DIGITALE VEILIGHEID

Veiligheidsrisico's in relatie tot de Wet bescherming persoonsgegevens en intellectueel eigendom

Digitale veiligheidsrisico's ontstaan vanuit een datalek. Een datalek is een opening in een intern netwerk dat eigendom is van een rechtspersoon. De opening in het netwerk maakt het voor anderen mogelijk om informatie van buitenaf in een netwerk te plaatsen en informatie in het netwerk te bewerken.

Bij een datalek is het bovendien vaak mogelijk om informatie vanuit het interne netwerk naar buiten te brengen. Met alle mogelijke gevolgen van dien. Een datalek kan ook van binnenuit ontstaan als medewerkers onzorgvuldig handelen of bewust informatie naar buiten brengen. Fysiek of digitaal.

Voor datalekken geldt een meldplicht bij het meldloket van de autoriteit van de persoonsgegevens. Hiervan is al sprake als een medewerker zijn of haar eigen mobiele telefoon verliest, waar bijvoorbeeld zakelijke e-mail op staat. Voor meer informatie over de Wet bescherming persoonsgegevens zie: autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens

Bij een datalek loopt je onderneming de volgende 3 risico's:

1. Een financiële boete oplopend tot € 820.000,- of 10% van de netto jaaromzet vanwege bestuurdersaansprakelijkheid
2. Het verliezen van intellectueel eigendom of andere gevoelige informatie die gestolen kan worden door (cyber)criminelen

EXtreem veilig

MaXimaal beschikbaar

3. Chantage door (cyber)criminelen die dreigen delen van een digitale werkomgeving plat te leggen of gevoelige informatie naar buiten te brengen
4. Imagoschade omdat publiekelijk blijkt dat jouw organisatie haar digitale veiligheid niet goed geregeld heeft

Hoe maak je veilig online werken mogelijk?

Je wilt veilig online kunnen werken en datalekken voorkomen. Maak daarom afspraken met elkaar en richt processen in die ervoor zorgen dat richtlijnen nageleefd worden. Neem dus organisatorische maatregelen die vastgelegd worden in reglementen.

Voorbeelden hiervan zijn bewerkersovereenkomsten die je met je toeleveranciers van ICT-toepassingen afsluit. Maar zeker ook met je collega's in je bedrijf. Omdat met name zij gegevens raadplegen, bewerken, opslaan op verschillende dragers en verspreiden.

Technologische hulpmiddelen

Je kunt er tegenwoordig niet omheen om technologische toepassingen in te zetten. Je hebt een degelijke back-up voorziening nodig en het liefst eentje buiten de deur. Een back-up voorziening die ervoor zorgt dat je op ieder gewenst moment cruciale gegevens terug kunt plaatsen in het geval van een datalek.

Je moet ervoor zorgen dat je besturingssystemen en firmware up-to-date zijn. Dit omdat veruit de meeste aanvallen een netwerk binnenkomen via systemen die niet up-to-date zijn. Daarom is het belangrijk dat je weet welke ICT-applicaties en websites medewerkers gebruiken. Want alleen dan kun je vaststellen of er toepassingen tussen zitten, die het netwerk kwetsbaar maken voor een datalek.

Ook zul je het vaste en mobiele internetverkeer moeten analyseren om kwetsbaarheden in het netwerk adequaat tegen te kunnen gaan. Al met al zaken waar technologische oplossingen een uitkomst bieden. Want als mens is dat allemaal niet bij te houden.

Voorkomen van kwetsbaarheden door de inzet van ICT-toepassingen

1. Management van internetverkeer
Onbetrouwbare data en toepassingen zoals virussen komen meestal via het internet een netwerk binnen. Daarom kun je het beste kwetsbaarheden afweren voordat ze een intern netwerk binnendringen. Dat doe je door internetverkeer te scannen en onbetrouwbare data en functionaliteiten zoals virussen tijdig af te

weren. Hetzelfde geldt natuurlijk voor data die ongewenst van binnenuit naar buiten wordt gezonden.

2. Management van werkstations

Als onbetrouwbare data en functionaliteiten zoals een virus een intern netwerk binnendringt, dan gebeurt dit meestal via een werkstation. Na de beveiliging van het internetverkeer is het daarom essentieel om ieder werkstation in je organisatie van de juiste beveiligingsmaatregelen te voorzien.

3. Management van servers

Als onbetrouwbare data en functionaliteiten zoals een virus voorbij het werkstation is gekomen, dan verspreidt de kwetsbaarheid zich verder via de servers vanaf waar je werkt. Na de beveiliging van het werkstation is het dus cruciaal om alle servers van de juiste veiligheidsmaatregelen te voorzien.

Managementrapportage voor data security

Als klant van BSU ontvang je standaard managementrapportages over onze data security dienstverlening. We doen dit zodat jij kunt aantonen welke maatregelen je treft op het gebied van data security. En dat je je beschermt in relatie tot de Wet bescherming persoonsgegevens.

Wil je weten of de digitale veiligheid van jouw bedrijf in orde is? Laat ons een gratis security scan doen. Neem contact met ons op via 0413 24 33 33.