AP ontvangt 7000 klachten en tips over vermeende privacyschendingen

De Autoriteit Persoonsgegevens heeft sinds de invoering van de Algemene verordening gegevensbescherming (AVG) op 25 mei van dit jaar meer dan 7000 tips en klachten over vermeende privacyschendingen ontvangen. De vragenlijn van de toezichthouder werd zo'n tienduizend keer gebeld, zo melden de Telegraaf en Trouw.

Bij een aantal van de klachten heeft de Autoriteit Persoonsgegevens een onderzoek naar mogelijke overtredingen ingesteld. Om hoeveel onderzoeken het gaat wil de toezichthouder niet kenbaar maken. Wel laat de AP weten dat het alle klachten en tips aan het analyseren is, om zo te kijken of er knelpunten zijn die prioriteit horen te krijgen. Volgend jaar januari volgt de eerste officiële evaluatie van de AVG.

In de AVG is een meldplicht datalekken opgenomen. Wanneer een datalek een risico vormt voor de rechten en vrijheden van een individu zijn organisaties verplicht om de betreffende toezichthouder binnen 72 uur na ontdekking van het lek te informeren. Eerder deze maand werd bekend dat alle Europese privacytoezichthouders sinds de introductie van de AVG in totaal 18.000 meldingen van datalekken hebben ontvangen. Vorig jaar werden er alleen bij de Autoriteit Persoonsgegevens 10.000 datalekken gerapporteerd.
Bron: www.security.nl

Even voorstellen.....

Hallo,
Mijn naam is Paul Scheper (40), bij Metis vervul ik de rollen van Security Officer, Kwaliteitscoördinator en Functionaris Gegevensbescherming.

Medio 2017 heb ik de opleiding tot Functionaris Gegevensbescherming gevolgd. Dit was, en is, een prima aanvulling op het werk waar ik mij reeds mee bezig hield; informatiebeveiliging. Het werkveld van de AVG is een uitdagende gebleken, iets waar ik me erg prettig bij voel.

Ik ben van mening dat de AVG niet iets is wat je over de muur kan gooien. Het is een proces waarbij steeds gewerkt wordt aan het verbeteren van de bescherming van persoonsgegevens. Daarbij moet er vooral praktisch en pragmatisch worden gekeken naar de inrichting. Dit houdt voor mij in dat ik actief betrokken ben bij mijn klant en de inrichting graag samen doe, de klant moet er tenslotte mee werken.

Naast de tijd die ik besteed aan mijn dochters, vrouw en Metis heb ik niet heel veel tijd over. De tijd die er over is vul ik graag met kijken van een filmpje en sporten.

Zo kunt u uw data simpel beveiligen!

De AVG vertelt ons (draagt ons op) om maatregelen te nemen om de beveiliging van systemen te waarborgen en/of te versterken. In vaktermen wordt dit hardening genoemd, oftewel, gij zult maatregelen treffen om uw systemen en dus de betrokkenen te beschermen. Dit zijn dan veelal technische en daarnaast ook organisatorische maatregelen.

Uit eigen onderzoek blijkt dat het MKB, en dan vooral de kleine ondernemers, niet of nauwelijks met beveiliging van gegevens bezig zijn, het kost immers tijd en geld. Toegegeven, het kan best wat tijd vergen, maar het hoeft niet altijd duur te zijn. Sterker nog, we kunnen zelf enkele basale beveiligingsmaatregelen nemen om in ieder geval de meest voorkomende kwetsbaarheden het hoofd te bieden, namelijk:

- zorg dat uw systeem regelmatig (automatisch) de beveiligingsupdates binnenhaalt;
- gebruik encryptie, wat noodzakelijk is bij gegevensverwerking;
- antivirus, er zijn diverse gratis alternatieven om u te beschermen tegen virussen.

Bovenstaand is uitgelegd hoe u "endpoint" beveiliging kunt initiëren, maar hoe kunt u organisatorische maatregelen nemen? Onderstaand noemen we enkele organisatorische maatregelen.

- Hanteer een wachtwoordbeleid en zorg dat iedereen zich hier aan houdt.
    - Wijzig het wachtwoord regelmatig (eens in de 60 – 90 dagen).
    - Een wachtwoord is persoonlijk.
    - Een wachtwoord moet geen volgnummer hebben.
    - Een wachtwoord moet een mate van complexiteit bevatten.
- E-mail beleid (bewustwording)
    - Aanbiedingen in e-mails die te mooi lijken te zijn om waar te zijn, zijn inderdaad vaak te mooi om waar te zijn. Nog steeds is phishing de meest voorkomende aanval!
    - E-mail over het reguliere internet (poortje 25) is NIET veilig. Verstuur dus geen persoonsgegevens via de reguliere e-mail.
    - Wees alert op bijlagen in de e-mail en kijk waar het vandaan komt.
- Toegangsbeleid, ga in uw organisatie na wie bij welke informatie kan en bepaal de noodzaak hiervan.

Uw IT-leverancier kan u helpen bij het treffen van organisatorische maatregelen.
Mocht u naar aanleiding van dit artikel vragen hebben dan kunt u contact opnemen met Metis Privacy B.V. op telefoonnummer 0512- 23 24 00.