TESORION

Veiligheid zonder zekerheid bestaat niet. Daarom geldt voor je netwerkbeveiliging: **never trust, always verify**. Dat klinkt niet aardig. Je vertrouwt je medewerkers toch? Maar mensen kunnen fouten maken en je wilt ze tegen zichzelf beschermen.

Zero Trust betekent dat een apparaat of account alleen het internet op kan als dat nodig is. En dat het dan ook goed beveiligd is. Wat heb je daarvoor nodig? Allereerst een cybersecurity-plan. Verder een goede firewall, netwerksegmentatie en 24-uursbewaking door een security operations center.

Tegenwoordig is een bedrijfsnetwerk een enorme kluwen van webapplicaties, mobiele apparaten en koppelingen met derden. Die kunnen allemaal contact maken met het internet. Hoe beveilig je al die openingen? Zonder dat het werk onmogelijk wordt gemaakt? Kortom: hoe combineer je veiligheid met vrijheid.

Next generation firewall

Beveiliging begint met een goed slot op je voordeur. Met een firewall houdt je ongewenst verkeer buiten. Next generation firewalls bieden extra bescherming. Mits goed ingericht herkennen ze gebruikers, applicaties, hackers en andere bedreigingen. Denk ook aan het uitschakelen van services en poorten die niet gebruikt worden. En multifactor-authenticatie voor accounts die van buitenaf toegankelijk zijn.

Netwerksegmentatie

Extra veiligheid krijg je door je netwerk op te delen in segmenten waardoor een binnengedrongen hacker al snel voor een volgende dichte deur komt te staan. De beveiliging kan verschillen per segment. Er zijn diverse mogelijkheden om de segmenten te scheiden. Denk aan een air-gapped netwerk of firewalls of access control lists (ACL's). Bij 'dynamische segmentering' werken de scheidingen als een soort brand-deuren, die sluiten zodra een alarm afgaat. Zo combineer je veiligheid met vrijheid.

Cybersecurity-plan

Wat zijn je bedrijfsgeheimen? En wie kan erbij? Voor een beveiligingsstrategie moet je eerst je data in kaart brengen. Dan kun je vervolgens bepalen hoeveel beveiliging er nodig is voor de verschillende soorten data. 'Kroonjuwelen' horen in een digitale brandkast, maar sommige andere data moet juist makkelijk toegankelijk zijn.

Je hebt dus een cybersecurity-plan nodig. Met een classificatie van je data en de bijbehorende risico's. Daaraan koppel je dan steeds de best passende beveiliging. Zorgvuldig maar ook pragmatisch.

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