DOCUMENT 7

SI nr 38 - GMS

Risicoanalyse beveiligingsincident

Melding: 38
Melder: [redacted] 5.1.2.e
Sector: GMK
Datum: 16 november 2020

Auteur: [redacted] 5.1.2.e

Omschrijving
Op dinsdag 10 november om 06.30 uur is versie 7.2 van de webservice geïnstalleerd. Daarna is geconstateerd dat er in specifieke situaties te veel informatie doorgestuurd werd.

Toelichting
Na onderzoek bleek dat in het geval van een multi-incident (met 2 of meer disciplines) alle informatie van het incident doorgestuurd werd in plaats van alleen die informatie te leveren van de discipline waarvoor u geautoriseerd bent.

Het is voor GMS beheer niet zichtbaar welke informatie exact ten onrechte is verstuurd en in hoeverre deze zichtbaar is voor uw organisatie.
Gezien de ernst van dit informatiebeveiligingsincident is donderdag 12 november om 23.30 uur besloten om terug te gaan naar de oude situatie (vorige versie). Dit besluit is genomen na het zorgvuldig afwegen van verschillende opties en belangen.

Effect
Ontvangende systemen kunnen informatie, en in het bijzonder persoonsgegevens, hebben ontvangen waarvoor het systeem niet geautoriseerd is. De melder wijst in dit verband op de geheimhoudingsplicht en gaan ervan uit dat deze niet geautoriseerde informatie uit de systemen worden verwijderd.

Door de CISO van de Politie is melding gemaakt bij de Autoriteit Persoonsgegevens.
Classificatie van de informatie
Het GMS zorgt voor een naadloze samenwerking tussen de meldkamers van de diverse hulpverleningsinstanties, én de communicatie op straat. Een melding van een burger kan middels GMS snel afgehandeld worden. De software kan zelf een inzetvoorstel doen op basis van locatie, mankracht en aanrijtijd.
Het GMS is als systeem eigendom van de gemeenschappelijke meldkamer. Het beheer is belegd bij het LMS. Iedere partij die gebruik maakt van het GMS is verantwoordelijk voor zijn eigen data binnen het GMS (bron: Convenant Gegevensverwerking Meldkamer).
Via het GMS worden brandweer, ambulancezorg en politie aangestuurd. In het systeem wordt informatie vastgelegd voor een adequate afhandeling van incidenten. Hieronder (bijzondere) persoonsgegevens waaronder patiëntinformatie, adresinformatie. Op basis van strikte autorisaties wordt informatie gedeeld met de juiste partijen. De BIV classificatie voor Vertrouwelijkheid van het GMS is Hoog. Gezien de vastgelegde bijzondere persoonsgegevens is de privacy gevoeligheid hoog.
Techniek

- Incidentinformatie wordt vastgelegd in het GMS door de centralist in de meldkamer
- De incidentinformatie wordt gedistribueerd naar systemen van de hulpverleningsdiensten via de GMS webservice of webbroker
- De informatie wordt geclassificeerd en gelabeld t.b.v. autorisatie en distributie. Hiermee wordt geborgd dat informatie naar de juiste organisatie, organisatieonderdeel en systeem wordt verzonden. Er zijn o.a. labels om onderscheid te maken tussen brandweer, ambulancezorg en politie.
- Ontvangende partijen en systemen zijn geautoriseerd voor ontvangst van specifieke datasets.

Analyse

De volgende systemen ontvangen data uit het GMS via de GMS webservice:

1. [redacted] 5.1.5
    a. Er is een controle op de ontvangen incidentinformatie uitgevoerd door de functioneel beheerder. Er zijn geen afwijkingen geconstateerd in de periode 10-11-2020, 06:30 – 12-11-2020, 23:30.
2. [redacted] 5.1.5
    a. Er is een controle op de ontvangen incidentinformatie uitgevoerd door de functioneel beheerder. Er zijn geen afwijkingen geconstateerd in de periode 10-11-2020, 06:30 – 12-11-2020, 23:30.
3. [redacted] 5.1.5

Bij de controle is gebruik gemaakt van de historische GMS data die door VRGZ wordt opgeslagen t.b.v. archivering en managementrapportage. Deze data wordt via de replicaserver van het GMS ontvangen. De gegevens van incidenten in bovenstaande applicaties is vergeleken met de historische data.

Conclusie

Het datalek heeft niet geleid tot het doorzenden van informatie naar systemen van VRGZ die daarvoor niet geautoriseerd zijn.

Advies

Er zijn geen maatregelen nodig.