Tips & advies

11 manieren om uw bedrijf beter te beveiligen

Met een handvol tips zet u nog geen volledige beveiliging op. Maar dit lijstje vormt wel een goede start en vat voor u de voornaamste aandachtspunten samen.

1. Weet waar de risico's zitten

Als u niet weet waar de risico's in uw netwerk zitten, kunt u ze onmogelijk onder controle houden. Een volledige risicoanalyse brengt uw bedrijfskritische processen in kaart, uw data, software, toestellen, netwerken, gebruikers enz. Als u gewonnen bent voor Bring Your Own Device (BYOD), dan is een inventaris van alle toestellen onontbeerlijk. Bij BYOD mogen medewerkers hun eigen laptop, smartphone of tablet gebruiken op het werk.

2. Bouw meerdere beveiligingsmechanismen in

Een goed beveiligingssysteem hangt nooit af van één product of verdedigingsmechanisme. Meervoudige verdediging verhoogt de effectiviteit van uw beveiliging.

3. Stem uw beveiliging af op uw bedrijfsprocessen

Een goede beveiliging is altijd gebaseerd op een goede kennis van de bedrijfsprocessen. Zo voorkomt u dat uw beveiliging de goede werking van uw bedrijf in het gedrang brengt.

4. Kies een vertrouwenspartner voor uw beveiliging

De beveiliging van computers en computernetwerken is een erg complex domein. Alleen grote bedrijven kunnen zich een eigen veiligheidsexpert veroorloven. Andere ondernemingen kiezen beter voor een externe partner. Vertrouwen is bij de keuze van zo'n partner essentieel. Ga na welke certificaten hij kan voorleggen en of hij objectief en onafhankelijk over veiligheidsproducten kan oordelen. Belangrijke certificaten, die garant staan voor de kwaliteit van uw partner, zijn onder meer CISSP, CISA en CEHA.

5. Stel een veiligheidsbeleid op

Welke toepassingen en URL's mogen uw werknemers wel en niet gebruiken? Misschien wilt u het gebruik van sociale media toelaten, maar enkel tijdens de middag? Dit soort afspraken kunt u vastleggen in een veiligheidsbeleid, dat elke werknemer vervolgens ondertekent. Wanneer u van op afstand een toestel met ongeoorloofde software of data wilt kunnen wissen, vermeldt u die mogelijkheid ook in uw beleidsdocument.

6. Maak medewerkers bewust van de risico's

Veiligheid is geen louter technisch probleem, maar een menselijk probleem. Leer medewerkers dat ze beter niet voor alle applicaties hetzelfde wachtwoord gebruiken. Wijs hen op de gevaren van downloaden, social engineering, mobiele toestellen enz.

7. Geef medewerkers enkel toegang tot data die ze nodig hebben

Een medewerker van de marketingafdeling heeft geen gegevens van de personeelsdienst nodig. Die data moeten voor hem dan ook ontoegankelijk blijven. Door bedrijfsgegevens te classificeren, kunt u fijnmazig filteren. Er kan bepaald worden wie de eigenaar van de gegevens is, wie ze mag lezen, wie ze mag aanpassen enz.

8. Blijf evalueren en testen

Blijf uw beveiliging evalueren en testen. Gedetailleerde beveiligingsonderzoeken, zoals pentesten (penetration tests), zijn niet voor elke onderneming haalbaar. Maar ook kleinere bedrijven kunnen op regelmatige tijdstippen hun beveiliging aan een test onderwerpen. Brengt een test zwakheden aan het licht, neem dan de gepaste maatregelen.

9. Stel een back-upplan op

Geen enkele beveiliging is 100% waterdicht. Hou er dus rekening mee dat ook in een goed beveiligde omgeving problemen kunnen opduiken. Weet wat uw bedrijfskritische toepassingen zijn, wat er gebeurt als ze uitvallen, en neem maatregelen zodat u in een dergelijke situatie toch kunt blijven werken.

10. Installeer een systeem voor logbeheer

Logs stellen u in staat om na te gaan waar zich problemen hebben voorgedaan en wat hun impact was. Hebt u geen logs, dan kunt u uit incidenten geen lessen trekken.

11. Stel een communicatieplan op

Hoe gaat uw bedrijf intern en extern communiceren als zich veiligheidsproblemen voordoen? Wie gaat u inlichten, wanneer en hoe? Als u over de nodige logs beschikt, kunt u correct en open over de kwestie communiceren. Dat is altijd beter dan trachten de problemen te verzwijgen of te minimaliseren.

Meer informatie

- **Bekijk onze beveiligingsoplossingen op www.telenet.be/security**
- **Bel 015 36 47 47 voor een afspraak met onze beveiligingsexperten**