Brandoefening Digitale Veiligheid

Samen Digitaal Veilig

Wis je dat…

De kans op een brand bij een bedrijf is **1** op **8000**

De kans op een inbraak bij een bedrijf is **1** op **250**

De kans op een cyberaanval bij een bedrijf is **1** op **5**

Bron: Rabobank

Voorkomen is beter dan genezen!

Je denkt misschien dat digitale criminaliteit alleen grote bedrijven treft. Niets is minder waar. Juist kleine en middelgrote bedrijven zijn een geliefd doelwit omdat ze hun beveiliging vaak minder goed hebben geregeld.

Elke dag worden ondernemers getroffen door digitale criminelen die inbreken. Dan komt het moment dat je ineens je klanten niet meer te woord kunt staan, factureren onmogelijk is en je het planningssysteem niet meer in kunt. De financiële impact is groot: je mist omzet en je moet kosten maken om alles weer in orde te brengen. De gevolgen zijn groot en voelbaar binnen je hele bedrijf, niet alleen financieel maar ook emotioneel. Een heleboel slapeloze nachten die je had kunnen voorkomen.

Het is helaas onmogelijk om alle cyberaanvallen te voorkomen. Wel is het verstandig om te oefenen met je medewerkers zodat iedereen zich bewust is van de risico's.

"Door cyberaanvallen na te bootsen, kan je je beter voorbereiden. Een digitale brandoefening."

Dit document geeft praktische tips hoe je een Brandoefening Digitale Veiligheid kunt uitvoeren.

Handleiding Brandoefening Digitale Veiligheid

Stap 1 Simulatie

Plan een datum waarop je de Brandoefening Digitale Veiligheid wil doen. Prik bijvoorbeeld een moment in de ochtend, wanneer de medewerkers hun computer of laptop opstarten. Bespreek met je IT-partij of het mogelijk is een beeld te tonen met een tekst zoals “U bent gehackt” lees hier meer… Als dat niet mogelijk is, dan kun je ook een mail versturen of iets plaatsen op het intranet van je organisatie.

Uiteraard wordt bij het klikken op “lees meer…” uitgelegd dat het bedrijf niet echt gehackt is, maar dat er vandaag een Brandoefening Digitale Veiligheid is. Dit is de start van de landering van het platform Samen Digitaal Veilig. Een online platform waar medewerkers aan de hand van 8 video’s de eerste stappen kunnen zetten op het gebied van digitale veiligheid.

Stap 2 Uitrol SDV

De beheerder van het SDV platform heeft alle medewerkers vooraf opgevoerd en verstuurt via het platform een uitnodiging naar alle medewerkers om deel te nemen. Een account aanmaken kan via Bouwend Nederland – Samen Digitaal Veilig

Stap 3 Meeting

Een aantal medewerkers is vooraf uitgenodigd om op deze dag een brandoefening te bespreken. Ze komen erachter dat het om een digitale brandoefening gaat. Samen stellen ze een handleiding op met verschillende afspraken in het geval er een echte cyberaanval is. Een van de medewerkers kan dit document ook voorbereiden.

Een voorbeeld van onderdelen die in de handleiding kunnen worden opgenomen zijn:

1. Overzichten

- Een overzicht met de sleutelfiguren binnen de organisatie + telefoonnummers
- Een overzicht van belangrijke IT-leveranciers (en verzekering) + telefoonnummers
- Een overzicht van telefoonnummers van de hulpdiensten (waaronder politie en meldpunten)

2. Incident response

Een term die wordt gebruikt om het proces te beschrijven waarmee je een cyberincident afhandelt. Doel is de schade, hersteltijd en -kosten zoveel mogelijk beperken. Beschrijf welke stappen je moet nemen. Bijvoorbeeld medewerkers informeren over wat ze wel of juist niet moeten doen. Informeren van IT-leverancier(s), terugroepen van hardware en uitrollen van nieuwe software. Of het terugzetten van een back-up in een beperkte afgesloten omgeving. Bespreek deze acties ook met de betrokken leveranciers.

2. Samenwerking

Bij een grootschalig cyberincident is het onvermijdelijk dat medewerkers, afdelingen en locaties met elkaar moeten samenwerken. Zorg dat je elkaar kan bereiken, bijvoorbeeld door een WhatsApp-groep aan te maken met de naam “Team Digitale Veiligheid”. Heb je een cyberverzekering, neem dan contact op met de verzekeraar.

3. Communicatie

De besluitvorming ligt bij het management. Bij cyberincidenten moet het management echter vaak expertise inschakelen van specialisten. Het oefenen op communicatie binnen een organisatie is daarom ook fundamenteel: hoe lopen de communicatielijnen? Is het management voldoende op de hoogte van de ernst van een cyberincident en de te nemen stappen? Hoe communiceren we naar onze stakeholders? Hoe gaan we om met media, zonder onze reputatie te schaden? Hoe bereiken we onze klanten?

Door crisissituaties na te spelen maak je de hele organisatie bewust van de digitale dreigingen, de eigen rol, verantwoordelijkheden en risico’s/consequenties van het eigen handelen. Door medewerkers toegang te geven tot het SDV platform, kunnen ze zelf met de instructievideo’s aan de slag.

Tip: Print de Brandoefening Digitale Veiligheid altijd uit!