Adviesrapport

Informatieveiligheid is zo sterk als de zwakste schakel

Een onderzoek naar de bewustwording van gemeentelijke medewerkers op informatieveiligheidsvlak en specifiek de wet Meldplicht Datalekken

wiifm?

Stageonderzoek van Evelien Fiere
Opleiding Communicatie, Avans Hogeschool
Uitgevoerd van september 2016 tot januari 2017, in opdracht van soul:made

Inhoud

1. Waarom dit onderzoek?

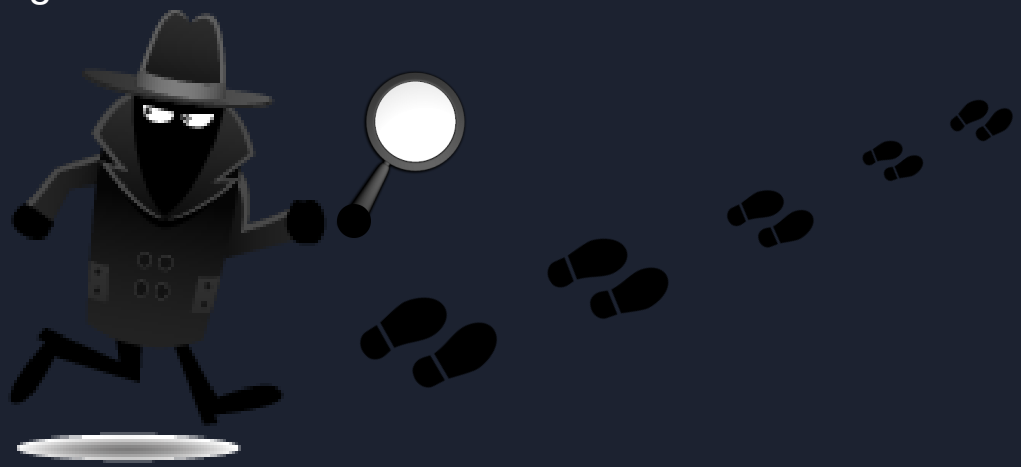
Twee aanleidingen voor dit onderzoek:

Wijziging wet Meldplicht Datalekken

Sinds januari 2016 is er een wijziging op de wet Meldplicht Datalekken van kracht. Door deze wijziging riskeren organisaties een boete van maximaal €820.000 als zij niet binnen 72 uur een datalek melden bij de Autoriteit Persoonsgegevens (AP). De AP verwachtte jaarlijks 66.000 meldingen van datalekken. In 2016 lag het werkelijke aantal meldingen echter een stuk lager, dit waren er namelijk slechts 5.500. Ongeveer tien procent van het werkelijke aantal meldingen is afkomstig van gemeenten. Het grootste deel van de datalekken wordt veroorzaakt door, al dan niet onbedoelde, foute handelingen van medewerkers.

Wist je dat..

..je nu zelf kan ervaren hoe je moet handelen bij een datalek? Kijk op bladzijde 11 voor meer informatie!



Algemene Verordening Gegevensbescherming (AVG)

Gemeenten zijn op dit moment druk bezig met het voorbereiden op de Algemene Verordening Gegevensbescherming (AVG) die vanaf 25 mei 2018 van kracht wordt. We zijn nu een jaar verder sinds de wet Melplicht Datalekken van kracht is gegaan en met de AVG in het vooruitzicht is het een goed moment om te peilen hoe het momenteel is gesteld met de kennis, de houding en het gedrag van gemeentelijke medewerkers op het gebied van informatieveiligheid. Deze informatie kan vervolgens worden gebruikt om het maximale uit bewustwordingscampagnes te halen.

Tijdens dit onderzoek lag de focus op het handelen van gemeentelijke medewerkers als het gaat om informatieveiligheid en specifiek de wet Meldplicht Datalekken. Informatieveiligheid is net zo sterk als de zwakste schakel; de mens. Informatieveiligheid kan technisch nog zo goed op orde zijn, als computers niet worden vergrendeld of phishing mails worden geopend, ligt een datalek iedere dag op de loer.

2. Wie hebben er deelgenomen aan dit onderzoek?

In totaal hebben **270 gemeentelijke medewerkers** deelgenomen aan dit onderzoek.

De deelnemers zijn verspreid over zowel **grote** (>50.000 inwoners) als **kleine** (<50.00 inwoners) gemeenten.

De deelnemers zijn werkzaam binnen **diverse afdelingen**.

De deelnemers zijn volledig **anoniem**. Er kan dan ook niet achterhaald worden welke gemeenten er hebben deelgenomen aan de enquête of wat het resultaat van een specifieke gemeente is.

