Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK
Minister van Justitie en Veiligheid
Minister voor Rechtsbescherming

Datum
28 januari 2021

memo

Memo duiding en achtergrond GGD - casus

Algemeen

Op 25 januari jl. is uit onderzoek van RTL Nieuwsjournalisten gebleken dat de persoonsgegevens van miljoenen Nederlanders worden verhandeld op het internet (via chatdiensten). Dit betreft zowel de mogelijkheid individuele gegevens te kopen als de mogelijkheid gehele gegevenssets (duizenden tot tienduizenden personen) te kopen. Het betreft een lek in twee informatiesystemen: CoronaIT (online registratiesysteem coronatesten) en HPZoneLight (systeem voor het bron- en contactonderzoek van de GGD). Vooral in HPZone staat hele gevoelige informatie (medische gegevens en contacthistorie). De Volkskrant van 28 januari gaat ook in op de situatie bij de GGD-en. Daarin wordt gesteld dat de uitspraken van de minister van VWS in het vragenuurtje van 26 januari onjuist zijn, en is men zeer kritisch over fundamentele inrichtingskeuzes van de ICT-systemen bij de GGD.

Gebleken is dat reeds in september 2020 via Nieuwsuur naar buiten kwam dat testlijnmedewerkers bij meer gegevens konden dan bij wet is toegestaan. Daarbij leek het evident dat de AVG werd overtreden. Vanuit de TK is toen de roep gekomen snel zaken recht te zetten. In december is na een risico-analyse reeds een aantal maatregelen genomen om het systeem beter te beveiligen. De Autoriteit Persoonsgegevens heeft op 27 januari om opheldering gevraagd. Hij heeft aangegeven dat eventuele nalatigheid kan leiden tot een boete, maar ook tot massale schadeclaims van slachtoffers. Onduidelijk is of er formeel melding is gedaan van een datalek.

Deze zaak volgt op de U-diagnostics zaak, een (sneltest)bedrijf, waarin journalisten van Nieuwsuur gegevens van onder meer militairen konden inzien door gebrekkige informatiebeveiliging.

Deze zaak raakt de JenV verantwoordelijkheid voor strafrechtelijke handhaving, het opsporen van de daders, waarover MJenV reeds is geïnformeerd. Daarnaast raakt het aan de verantwoordelijkheid voor bescherming persoonsgegevens/AVG (MRb) en de coördinerende rol van MJenV voor cybersecurity. In deze nota treft u achtergronden aan die de ernst van de casus trachten te duiden.

Verplichting GGD tot nemen passende organisatorische en technische maatregelen o.g.v. AVG

Er is in casu - en in tegenstelling tot wat sommige partijen in het debat naar voren brachten - geen twijfel over óf de GGD deze gegevens had mogen verwerken. De vraag die hier centraal staat is of door de GGD voldaan is aan de verantwoordelijkheden die zij heeft als 'verwerkingsverantwoordelijke' ex artikel 24 AVG en meer specifiek of is voldaan aan artikel 32 AVG betreffende beveiliging.

Artikel 32 van de AVG verplicht de verwerkingsverantwoordelijke (de GGD) om passende technische en organisatorische maatregelen te nemen teneinde een verwerking te beveiligen. Dit betreft dus geen technische maatregelen om 'hackers' buiten de deur te houden, maar de interne organisatorische maatregelen: wie kan waarbij en hoe zorgen we dat er geen fouten worden gemaakt? Tevens geldt de meldplicht bij datalekken.

Berichtgeving in de media indiceert dat:

- De systemen in september niet op orde waren omdat de toegang tot gegevens niet begrensd was. (berichtgeving Nieuwsuur);
- Dat er volledige datasets zijn gedownload en verspreid door een voor werknemers beschikbare 'exporteerfunctie' (Verlaan, RTL)
- Dat werknemers nog steeds bij veel meer gegevens dan nodig kunnen (Modderkolk, VK)
- Het lek nog steeds niet in volledigheid gedicht zou zijn (Verlaan, RTL).

Debat 26 januari en reactie media

De toelichting van de minister van VWS in het debat van 26 januari jl. en de reactie daarop van de journalisten in kwestie is als volgt:

- De minister van VWS heeft in het debat gesteld dat het gaat om diefstal door het maken van screenshots. Verlaan (RTL) stelt te kunnen bewijzen dat het systeem een voor velen beschikbare exportfunctie had waardoor hele datasets uit het systeem kunnen worden gehaald. Dit lek zou in december zijn gedicht, maar de stelling van Verlaan lijkt niet onaannemelijk.
- Gesteld is dat diefstal niet voorkomen kan worden en alleen hetgeen redelijkerwijs gevraagd kan worden is gedaan (zoals in de AVG verplicht). Het heeft er echter de schijn van dat in elk geval in het verleden niet aan die verplichting is voldaan.
- Er zou continu zijn en worden gecontroleerd of medewerkers geen misbruik maakten. Verlaan (RTL) stelt dat er slechts is gewerkt met steekproeven en dat nu pas wordt gewerkt aan de automatische analyse van 'logs' (waardoor misbruik van gegevens beter gesignaleerd kan worden).
- Het systeem voldoet sinds een 'risico-analyse' in december 2020 aan de NEN-normen over informatiebeveiliging. De media schetst de onwenselijkheid dat dit niet reeds bij aanvang het geval was.
- Het autorisatiemanagement zou op orde zijn, terwijl de media het beeld oproept dat medewerkers toegang hadden tot meer gegevens dan nodig.

- Er bestaat onduidelijkheid over of er al dan niet grote whatsapp-groepen met medewerkers zijn geweest waarin persoonsgegevens zijn gedeeld, hetgeen geen adequate beveiligingspraktijk is. Dhr. Verlaan meldt dat deze groepen nu onder druk van de GGD worden verwijderd.

