DOCUMENT 2

43. [redacted] 5.1.2.f en ongeautoriseerde toegang

Melding

Goedemiddag [redacted] 5.1.2.e,

Van een brandweer vrijwilliger hebben wij een melding ontvangen over het gebruik van [redacted] 5.1.2.f. [redacted] 5.1.2.f is ons vakbekwaamheid en incidentmanagement systeem en wordt ook gebruikt om de vergoedingen van de vrijwilligers te registeren. [redacted] 5.1.2.f De betreffende vrijwilliger is beroepsmatig 'legal hacker' en heeft [redacted] 5.1.2.f

De betreffende vrijwilliger gaf aan zich af te vragen of hij op basis van deze toegang ook de vergoedingsgegevens van andere te kunnen inzien.

Dit laatste heeft mij getriggerd. Ik heb hier samen met [redacted] 5.1.2.e een onderzoek naar gedaan. Conclusie het was inderdaad mogelijk om op basis van een soortgelijke route gegevens van personen van dezelfde post in te zien. Het gaat hierbij om gegevens over:

- Naam, adres, e-mailadres en telefoonnummer
- Keuringgegevens (geen medische gegevens, deze leggen wij uberhaupt niet vast in [redacted] 5.1.2.f)
- Opleiding diploma gegevens
- Vergoeding gegevens (activiteit, tarief, aantal uren, bedrag)

Dit laatste is echter niet te wijten aan onze leverancier, maar ligt aan onze eigen inrichting van de rechten in [redacted] 5.1.2.f Dit moeten we dan ook zelf herstellen. De impact van deze aanpassing van de rechten op de applicatie moet wel even goed onderzocht worden.

Dit bericht is een voorsignalering. Komende donderdag hebben [redacted] 5.1.2.e en ik hier overleg over. [redacted] 5.1.2.e en ik kennen de details [redacted] 5.1.2.e weten op dit moment enkel van het bestaan van het probleem. Mochten er direct vragen zijn dan horen we het graag. Wordt vervolgd.

Met vriendelijke groet,
[redacted] 5.1.2.e

Melding 1. Correspondentie met [redacted] 5.1.2.f

Op Wo, 3 Mrt om 4:20 PM , [redacted] 5.1.2.f Helpdesk <helpdesk1@[redacted] 5.1.2.f.nl> schreef:
Goedemiddag [redacted] 5.1.2.e,
Bedankt voor jullie melding. We gaan dit de komende dagen nader onderzoeken en houden jullie op de hoogte.
Met vriendelijke groet,

[redacted] 5.1.2.e Op Wo, 3 Mrt om 4:49 PM , [redacted] 5.1.2.f Helpdesk <helpdesk1@[redacted] 5.1.2.f.nl> schreef:
Uw ticket online bekijken

Geachte [redacted] 5.1.2.e,
Mijn collega [redacted] 5.1.2.e heeft mij op de hoogte gebracht van het gemelde beveiligingsincident.
Conform onze beleidsregels hebben we de volgende processen opgestart:

1. Uitvoeren van een impactanalyse en opstarten van een RCA (Root Cause Analyse) met onze Manager R&D
2. Het MT is op de hoogte geïnformeerd.

We houden jullie op de hoogte van onze onderzoeksbevindingen en eventuele te ondernemen acties.
Graag verzoeken wij jullie vertrouwelijk om te gaan met de uitgewisselde informatie.
Vragen of aanvullende informatie kunnen worden toegevoegd aan dit ticket.
Met vriendelijke groet,
[redacted] 5.1.2.e

Van: Helpdesk<helpdesk@[redacted] 5.1.2.fnl>
Verzonden:donderdag4maart202112:56
Aan: [redacted] 5.1.2.e
CC: [redacted] 5.1.2.e
Onderwerp: Re: Inactieve
Uw ticket online bekijken
Beste [redacted] 5.1.2.e

Zoals besproken hebben we een impactanalyse uitgevoerd op basis van het door jullie ingediende incident.

De conclusie uit onze analyse is als volgt:
1. Verstoring standaard dagelijks gebruik
Andere gebruikers hebben geen hinder van de acties die de betreffende persoon heeft uitgevoerd. Ze kunnen dit activiteit type niet zien en dus ook niet gebruiken. Alle werkzaamheden gewoon plaatsvinden.
2. Data risico
De betreffende persoon heeft geen toegang gehad tot persoonsdata van andere gebruikers. Ook overige data is niet in gevaar geweest. [redacted] 5.1.2.f

Vervolgstappen
De persoon heeft aanpassingen kunnen doen via [redacted]

[redacted] 5.1.2.f

Wij zijn blij dat de melding, wat in het begin leek op een beveiligingsincident, na onderzoek blijkt mee te vallen. Hiermee beschouwen wij dit onderzoek dan ook als afgerond.

Bedankt voor jullie input en alerte reactie.

Met vriendelijke groet,

[redacted] 5.1.2.e

Dag [redacted] 5.1.2.e,
Dank voor jullie professionele aanpak. Volgens mij correcte conclusie. Ook wij hebben onderzoek gedaan of de betreffende persoon o.b.v. zijn autorisatie persoonsgegevens van andere personen had kunnen inzien. Ook onze conclusie was dat dit niet het geval was. [redacted] 5.1.2.f

Met vriendelijke groet,

[redacted] 5.1.2.e

Terugkoppeling door [redacted] 5.1.2.e aan FG (6 maart 2021):

Dag [redacted] 5.1.2.e,
Even een status update. Voor wat betreft het eerste punt:
Van een brandweer vrijwilliger hebben wij een melding ontvangen over het gebruik van [redacted] 5.1.2.f. [redacted] 5.1.2.f is ons vakbekwaamheid en incidentmanagement systeem en wordt ook gebruikt om de vergoedingen van de vrijwilligers te registeren. [redacted] 5.1.2.f De betreffende vrijwilliger is beroepsmatig 'legal hacker' en heeft [redacted] 5.1.2.f De betreffende vrijwilliger gaf aan zich af te vragen of hij op basis van deze toegang ook de vergoedingsgegevens van andere te kunnen inzien.
Van bovenstaand punt is een melding gemaakt bij de leverancier. Zij hebben dit zeer serieus opgepakt en intern een beveiligingsmelding gemaakt. Zij geven aan dat deze persoon geen toegang heeft gehad tot gegevens van andere vrijwilligers. Dit is ook uit ons eigen interne onderzoek gekomen. Daarnaast geven zij aan om [redacted] 5.1.2.f Onderstaand het bericht dat ik heb ontvangen van [redacted] 5.1.2.f (Dat staat eerder in dit verslag [redacted] 5.1.2.e).

Melding 2 Gesprek met functioneel beheer

Aanwezig: [redacted] 5.1.2.e
Afwezig: [redacted] 5.1.2.e

[redacted] 5.1.2.e schetst de bevindingen die hij met [redacted] 5.1.2.e heeft gedaan. Geconstateerd dat sommige groepen (post gebruikers) rechten hebben op de data van collega's van dezelfde post. [redacted] 5.1.2.f

Vervolgacties

- Inventarisatie van de rechten ([redacted] 5.1.2.e)
- Analyse van de impact van het aanpassen naar de juiste situatie (worden deze rechten niet voor een ander, legitiem doel gebruikt) ([redacted] 5.1.2.e)
- Verwijderen van de rechten ([redacted] 5.1.2.e)
- Voortgangsmelding naar FG ([redacted] 5.1.2.e)
- Agenderen van periodieke rapportages in het overleg met de functioneel beheerders ([redacted] 5.1.2.e)