FLYER TIPS & TRICKS
OMGAAN MET DATALEKKEN

Omgaan met datalekken: voorkom veelvoorkomende datalekken met onze praktische tips!

Iedere ondernemer kan te maken krijgen met datalekken. Heeft u weleens een e-mail naar de verkeerde ontvanger gezonden? Of bent u ooit een usb-stick of losse documenten kwijtgeraakt? Deze situaties kunnen datalekken opleveren. In deze flyer zullen een aantal concrete voorbeelden van datalekken genoemd worden met praktische handvatten voor hoe u dient te handelen bij een datalek. Hiermee voorkomt u mogelijk hoge boetes!

VOORBEELDEN VAN DATALEKKEN

❖ (Per ongeluk) een e-mail zenden naar de verkeerde ontvanger.

Het verzenden van persoonsgegevens naar de verkeerde ontvanger omvatte in het eerste kwartaal van 2017 45% van datalekken. De kans is dus groot dat u ooit te maken zult krijgen met een e-mail die verzonden wordt naar een verkeerde ontvanger of een e-mail waarin persoonsgegevens worden gedeeld zonder toestemming van de betrokken persoon. Het is van belang dat u weet hoe u moet handelen in deze situaties. Het is niet mogelijk om dit volledig te voorkomen, maar u kunt wel bepaalde maatregelen nemen:

- Zet e-mailadressen in bcc en niet in cc. Ontvangers mogen elkaars e-mailadressen in beginsel niet zien!
- Als u bijlagen meestuurt met een e-mail, zet dan indien mogelijk een link in de e-mail naar het bestand met een beperkte geldigheidsduur. In de bijlage kunt u ook een watermerk opnemen met de details van de afzender en ontvanger, zodat sneller duidelijk is voor onbevoegden dat de e-mail en bijlagen niet voor hun bestemd is.
- Neem een disclaimer in uw e-mail op, waarin u de niet-beoogde ontvanger verzoekt de e-mail niet verder te lezen, te vernietigen en te verwijderen van de computersystemen en u te waarschuwen ten aanzien van de verkeerde verzending.

Er zal bij het verzenden van een e-mail aan de verkeerde ontvanger snel sprake zijn van een datalek. Als gevoelige persoonsgegevens in de e-mail stonden (bijvoorbeeld medische gegevens), moet dit gemeld worden bij de Autoriteit Persoonsgegevens. Heeft u achteraf bevestiging van de onrechtmatige ontvanger dat de e-mail is verwijderd en de persoonsgegevens niet verwerkt zijn, dan kan een melding bij de betrokkene achterwege blijven. Zorg ervoor dat u een intern protocol heeft voor deze situatie.

❖ Hacken, phishen, malware

Hoewel hacken, phishen en malware 'slechts' 7% van datalekken waren in het eerste kwartaal van 2017, kunnen de gevolgen hiervan groot zijn voor ondernemingen. Uw server of computernetwerk zal nooit 100% veilig zijn. Het is dus niet te voorkomen dat u ooit gehackt zou kunnen worden.

Er zijn manieren om uw bedrijfsgegevens zo goed als mogelijk te beveiligen:

- Biedt uw website slechts aan in https-mode en maak gebruik van een firewall.
- Zorg voor adequate wachtwoorden die regelmatig gewijzigd worden, beperk de toegang tot de server en beperk de mogelijkheid persoonsgegevens op te slaan.
- Sluit een goede verwerkersovereenkomst met internetbureaus of providers die onderhoud verrichten.

Bij hacken en malware zal sprake zijn van een datalek. U dient dit te melden bij de Autoriteit Persoonsgegevens als het lekken van de gegevens een risico oplevert voor betrokkenen. Bij een grootschalige hack is het raadzaam om dit te melden bij betrokkenen.

❖ Datalek bij een webshop

Steeds meer mensen maken gebruik van webshops. Dit betekent dan ook dat steeds meer mensen hun persoonsgegevens op internet invullen bij bestellingen. Als u een webshop heeft, is het van belang dat u ten minste voldoende maatregelen neemt om datalekken te voorkomen. De volgende maatregelen kunt u nemen:

- Zorg voor een goede beveiliging.
- Vermeld onderin op uw website niet welke software u gebruikt. Hiermee kunnen hackers zwakke plekken vinden. Verwijder ook oude versies van uw website na het installeren van nieuwe software.
- Maak een back-up van uw website.

Mocht het gebeuren dat een hacker de persoonsgegevens van uw klanten in handen krijgt, dan zal sprake zijn een datalek. Als het gaat om een grootschalige hack, waarbij de persoonsgegevens van vele klanten gelekt worden, dient u dit te melden bij de Autoriteit Persoonsgegevens en bij betrokkenen.