TESORION

Je wilt dat er verantwoordelijk wordt omgegaan met je **data** en **systemen**. Dus er mogen alleen mensen bij die daar recht op hebben. Maar dat moet je dan wel goed regelen. Niet alleen de **rechten** maar ook de **toegang**.

Veel mensen zijn slordig met hun persoonlijke toegangsrechten. Maar ook organisaties rommelen vaak maar wat aan: ze hebben geen overzicht van wie bij welke data en systemen kan. Soms hebben ze de toegangsrechten gekoppeld aan functies, maar ook dat is geen garantie dat alles goed gaat.

De beste benadering is tweeledig. Enerzijds role-based access control. Dan kan iedereen bij de informatie die hij nodig heeft, en niet bij de rest. En anderzijds: automatiseer de toegang, zodat het makkelijk wordt om veilig te werken.

Het gebeurt maar al te vaak. Een medewerker heeft geen toegang op een deel van het netwerk waar hij bij moet. Geen nood: een collega biedt een helpende hand en laat hem even via zijn eigen account werken. We vertrouwen elkaar toch? Maar achteraf heeft die collega spijt: er blijken er fouten in de spreadsheet te zijn gekomen.

Maak toegang simpel

Als je de toegang tot systemen te ingewikkeld maakt, wordt het werken bemoeilijkt. Dus gaan mensen de regels omzeilen. Ze loggen in voor collega's, zodat die kunnen werken op hun account. Lange wachtwoorden worden met een post-it op het beeldscherm geplakt.

Zorg dus dat toegang simpel wordt. Veilig werken moet de logische keuze zijn.

Hou alle touwtjes in handen

Simpele toegang is mogelijk door automatisering van processen. Diezelfde automatisering zorgt ook dat jij de centrale controle houdt. Op elk moment kun je bepalen wie waarbij kan. Of zorgen dat er snel nieuwe wachtwoorden komen.
Als een medewerker vertrekt, hoef je je ook niet af te vragen of hij nog wachtwoorden heeft van systemen: je hoeft alleen zijn account te beëindigen. Dit alles doe je op basis van een heldere verdeling van taken en bevoegdheden. Ook daarmee kun je hackers het leven zuur maken.

Maak een roadmap

Breng de rollen van je mensen in kaart met een roadmap voor identiteits- en toegangs-management. Zodat mensen uitsluitend toegang hebben tot data waar zij ook volgens hun rol bij moeten kunnen.

Elke medewerker moet snel en gemakkelijk bij de informatie kunnen die hij of zij nodig heeft. Maar niet méér dan dat! Denk niet alleen aan bedrijfsvertrouwelijke data, maar ook aan wetgeving zoals de privacyregels. De basis is dus het principle of least privilege. Daar moet je je interne processen op inrichten.

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