Al met al lijkt er vanuit de overheid vooral de nadruk gelegd te worden op het vergroten van de pakkans van dieven. De maatschappelijke onrust komt vooral voort uit het niet op orde zijn van basisprincipes op het gebied van informatiebeveiliging.

Hoewel het gelet op onze informatiepositie (gebaseerd op open bronnen) lastig is een formeel oordeel te geven over de rechtmatigheid van de door de GGD ingezette systemen lijkt het aannemelijk dat de GGD niet heeft voldaan aan de basisvereisten uit artikel 32 AVG. Er zijn onvoldoende organisatorische maatregelen getroffen: het autorisatiemanagement en de rechtenverdeling in genoemde systemen lijkt niet op orde. Onduidelijk is of de inmiddels in december en januari genomen maatregelen de gegevensverwerking nu rechtmatig maken en er bij deze (en andere) systemen in relatie tot de COVID-aanpak adequate basisbeveiligingsmaatregelen zijn genomen.

Cybersecurity – basisbeveiliging verantwoordelijkheid GGD

Omdat de onderhavige casus niet een hack betreft, maar datadiefstal, is er geen specifieke cybersecurityverantwoordelijkheid voor de minister van Justitie en Veiligheid.

De minister van JenV is coördinerend bewindspersoon cybersecurity. Vanuit die rol heeft JenV ondermeer de Wet beveiliging netwerk- en informatiesystemen (WBNI) opgesteld. Deze ziet primair op vitale aanbieders en de rijksoverheid en regelt de taken van het Nationaal Cyber Security Centrum (NCSC) daarin. De GGD-en vallen niet onder die categorieën. En hoewel de spoedwet COVID meer mogelijkheden biedt om organisaties in de volksgezondheidssector bij te staan met dreigingsinformatie over cyberaanvallen biedt dat ook in deze casus vooralsnog weinig soelaas, omdat GGD-en buiten het bereik van de wet lijken te vallen.

De WBNI wijst als nationaal bevoegde autoriteit voor de gezondheidszorg de minister voor Medische Zorg aan. Uiteindelijk is het aan de aanbieders van diensten zelf, i.c. GGD-en, om voor hun basisbeveiliging te zorgen, ook als ze niet onder de WBNI vallen.

Voor de gehele overheid heeft het ministerie van Binnenlandse Zaken, vanuit zijn verantwoordelijkheid voor informatiebeveiliging bij de overheid, de baseline informatievoorziening (BIO) overheid opgesteld en provincies, gemeenten en waterschappen hebben zich hieraan bij bestuurlijk akkoord gecommitteerd. Deze BIO bevat eisen voor adequate basisbeveiliging naar gelang het risico. Eisen die mogelijk een bijdrage aan het voorkomen, dan wel snel opsporen van deze datadiefstal hadden kunnen leveren. VWS heeft inmiddels contact gehad met BZK hierover, en de informatie beveiligingsdienst voor gemeenten (IBD/VNG) staat net als het NCSC in contact met Z-CERT.

GGD-en hebben als openbaar lichaam een eigen rechtspositie en gelden als verlengd lokaal bestuur, via een wettelijke regeling van VWS. Verantwoording leggen zij af aan de lokale wethouder(s). En hoewel er voor de gezondheidssector sectorspecifieke cyberveiligheidsnormen gelden, is gelet hierop ook relevant om de BIO in ogenschouw te nemen.

Het ministerie van VWS en het RIVM vallen als rijksoverheidsorganisaties onder de doelgroep van het NCSC. Het NCSC kan hen adviseren en bijstaan. De GGD-en vallen niet onder de doelgroep van het NCSC, waardoor zij in beginsel niet worden geadviseerd of bijgestaan door het NCSC. In geval van een ernstig incident met aanzienlijke gevolgen voor de dienstverlening kan de GGD wel een 'vrijwillige melding' doen bij het NCSC, waarna het NCSC kan adviseren en kan ondersteunen bij de incident respons. Voor de structurele inrichting en verbetering van de informatiebeveiliging zal de GGD een beroep moeten doen op andere partijen, bijvoorbeeld in de private sector.

De GGD-en hebben tot op heden geen computercrisisteam dat hen voorziet van advies en informatie om hun digitale weerbaarheid te vergroten, bijvoorbeeld zoals het NCSC dit doet voor vitale aanbieders. Naar aanleiding van een aangenomen Kamermotie om zo snel als mogelijk de gehele zorgsector onder te brengen bij Z-CERT, het computercrisisteam voor de zorg, is besloten om de GGD-en in de loop van 2021 aan te sluiten op deze organisatie. Dit is dus op dit moment nog niet het geval. Het NCSC werkt nauw samen met Z-CERT en deelt informatie over dreigingen, incidenten en kwetsbaarheden met hen.

Naar aanleiding van het incident bij de GGD heeft het NCSC contact gehad met Z-CERT. Daarbij is afgesproken dat Z-CERT vooruitlopend op de daadwerkelijke aansluiting van de GGD-sector op hun dienstverlening later dit jaar, alvast beginnen met het delen van informatie over informatiebeveiliging en het aanbieden om bestaande informatiebeveiliging te reviewen. Dit wordt door Z-CERT opgepakt en zij onderhouden hierover contact met het NCSC.

Gelet op het bovenstaande komt de minister van Justitie en Veiligheid, noch de minister voor Rechtsbescherming, een specifieke rol of bevoegdheid toe om hierop in te grijpen dan wel aanwijzingen te geven. De onder JenV ressorterende diensten leveren zoals hierboven geschetst naar vermogen bijstand.