

Eerste stappen naar een digitaal veiliger bedrijf

Elk bedrijf werkt tegenwoordig digitaal. Met computers op kantoor, op laptops en smartphones die ook buiten kantoor gebruikt kunnen worden en steeds vaker via het internet ('de cloud') waar ook gegevens worden opgeslagen. Daarnaast hebben veel bedrijven een website waarmee ze in contact staan met klanten. Op veel websites kunnen klanten ook hun bestelling doen

Digitaal verzamelt een bedrijf dus veel: klantgegevens, financiële informatie, bedrijfskritische documenten zoals prijslijsten, personeelsdossiers. En steeds vaker gaan processen in het bedrijf ook digitaal: betalingen, bestellingen van klanten en bij de toeleverancier en het aansturen van productie. En net zoals je je bedrijfsbelangen beschermt met een kluis en een inbraakalarm zo neem je ook maatregelen om je bedrijf digitaal te beschermen tegen onder andere hackers, virussen en gegevensdiefstal.

Beveiliging regel je niet eenmalig om er daarna nooit meer naar om te kijken, je moet er altijd aandacht voor hebben. Maar je kunt wel klein beginnen met een aantal basisstappen. Bespreek het ook eens met je ICT-partner of een beveiligingsexpert

- **Ken je eigen ICT-omgeving:** weet welke hardware en software je hebt en welke informatie belangrijk is om te beschermen
- **Spreek met medewerkers over het belang van beveiliging:** zorg dat ze weten hoe zorgvuldig jouw bedrijf met gegevens wil omgaan.
- **Beveilig alle computers en het computernetwerk:** installeer antivirusprogramma's en een firewall. Kijk voor meer praktische tips op [Digibewust](#).
- **Beveilig het draadloze netwerk:** voorkom dat onbevoegden op je netwerk kunnen komen en zorg voor een sterke beveiliging (WPA2) en een sterk wachtwoord.
- **Zorg ervoor dat software en hardware altijd bijgewerkt zijn:** installeer updates meteen als je daarvan melding krijgt, zodat zwakke plekken gedicht worden. Op www.waarschuwingsdienst.nl vind je extra informatie over urgente updates
- **Maak regelmatig een back-up en bewaar deze buiten het kantoor:** voorkom dat gegevens kwijt raken.
- **Organiseer trainingen voor medewerkers:** getrainde en geïnformeerde medewerkers zullen zorgvuldiger omgaan met informatie. Je bedrijf loopt dus minder risico als je personeel beter op de hoogte is.
- **Zorg voor een sterk wachtwoord:** een sterk wachtwoord is minder snel te kraken en dus veiliger. Zorg dat iedere medewerker in het bedrijf een sterk wachtwoord heeft.
- **Doe altijd aangifte bij de politie als je bedrijf slachtoffer is geworden van cybercrime,** bijvoorbeeld wanneer gevoelige informatie is gestolen door internetoplichters.
- **Schakel een externe partij in wanneer je zelf niet de benodigde kennis en vaardigheden in huis hebt** om de beveiliging van computers en netwerk te garanderen. Vraag bij collega's, leveranciers en andere partners na bij wie zij hun ICT-ondersteuning inkopen, wellicht kunnen zij je uit ervaring tips geven bij het zoeken naar advies en begeleiding. Kijk op beschermjebedrijf.nl meer tips voor het vinden van een ICT-leverancier.