DIGITALE VEILIGHEID

Checklist

In de wereld waarin we steeds meer digitaal werken, is het van belang dat we zorgvuldig omgaan met **onze data**. Wat kun je als bedrijf doen om te voorkomen dat je een **makkelijk doelwit** bent voor **hackers** en hoe kun je **beveiligingsrisico's** beperken?

Neem verantwoordelijkheid en onderschat het niet
"Het overkomt mij niet" en "zo'n vaart zal het niet lopen", is in deze tijd van toenemende cybercrime zeer onverstandig. Ben je bewust van de gevaren en neem verantwoordelijkheid.

Creëer ook bewustwording in je organisatie
Zorg voor routine in veilig gedrag. Zorg dat veilig gedrag routine wordt door het de waardering te geven die het verdient en door consequenties te verbinden aan onveilig gedrag. Wijs elkaar regelmatig op risico's en mogelijke consequenties.

Laat jezelf hacken
Door jezelf te laten hacken, bijvoorbeeld door het inhuren van ethische hackers, komen risico's aan het licht. Daarna kun je maatregelen nemen en veilig gedrag dieper in je organisatie verankeren.

Ben op de hoogte van de wetgeving
Weet hoe te handelen wanneer er persoonsgegevens op straat liggen waar jij vanuit je bedrijfsvoering verantwoordelijk voor bent. De Meldplicht Datalekken verplicht je om dit binnen 72 uur te melden!
https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

Zorg voor de juiste technische oplossingen
Het is een open deur, maar het is wel essentieel dat het technische fundament van je organisatie staat als een huis. Dat zorgt voor de juiste preventieve maatregelen en geeft daardoor rust. Als er iets gebeurt zorgen deze maatregelen ervoor dat je gemakkelijker een interventie kan plegen. Heb je niet de juiste preventieve maatregelen getroffen, dan zijn de risico's vaak niet te overzien. Het gevolg is dat je (digitale) bedrijfsvoering totaal onderuit gaat, waardoor je de gangbare werkzaamheden niet kunt uitvoeren.

Wees bewust waar je je data in the cloud opslaat
Wanneer je data buiten Nederland opslaat in een datacenter, gelden ook de wetten van het desbetreffende land. Ken je die wet en weet je welke rechten/plichten daarbij horen? Zo niet, zorg dat je weet waar je aan toe bent. De datacenters van KPN staan allemaal in Nederland en vallen daarom per definitie onder het Nederlandse rechtssysteem.

Voer updates regelmatig uit
Het gebeurt vaak bij bedrijven dat updates niet adequaat worden doorgevoerd. Toch is dit zeer belangrijk. 99% Van alle hacks komt voort uit het niet up to date zijn van je software. Updates zijn er niet voor niks: daarin worden onder andere (potentiële) beveiligingslekken gedicht.

Verander eens per maand je wachtwoord
Het is niet prettig om vaak je wachtwoord te wijzigen. Toch is het een noodzaak voor een veilige online aanwezigheid. Als een onbekende je wachtwoord heeft, hebben ze onbeperkt toegang tot alles waar jij toegang toe hebt. Kies sterke wachtwoorden, schrijf ze niet op papiertjes en zet ze in een wachtwoordenprogramma als je ze niet kunt onthouden. Je kunt er ook voor kiezen om via 2-weg-authenticatie in te loggen. Dit is een eenvoudige toepassing waarbij je inlogt met je vaste gebruikersnaam en wachtwoord en vervolgens een unieke code ontvangt, bijvoorbeeld via sms.

Laat USB's, telefoons en laptops niet slingeren
Een USB kwijt? Een datalek. Een telefoon gestolen? Weer een datalek. Dat heeft dus consequenties voor de Meldplicht Datalekken. Maar belangrijker nog: daarmee kan een belangrijk deel van je bedrijfsvoering op straat liggen. Het meest verstandige is geen USB sticks meer gebruiken en telefoons voorzien van een Mobile Device Manager. Hiermee kun je de telefoon op afstand afsluiten voor ongewenst gebruik.

Schaam je niet en sta open voor advies
Er worden duizenden hacks per dag gepleegd en het overkomt steeds meer bedrijven. Schakel professionele hulp in om de schade te beperken. Je bent niet de eerste en niet de enige. Voorkom reputatieschade achteraf. Je kunt een aanval, mits je op de juiste manier handelt, omzetten in de versterking van je bedrijfsvoering. Dit kan alleen door er open over te praten met deskundige partijen die jou in staat stellen om je digitale bedrijfsvoering op een hoger niveau te beveiligen.

Advies of vragen?

VTM

Excellence
platina business partner kpn