QSN ABR WHITE PAPER

STAPPENPLAN
INFORMATIEBEVEILIGINGSBEWUSTZIJN

De volgende stappen geven u een handvat om het informatiebeveiligingsbewustzijn binnen uw organisatie in kaart te brengen en te verhogen:

1

Inventariseer alle bedrijfsmiddelen

Maak een overzicht van alle bedrijfsmiddelen die u in gebruik heeft en die invloed kunnen hebben op informatiebeveiliging. Denk hierbij heel breed: software, hardware (computers, printers, USB sticks, harddisks, smartphones etc.), sleutels, toegangspasjes, medewerkers.

2

Breng de risico's in kaart

Om te bepalen welke acties of maatregelen u zou moeten nemen om informatiebeveiliging te verhogen, is het van belang dat u bepaalt welke informatiebeveiligingsrisico's voor uw organisatie van belang zijn. Gebruik hierbij als leidraad het overzicht van bedrijfsmiddelen.

3 Neem maatregelen

Neem afhankelijk van de risico's maatregelen om de risico's te beperken:

- Fysieke beveiliging (b.v. sloten op deuren en kasten, brandbeveiliging, bezoekersregistratie, etc)
- Beveiliging van apparatuur (b.v. periodiek onderhoud, hergebruik en vernietiging van apparatuur, omgang met usb/telefoon/tablets/laptop, etc)
- Beveiliging van systemen (b.v. firewalls, toegangsbeveiliging, softwarebeveiligingsupdates, etc)
- Beveiliging van gegevens (b.v. clear desk & clear screen, gebruikersrechten, ect)
- Communicatie en medewerkersbewustzijn (b.v introductie, beleid/reglement)

De volgende maatregelen zijn van toepassing op alle organisaties, ongeacht de risico's:

- Fysieke beveiliging: Sluit kasten met persoonsgegevens af, bepaal wie toegang heeft en leg dit vast in een sleutelplan.
- Beveiliging van apparatuur: Stel richtlijnen op hoe u om wilt gaan met mobiele gegevensdragers als telefoons, tablets, usb-sticks, etc. Hoe kunt u deze gegevensdragers beveiligen? Wilt u een wachtwoord afdwingen? Wilt u encryptie doorvoeren? Wilt u het gebruik beperken?
- Beveiliging van systemen: Zorg ervoor dat op systemen te allen tijde de juiste softwarebeveiligingsupdates geïnstalleerd zijn, zodat de systemen goed beveiligd zijn tegen hackers en malware.
- Beveiliging van gegevens:
  - Stel een autorisatiematrix op om inzichtelijk te maken welke medewerker toegang heeft tot welke informatie.
  - Zorg voor een papierversnipperaar of een afsluitbare papierbak.
  - Zorg voor veilige wachtwoorden.
- Communicatie en medewerkersbewustzijn: Stel een beleid/(huis)reglement op waarin staat aangegeven hoe u wilt dat uw medewerkers met informatiebeveiliging omgaan.

4 Check regelmatig uw maatregelen

Check vervolgens minimaal 1 keer per jaar of de maatregelen voldoende zijn geïmplementeerd en of de maatregelen de risico's nog steeds voldoende beperken. De ontwikkelingen op het gebied van digitale informatie gaan erg snel, wellicht zijn er nieuwe risico's bijgekomen.

5 Leer van beveiligingsincidenten

Registreer situaties waarbij de informatiebeveiliging geschonden is of mogelijk geschonden had kunnen worden. Leer van deze incidenten om uw informatiebeveiligingsbewustzijn verder te verhogen.