WHITEPAPER

GEGEVENS BESCHERMEN LASTIG? NIET MET DEZE TIPS!

Financiële gegevens, klant accountgegevens, gegevens in een multomap in de kast op kantoor of medische gegevens in een patiëntendossier. Al deze gegevens zijn te herleiden tot personen. Maar niet iedereen hoeft alles van iedereen te weten. Daarom moeten zowel mensen als deze gegevens beschermd worden en is vanaf 25 mei 2018 de Algemene Verordening Gegevensbescherming (AVG) van kracht.

WHITEPAPER

GEGEVENS BESCHERMEN LASTIG? NIET MET DEZE TIPS!

De AVG heeft betrekking op het beschermen van persoonsgegevens tegen misbruik door onbevoegden. Welke gegevens dit zijn, is voor ieder bedrijf anders. Een groot deel van deze gegevens betreft digitale data. Ter ondersteuning op uw voorbereiding op de AVG geven we u in deze whitepaper een aantal tips vanuit onze expertise als ICT-adviseur.

Bescherming van uw digitale data

De invoering van de AVG heeft consequenties voor uw bedrijf. Want ook uw bedrijf houdt zich bezig met het verwerken van gegevens. Gegevens die betrekking hebben op de privacy van uw klanten, personeel of voor de veiligheid van uw organisatie. Deze gegevens worden voortdurend verplaatst. Binnen uw eigen netwerk, tussen externe netwerken en in de cloud. U moet deze gegevens dus goed beschermen en ervoor zorgen dat er geen inbreuk op uw data plaatsvindt.

Een eenvoudige manier om uw digitale data minimaal te beschermen en een basis te leggen tegen misbruik door derden is het versleutelen van de data en te controleren wie er toegang heeft tot deze data.

Versleutelen en bewaken

De data waarmee u werkt bevinden zich zowel binnen als buiten uw organisatie. Alleen de poort beveiligen door middel van bijvoorbeeld een firewall is niet voldoende. Niet alleen de toegang, maar ook de data zelf moeten ontoegankelijk zijn voor een kwaadwillende.

Het beveiligingen van uw data d.m.v. encryptie is een makkelijke manier om uw gegevens te beschermen. Encryptie houdt in dat uw data worden versleuteld. Met andere woorden, er is een sleutel nodig om toegang tot de data te krijgen.

WAAR DIENT U OP TE LETTEN?

De BrainCheck is o.a. opgesteld aan de hand van fouten die bedrijven regelmatig maken. Deze punten zijn van belang voor ieder bedrijf, ongeacht grootte of branche. Met de opkomst van cybercriminaliteit is men geneigd om, gedreven door paniek en publieke opinie, de nadruk hier op te leggen. Echter, voor een bedrijf dat zijn algehele digitale veiligheid goed op orde wil hebben, is het van belang deze top 10 punt voor punt door te lopen.

Het doel van encryptie is om ervoor te zorgen dat wanneer gegevens worden uitgewisseld, dit op een veilige manier gebeurt. Is bijvoorbeeld de verbinding niet veilig, dan is het nog steeds mogelijk om (privacy)gevoelige data veilig te versturen omdat deze versleuteld zijn. U wilt daarom, voordat u tot encryptie toepast, eerst in kaart brengen welke data u wilt versleutelen. En leg dat dan meteen langs de AVG-lat.

Wanneer u eenmaal overgaat tot encryptie is het van belang dat u inzicht heeft in de locatie van de data die u wilt versleutelen en op welk niveau. Dat kan in een fysiek netwerk zijn of in de cloud. U kunt een volledige harde schijf versleutelen of bestanden op applicatieniveau.

Wees zuinig op de sleutel

Bedenk zelf maar hoe u met uw huissleutel omgaat. Deze bewaakt u met uw leven. Hetzelfde geldt voor het versleutelen van data. Wanneer u de sleutel onder de deurmat legt, heeft het weinig zin de deur op slot te doen. De sleutel kan het beste in een virtuele kluis bewaard worden. Deze staat los van de data, op (externe) hardware. Deze kluis is uiteraard alleen toegankelijk voor bevoegden en de sleutel moet regelmatig veranderd worden om misbruik te voorkomen. Tot slot heeft u een platform nodig om de encryptie te beheren. Hier adviseren wij u graag over.

Beperk de toegang

Is de deur naar de data eenmaal dichtgetimmerd en zijn de gegevens versleuteld, dan is het slim om zicht te houden op welke personen er op welke wijze toegang hebben tot de data. U doet dat door het instellen van tweestapverificatie, een extra stap in het verifiëren van de toegang tot de gegevens.

Dit betekent dat er naast de eerste stap in het verificatieproces (de combinatie van een statisch wachtwoord met een gebruikersnaam) nog een tweede stap is: die van een (dynamisch) wachtwoord of code op een ander veilig apparaat. Stel dat uw wachtwoord gehackt wordt, dan heeft de hacker nog steeds geen toegang tot uw gegevens.

Manage uw wachtwoorden

Gebruik, om de kans op het achterhalen van uw wachtwoorden zo klein mogelijk te maken, een wachtwoordmanager. Het gebruik van een wachtwoordmanager is veiliger dan hetzelfde wachtwoord gebruiken voor verschillende diensten, zoals recente datalekken hebben aangetoond. Een wachtwoordmanager maakt het makkelijk om wachtwoorden te beheren, aan te maken en te wijzigen en lost het probleem op dat u voor elke site een apart wachtwoord moet bedenken. Wat van groot belang is, is de keuze van een hoofdwachtwoord. Wilt u meer weten over wachtwoordmanagement? Neem dan contact met ons op.

Bovenstaande tips zijn slechts een greep uit de vele maatregelen die u kunt nemen om goed beslagen ten ijs te komen in mei. AVG-specialist zijn wij niet, ICT-specialist wel. Wilt u meer weten over welke maatregelen u kunt nemen om uw organisatie digitaal zo veilig mogelijk in te richten, doe dan de BrainCheck.

Doe de BrainCheck

Om u inzicht te geven in uw huidige niveau van digitale beveiliging en veiligheid, heeft BrainCap de BrainCheck ontwikkeld. De BrainCheck behandelt een 10-tal punten die essentieel zijn met betrekking tot ICT-beveiliging en de veiligheid van de gegevens binnen een bedrijf en bestaat uit de volgende lijst van aandachtspunten:

- Back-up policy
- Gebruikersrechten
- Patchmanagement
- Wachtwoordpolicy
- Cloud Bestandsdeling en Synchronisatie
- Awareness
- Toegang van buitenaf
- Endpoint beveiliging
- Versleuteling van data
- Security Network Monitoring

Wat dit allemaal inhoudt? Dat leggen we graag aan u uit. Nadat deze cruciale aandachtspunten besproken zijn, volgt er een rapportage met uw score op het gebied van digitale beveiliging en een aanbeveling. Met dit rapport kunt u zelf beslissen hoe u verdere invulling geeft aan een veilig ICT-beleid, waar we u vakkundig over kunnen adviseren. **Neem contact met ons op via services@braincap.nl of bel ons op 088-275 48 00.**

BRAINCAP
SOFTWARE & SERVICES