkt.

Endpoint Protection maakt ook overzichten van geïnstalleerde software. Je krijgt het overzicht dat je nodig hebt om risico's meteen te signaleren. Plus de tools om dreigingen uit te schakelen.

Bescherm alle apparaten

Bedrijfsnetwerken bestaan tegenwoordig vooral uit laptops. Je mensen werken er altijd en overal op. Als ze een tool nodig hebben, gaan ze even googelen.

Met alle risico's van dien: hackers en malware proberen vaak via 'normale' tools binnen te komen. En ze worden steeds slimmer. De laptops moeten dus een beveiliging krijgen die ook nieuwe gevaren meteen herkent en aanpakt. Zonder dat je mensen daarbij gehinderd worden.

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

EUROPOL The No More Ransom Project EC3 European Cybercrime Centre