Alvorens de rapportage te lezen is het van belang het volgende in aanmerking te nemen: er hebben 270 gemeentelijke medewerkers deelgenomen aan dit onderzoek. In totaal zijn er meer dan 20.000 gemeentelijke medewerkers. Het onderzoek is dus niet representatief te noemen voor alle gemeentelijke medewerkers.

3. Wat weten medewerkers over de wet Meldplicht Datalekken?

Voordat je in staat bent om een datalek melden, dien je eerst te weten wat een datalek is. Daarnaast moeten medewerkers uiteraard weten dat ze een datalek intern moeten melden, bij wie ze dat kunnen doen, hoeveel tijd ze hebben om dit te doen en belangrijker nog.. wat ze kunnen doen om een datalek te voorkomen. Maar wat is het huidige kennisniveau van de deelnemende gemeentelijke medewerkers?

- **33%** geeft aan dat zij weet wat de wet Meldplicht Datalekken inhoudt
- **75%** weet dat zij direct een datalek intern dient te melden
- **73%** weet bij wie zij een datalek intern kan melden

Een groot deel van de gemeentelijke medewerkers die heeft deelgenomen aan het onderzoek heeft al de juiste kennis over datalekken. Echter is er natuurlijk altijd ruimte voor verbetering. Het is belangrijk dat er tijdens het uitzetten van een bewustwordingscampagne wordt ingezet op het blijvend vergroten van de kennis van medewerkers.

4. Hoe staan medewerkers tegenover de wet Meldplicht Datalekken?

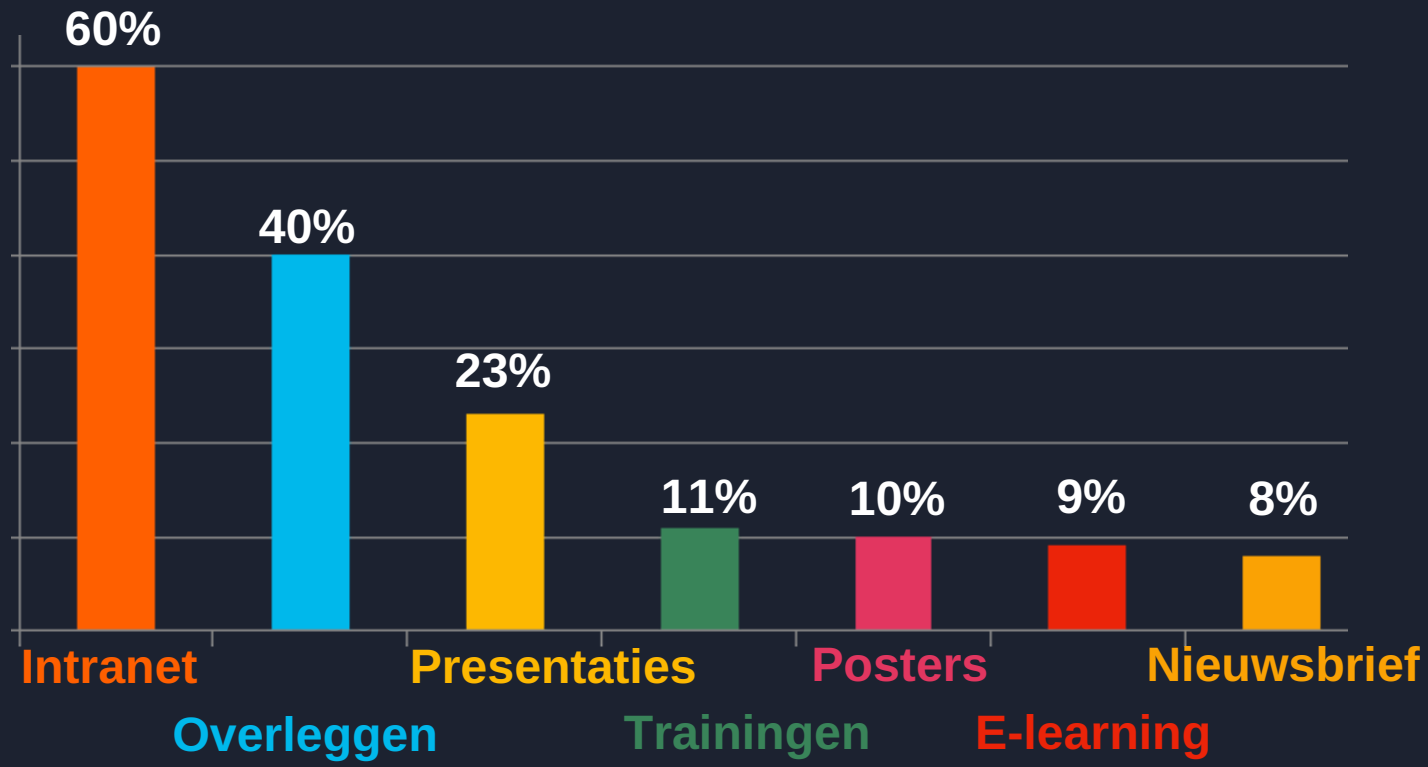
Indien medewerkers eenmaal over de juiste kennis beschikken, is het van belang dat zij ook de juiste houding hebben om daadwerkelijk, indien nodig, tot het melden van een datalek over te gaan. Hoe zit het met de houding van de deelnemende gemeentelijke medewerkers?

