TESORION

Versleutelen: wat en hoe? Waar staat je data? In de **cloud** bij Microsoft of Google, maar ook op de **laptops** van je **medewerkers**. Dat laatste leidt vaak tot een datalek.

Hoe groot is die kans? Dat hangt af van het apparaat, de plaats en de tijd. Met risicoprofielen van je medewerkers bepaal je hoe zwaar de beveiliging moet zijn. Dan kun je ook kijken of, en hoe zwaar de gegevens versleuteld moeten worden. Gebruik goede encryptiesoftware. Zelfs met de laptop in handen kan de crimineel er dan niet bij.

Bijna dagelijks horen we in de media over datalekken. Niet alleen bij allerhande bedrijven, maar ook bij overheden, verzekeraars en andere organisaties die met privacygevoelige gegevens werken. Het lijkt dus bijna gewoon. Maar zo voelt het helemaal niet voor de organisaties met een datalek. Uiteraard vanwege de reputatieschade. Maar ook omdat de Autoriteit Persoonsgegevens er boetes voor oplegt: inmiddels al voor meer dan vijf miljoen euro.

Onderweg naar een klant stopt je medewerker bij een wegrestaurant. Na de lunch merkt hij dat zijn tas weg is. Met zijn laptop! En alle gevoelige gegevens die hij daarop bewaart … Wat gaat daarmee gebeuren? Hoe kan je een datalek voorkomen? Door gegevens te versleutelen hou je ze veilig. Zelfs als de laptop verdwenen is.

Beperk de schade

Wat doe je als het ergste gebeurt? Na een cyberaanval moet je eerst een totaalbeeld krijgen van de situatie. Van welke cyberschade is er sprake? Wat voor maatregelen kun je treffen om erger te voorkomen? En hoe krijg je je organisatie snel weer op de been?

Goede versleuteling maakt in zo'n situatie een wereld van verschil. Zelfs al is de laptop weg, je data zijn toch veilig. Evenals je reputatie.

Pragmatische hulp

Tesorion staat klaar met raad en daad. Onze experts kunnen je helpen om de meest geschikte encryptie-oplossing te selecteren. Dat doen ze pragmatisch, met oog voor jouw specifieke situatie. Ze zijn sparring-partner bij de classificatie van je gegevens en het maken van risicoprofielen. Bovendien leren ze je mensen om veilig te werken. En als het dan toch misloopt, staan ze meteen klaar om de brand te helpen blussen.

Breng je data in kaart

Data is voor veel organisaties het belangrijkste bedrijfskapitaal. Denk daarbij aan klant -en projectdata, persoonlijke gegevens of data met specifieke, al dan niet gevoelige, informatie. Het is belangrijk dat je weet wat je moet beschermen.

Waar begin je dan? Kijk dan eerst waar je data staat, en maak vervolgens een goede classificatie. Daarbij bepaal je hoeveel bescherming er nodig is. Koppel daar risicoprofielen van je medewerkers aan.
Denk eraan: bij een datalek ben je zelf eindverantwoordelijk.

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