BIJLAGE 2 – Meldingen beveiligingsincidenten en datalekken

Het betreft meldingen vanuit WPI over het eerste half jaar 2024.

N.B. Meldingen worden geregistreerd op melder en niet op veroorzaker.

Beveiligingsincidenten

In totaal zijn er bij de Servicedesk 21 meldingen van beveiligingsincidenten binnengekomen vanuit WPI.

- 14 meldingen betreffen onjuiste autorisaties.
- 6 meldingen gaan over (mogelijke) phisingmail, spam en dergelijke.
- Melding 21 betreft het niet functioneren van Suwinet-mail.

Dit is de eerste keer dat wij deze cijfers hebben opgevraagd.

Datalekken

In totaal zijn er bij de Servicedesk 18 meldingen van datalekken binnengekomen vanuit WPI.

- 5 meldingen betreffen verkeerd geadresseerde mail of post.
- Ook 5 meldingen hebben betrekking op verlies of diefstal van gegevens(dragers).
- 3 maal zijn persoonsgegevens in een verkeerd dossier beland.
- Over zowel publicatie van persoonsgegevens, verkeerde autorisaties als van gebruik van cc in plaats van bcc is telkens 1 melding ontvangen.
- De overige 2 meldingen vallen in de categorie "overig".

Er lijkt een stijgende trend te zijn. In 2022 waren er gemiddeld slechts 3 meldingen per kwartaal in 2023 ruim 6 en nu dus 9.

Uitgelichte meldingen

1. Niet functioneren Suwinet-mail

Suwimail is een besloten netwerk om binnen de Suwi-keten beveiligd te mailen. Alle suwi-partners zijn aangesloten, dat wil zeggen: niet alleen alle gemeenten, Uwv, Svb, maar ook andere instanties zoals de IND, het Ciz en het ministerie van SZW. Suwinet-mail is voor elk adres binnen het domein van een van de aangesloten partijen te gebruiken door achter het reguliere mailadres 5.1, 2, i toe te voegen 5.1, 2, i amsterdam.nl5.1, 2, i . Het WSP als samenwerkingsorganisatie maakt hier veelvuldig gebruik van, Inkomen wisselt geregeld gegevens uit met de Svb en bij verhuizing van een bijstandsgerechtigde van of naar een andere gemeente is suwimail het aangewezen kanaal voor gegevensdeling.

Voor zo ver ons bekend is in april een eerste melding gedaan vanuit Functioneel Beheer. Hier zijn later meldingen vanuit verschillende hoeken van de organisatie bij gekomen. Het laatste bericht is, dat er een nieuwe tussenarchitectuur gemaakt moest worden. Deze zou op 8 juli klaar zijn en na testen et cetera zou suwinet-mail vanaf 12 of 15 juli weer moeten werken.

In de tussentijd hebben collega's hun eigen workarounds moeten zoeken en de vrees is, dat er soms "dan maar gewoon" gemaild is.

2. Snelkoppeling ADW

Deze melding is in juli gedaan en is dus niet in de cijfers hierboven opgenomen, maar het probleem ligt mogelijk wel ten grondslag aan twee eerdere datalekmeldingen. Daarom en vanwege de potentiële impact lichten we ook deze melding hier uit.

Binnen het nieuwe ADW is de functionaliteit beschikbaar om na het opslaan van bestanden de locatie van bestanden onder een "snelle toegang" neer te zetten. Deze functionaliteit is standaard aangezet. Dit gebeurt ook voor bestanden die je via een applicatie opslaat. Via deze ADW-functionaliteit kan je bij de map waar alle bestanden staan van een applicatie. Rechtstreeks en dus niet via de applicatie. Dit brengt een tweetal risico's met zich mee:

- Aangezien je rechtstreeks bij de bestanden kunt, is de autorisatiematrix met bijbehorende toegangsrechten niet van toepassing. Als gebruiker kan je mogelijk meer zien dan noodzakelijk is voor je werk, maar ook meer (bewerk)rechten gebruiken dan je officieel hebt.
- Gebruikers zien een mogelijk onbekende map staan onder snelle toegang en daarmee de mogelijkheid dat gebruikers gaan opruimen (map met inhoud verwijderen). Wat niet iedereen zich zal realiseren, is dat in dat geval de bestanden ook verdwijnen uit de oorspronkelijke applicatie.

Voor beide risico's geldt dat hier sprake is van een (mogelijk) datalek. Het 2e risico is al tweemaal voorgekomen.

Voor sommige bestandslocaties is het onwenselijk dat zij beschikbaar komen bij de snelle toegang. Zeker gezien de inhoud van de WPI-applicaties met allemaal kwetsbare burgers, de hoeveelheid aan burgers in de applicatie en het aantal gebruikers bij WPI is dit heel onhandig en niet wenselijk.