- **87%** voelt geen angst voor het melden van een datalek
- **88%** schaamt zich niet voor het melden van een datalek
- **96%** ziet het melden van een datalek als haar taak

De houding van de deelnemende gemeentelijke medewerkers is dus positief. Zij zijn niet bang om een datalek te melden en zien het melden van een datalek als hun taak.

5. Wat doen gemeenten op het gebied van bewustwording?

Gemeenten zijn druk bezig met het implementeren van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), het voorbereiden op de AVG en het voldoen aan diverse andere (nieuwe) privacywetgevingen. De deelnemende gemeentelijke medewerkers hebben tijdens dit onderzoek aangegeven welke middelen hun gemeente momenteel inzet om de bewustwording op het gebied van informatieveiligheid te vergroten.
En wat blijkt? Maar liefst 80% van de deelnemende gemeentelijke medewerkers geeft aan dat hun gemeente inzet op bewustwording op het gebied van informatieveiligheid!



6. Aandachtspunten

Uit het onderzoek zijn een aantal opvallende resultaten gekomen. Tijdens het uitzetten van een bewustwordingscampagne kan het raadzaam zijn om rekening te houden met twee aandachtspunten.

75% van de deelnemende gemeentelijke medewerkers geeft aan dat twijfel over het feit of er wel of niet sprake is van een datalek, een mogelijke reden is voor het niet melden van een datalek. Het is dus belangrijk dat de gemeente deze twijfel weghaalt. Zo dient er tijdens een bewustwordingscampagne aandacht te worden besteed aan het vergroten van de kennis over datalekken. Welke vragen moet je stellen om erachter te komen of er sprake is van een datalek? En medewerkers dienen te weten dat ze bij twijfel altijd naar de CISO of FG aan kunnen kloppen.

54% van de deelnemende gemeentelijke medewerkers geeft aan geen behoefte te hebben aan informatie over informatieveiligheid. Tijdens het opzetten van een bewustwordingscampagne dient er dus rekening mee te worden gehouden dat dit deel van de medewerkers niet uit zichzelf, op bijvoorbeeld intranet, op zoek gaat naar (nieuwe) informatie. De informatie dient dus actief naar medewerkers toe te worden gebracht.

7. Tips & tricks

1. Zorg dat je medewerkers actief informeert, involveert en inspireert.

2. Zorg voor een meerjarige campagnematige aanpak, gericht op het opbouwen en ondersteunen van een beveiligingspositieve omgeving.

3. Focus daarbij eerst op het bevorderen van de kennis. Je kan geen datalek melden als je niet weet wat een datalek is en waar je dit dient te melden.

4. Gebruik voor alle communicatie-uitingen rondom informatieveiligheid dezelfde beeldlijn, zo zijn de materialen herkenbaar voor alle collega’s en wordt er een rode draad gevormd, waardoor de informatie beter beklijft.

5. Laat zien dat het melden van een datalek positief is en maak het laagdrempelig.

HACKERS NIEUW

Handel jij juist bij een datalek?

Weet jij hoe je moet handelen als er een datalek plaatsvindt? Wie moet je inschakelen? En doe je dit meteen, of wacht je hiermee? Betaal je bitcoins zodat je direct weer overal toegang tot hebt of doe je dit juist niet?
Een goede manier om hierachter te komen is door een datalek zelf te ervaren. Dit kan tijdens een crisisoefening! Een hacker heeft toegeslagen en eist een flink bedrag aan bitcoins. Jij stapt in het crisiscentrum om samen met anderen het datalek aan te pakken. Lukt het jullie om de schade te beperken?

Nieuwsgierig? Meld je nu kosteloos aan voor deelname aan de crisisoefening bij soul:made op 31 mei 2017 door een mail te sturen naar evelien@soulmade.nl. Er kunnen maximaal 25 personen deelnemen, dus wees er snel bij!

Datum: 31 mei 2017

Tijd: 15:00 - 17:00
Aansluitend een borrel

Locatie: Oosterhout (NB)

Aanmelden:
evelien@soulmade.nl

9. Contact

Wist je dat..
..ik inmiddels werkzaam ben bij soul:made?
Bel of mail mij gerust bij vragen!

evelien@soulmade.nl
0162 - 430 345

Meer weten over informatieveiligheid? Neem dan een kijkje op www.wiifm.info!