

Hoe digitaal veilig is jouw bedrijf?

10 vragen voor je ICT-leverancier



Veilig ondernemen.
Daar maken we
ons sterk voor.

PVO / Noord-
Nederland



10 vragen voor je ICT-leverancier

- 1. Zijn de laatste beveiligingsupdates geïnstalleerd op alle programma's?**
Door te werken met de laatste versie loop je de minste kans op virussen en hacks. Deze maken namelijk gebruik van kwetsbaarheden in oudere versies van programma's. Het is van belang om alle updates direct uit te voeren.
- 2. Worden er regelmatig back-ups gemaakt en wordt er gecontroleerd of deze geslaagd zijn?**
Vraag zelf eens een restore aan van een bestand van een dag eerder ter controle.
- 3. Wordt er gebruikgemaakt van een virusscanner en firewall?**
Virusscanners en firewalls kunnen een deel van de hacks voorkomen. Installeer altijd de updates om te voorkomen dat nieuwe virussen een kans krijgen.
- 4. Zijn er logfiles beschikbaar (van o.a. de firewall)?**
Hieraan kun je zien wie wanneer heeft ingelogd. Ook kun je zien of jouw netwerk aangevallen wordt door hackers en op welke wijze dit heeft kunnen plaatsvinden.
- 5. Worden de medewerkers getraind in cybersecurity?**
Organisatorische maatregelen zijn minstens zo belangrijk als technische maatregelen om cybercrime te voorkomen. Het team is zo sterk als de zwakste schakel. Er hoeft maar één medewerker op een verkeerde link te klikken en de kans bestaat dat het hele bedrijf stil komt te liggen.
- 6. Worden mijn data versleuteld opgeslagen en kunnen persoonsgegevens indien gewenst verwijderd worden?**
Versleutelde data zijn geheel onleesbaar zonder de juiste sleutel, dus als iemand jouw bestanden steelt kunnen ze er niets mee doen. Het veilig opslaan en eventueel verwijderen van persoonsgegevens is ook van belang in het kader van de Algemene Verordening Gegevensbescherming (AVG).
- 7. Hoe vaak worden security testen gedaan en wat gebeurt er met de resultaten?**
- 8. Zijn er in het verleden security incidenten geweest?**
- 9. Waar worden mijn data opgeslagen en hoe is dit beveiligd?**
Er zijn landen buiten de EU die geen waarborg bieden voor een passend beschermingsniveau. Data kan zo in verkeerde handen vallen.
- 10. Wat wordt er gedaan zodra mijn bedrijf toch gehackt wordt?**
Maak vooraf afspraken over de inzet van jouw ICT-leverancier en ga er niet (zomaar) vanuit dat zij de hack oplossen.