Hulp bij beveiligingsplan

Tegen diefstal heb je een inbraakalarm, geld bewaar je in een brandzekere kluis en procedures bepalen wat medewerkers op het kassasysteem mgoen. Daarnaast heb je ongetwijfeld nog allerlei andere maatregelen getroffen om jouw bedrijfsbelangen te beschermen. De basis van deze beveiliging is dat je in kaart hebt waar jouw risico's liggen en hoe hoe goede maatregelen deze risico's verkleinen.

Wanneer het gaat om ICT en (digitale) informatie, is het principe hetzelfde. Ieder bedrijf is anders, dus ook in de digitale wereld bestaat geen uniform beveiligingsplan. Maak een risicoanalyse van de belangrijkste bedrijfsprocessen en van de informatie die de kern voor jouw organisatie vormt. De kracht van de bescherming van jouw organisatie ligt in een aanpak op drie vlakken tegelijk.

1. Plan (richtlijnen/beleid)
Welke bedrijfsprocessen en informatie zijn essentieel? Waar liggen de risico's en bedreigingen? Welke gegevens bewaar je(digitaal)? Maak een plan hoe je de bedrijfsprocessen en de benodigde informatie en (privacygevoelige) gegevens gaat beschermen. Dit hoeft niet altijd uitgebreid te zijn, het kunnen ook hoofdpunten zijn op één a4.

Wat moet er in ieder geval in het plan van aanpak:
- Beschrijf welke informatie en welke systemen beschermd moeten worden
- Wees duidelijk over de risico's die je probeert te vermijden.
- Beschrijf hoe bedreigingen te voorkomen zijn en opgespoord kunnen worden (bijvoorbeeld met grotere bewustwording onder medewerkers)
- Beschrijf hoe gereageerd moet worden op bedreigingen of incidenten (wie moet ingelicht worden?)
- Maak duidelijk wie verantwoordelijk is voor de beveiligingsrichtlijnen en het uitvoeren en controleren van procedures.
- Leg ook vast welke taken en verantwoordelijkheden medewerkers hebben in beveiliging.
- Leg de informatierichtlijnen vast (wie mag bij welke informatie, mag iedereen alles inzien?).
- Beschrijf welke hoe hardware en software up-to-date en beveiligd moeten zijn.
- Stel een tijdschema op voor de uitvoering en evaluatie van het plan.

Vraag een ICT-partner om de noodzakelijke begeleiding. Het wiel is al een keer uitgevonden, daar hoef je jouw kostbare tijd niet in te steken. Zorg er wel voor dat je zelf de keuzes voor het beleid maakt. Het is immers jouw onderneming en het beleid moet vanuit jezelf komen.

Kijk voor een volledig overzicht ook in de Code voor Informatiebeveiliging.

2. Procedure
Vertaal het beleid naar heldere procedures en eventuele technische middelen die daarbij horen. Procedures werken alleen als deze bekend zijn en ook worden uitgevoerd.. Zorg er daarom voor dat alle relevante procedures bekend zijn bij de juiste medewerkers en fris de kennis regelmatig op.

3. Controle
Controleer regelmatig of het beleid en de procedures ook echt worden uitgevoerd. Als dat te veel tijd kost, kun je dit controleproces natuurlijk ook automatiseren, zodat je slechts een overzicht krijgt van de gevallen die wel jouw aandacht nodig hebben. Herzie en update het plan zes tot twaalf maanden na implementatie of na grote veranderingen in het bedrijf.

Tips over het voorbereiden en implementeren van de beveiligingsrichtlijnen

- Wees duidelijk over de risico's die je probeert te vermijden.
- Raadpleeg je medewerkers over de voorgestelde richtlijnen en vraag om hun input.
- Het is belangrijk om een evenwicht te hebben tussen praktijk en controle. Onthoud dat vertrouwen even belangrijk is als supervisie.
- Zet de nieuwe richtlijnen in personeelshandboeken, medewerkerintroductie, intranet sites etc.
- Richtlijnen moeten verband houden met je disciplinaire procedures, werknemerscontracten en ander beleid zoals non-discriminatie.
- Zorg ervoor dat iedereen de richtlijnen te zien krijgt zodra het klaar is.
- Zorg ervoor dat de richtlijnen beschikbaar zijn om te raadplegen.
- Moedig feedback van medewerkers aan. Als de richtlijnen zo restrictief zijn dat het onuitvoerbaar wordt, zullen ze eerder omzeild worden dan dat er aan wordt voldaan – het is beter om te weten waar de schoen knelt.
- Iemand in het bedrijf moet verantwoordelijk zijn voor de implementatie en controle van de richtlijnen.