Voorbeeld overzicht beheersmaatregelen

In 2017 heeft de Haagse Hogeschool onderzoek gedaan naar cyberveiligheid in samenwerking met MKB-Nederland, VNO-NCW en enkele brancheorganisaties waaronder Adfiz. Daarin is ook gekeken naar relevante beleidsmaatregelen. Hieronder zie je dit overzicht en de mate waarin ondernemers deze maatregelen hadden getroffen.

- ☑ Er is een schriftelijke weergaven van de huidige ICT/infrastructuur (netwerk/computersystemen)
- ☑ Er zijn scenario's ontwikkeld waarin is beschreven hoe het bedrijf slachtoffer kan worden van cybercrime (bijv. een ex-medewerker die inlogt op het systeem)
- ☑ Er is een protocol opgesteld waarin is beschreven hoe te handelen bij cybercrime
- ☑ Er is informatiebeveiligingsbeleid aanwezig
- ☑ Werknemers worden bewust gemaakt van online risico's
- ☑ Werknemers hebben geleerd om geen e-mail van potentieel onbetrouwbare afzenders te openen
- ☑ Werknemers hebben geleerd goed op te letten bij het doen van online betalingen (Bijv. op 's' achter http of op het slotje in de browser)
- ☑ Werknemers hebben geleerd om geen gevoelige informatie op internet te verstrekken
- ☑ Werknemers moeten verschillende sterke wachtwoorden voor online accounts gebruiken (combinatie van minstens 8 cijfers en letters)
- ☑ Er worden regelmatig (veiligheids-)audits uitgevoerd
- ☑ Er zijn (schriftelijk) regels opgesteld over het gebruik van ICT voor privé-doeleinden
- ☑ Er zijn (schriftelijk) regels opgesteld voor het doen van online betalingen
- ☑ Er zijn (schriftelijk) regels opgesteld over het omgaan met vertrouwelijke informatie zoals persoonsgegevens van u, uw medewerkers, gasten en/of klanten
- ☑ Er zijn (schriftelijk) regels opgesteld over het openen van onbekende bestanden (zoals attachments bij e-mail)
- ☑ Er zijn (schriftelijk) regels opgesteld over het (op verzoek) afgeven van bedrijfsgegevens
- ☑ Het is verplicht wachtwoorden regelmatig te wijzigen