29 668 Beleidsplan Crisisbeheersing

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 58 Brief van de minister van Justitie en Veiligheid

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 april 2021

Met mijn brief van 30 april 2020[1] heb ik uw Kamer op de hoogte gebracht van een mogelijk datalek in de toen net ontwikkelde app van NL-Alert. Mijn ministerie heeft in april vorig jaar bij een gespecialiseerd advocatenkantoor advies ingewonnen over een mogelijke inbreuk in verband met persoonsgegevens bij de app van NL-Alert. Dit advocatenkantoor kwam op basis van de toen beschikbare informatie tot de voorlopige bevinding dat er mogelijk sprake was van een datalek, waarna mijn ministerie op 30 april hiervan melding heeft gemaakt bij de Autoriteit Persoonsgegevens (AP). Op 6 mei jl.[2] heb ik uw Kamer tevens geïnformeerd over een geconstateerde en verholpen kwetsbaarheid in de app.

Zoals destijds aangekondigd, heb ik de Auditdienst Rijk (ADR) gevraagd een intern onderzoek te doen naar de totstandkoming van de app om daaruit lering te trekken voor vergelijkbare trajecten in de toekomst. Ook heb ik het bedrijf Fox-IT opdracht gegeven de app door te lichten op mogelijke andere kwetsbaarheden en heb ik de Landsadvocaat gevraagd het mogelijke datalek nader te onderzoeken. De Autoriteit Persoonsgegevens heeft de door mijn ministerie gemaakte melding eveneens onderzocht.
Ik heb uw Kamer toegezegd dat ik u na afronding van de onderzoeken zou informeren over de uitkomsten daarvan. Met deze brief geef ik uitvoering aan die toezegging. Ik zal eerst kort in gaan op de constateringen en gedane aanbevelingen en ga daarna in op de maatregelen die naar aanleiding van deze onderzoeken zijn en worden genomen.

**Bevindingen Landsadvocaat, Autoriteit Persoonsgegevens, Auditdienst Rijk en Fox-IT**

Landsadvocaat

De Landsadvocaat is direct na mijn melding bij de AP gestart met een onderzoek naar het mogelijke datalek. De Landsadvocaat concludeert dat er geen sprake is geweest van een meldplichtig datalek.

Autoriteit Persoonsgegevens

De bevindingen van de Landsadvocaat zijn met de AP gedeeld. De AP heeft aangegeven de bevindingen van de Landsadvocaat te volgen.
In de reactie van de AP op de melding staan verder drie onderdelen centraal; de tijdigheid van de melding, de Data Protectie Impact Assessment (DPIA) en de getroffen beveiligingsmaatregelen.

[1] Kamerstukken 29 668 en 26 643, nr. 54.
[2] Kamerstukken 29 668 en 26 643, nr. 55.

De AP merkt over de tijdigheid van de melding op dat mijn ministerie bij de eerste signalen van een mogelijke inbreuk dit bij de AP had moeten melden, ongeacht of in dat stadium voldoende informatie voorhanden was over de aard en omvang van de mogelijke inbreuk.
Ten aanzien van de getroffen beveiligingsmaatregelen merkt de AP op dat de beveiliging van de app niet op orde was, omdat onder meer een kwetsbaarheid was geconstateerd en geen review was uitgevoerd op de laatste versie van de app waarmee de tekortkomingen van de app geïdentificeerd hadden kunnen worden.

<u>De Auditdienst Rijk</u>
De ADR constateert in zijn bevindingen tekortkomingen in de aansturing en beheersing van het project en het toezicht daarop. De ADR constateert onder meer dezelfde punten als de AP over de informatiebeveiliging en de DPIA.
Een projectmatige aanpak had volgens de ADR voor betere beheersing van het gehele traject en borging van (privacy)risicoanalyses kunnen zorgen.
Volgens de ADR lijken de problemen bij het ontwikkelen van de app o.a. te zijn ontstaan doordat de betrokken medewerkers weinig ervaring hadden met projectmanagement en inkooptrajecten en ze misten ook inhoudelijke technische kennis die noodzakelijk is voor dit soort ontwikkeltrajecten. De medewerkers zijn hierdoor onvoldoende in staat geweest om de risico's te inventariseren en te mitigeren.

<u>Fox-IT</u>
Over de uitvoering van dit onderzoek bent u reeds geïnformeerd in de brief van 6 mei 2020[3]. Fox-IT heeft in zijn analyse de eerder geconstateerde en verholpen kwetsbaarheid bevestigd. Fox-IT heeft geen verdere kwetsbaarheden in de app aangetroffen die ongeautoriseerde toegang of ongewenste verspreiding van persoonsgegevens mogelijk maakten.

**Reactie op de bevindingen**
De mogelijke inbreuk had onverwijld gemeld moeten worden bij de AP. Ik zie dit als een belangrijk leerpunt dat inmiddels in de werkwijze is verankerd. Bij twijfel of een incident wel of niet bij de AP moet worden gemeld, geldt de regel dat een voorlopige melding wordt gedaan. Mijn ministerie beschikt over een actueel Stappenplan Meldplicht Datalekken voor medewerkers en leidinggevenden. Dit stappenplan wordt actief onder de aandacht gebracht. Dat gebeurt onder meer in een voor alle medewerkers verplichte e-learning die dit jaar wordt aangeboden. In de e-learning wordt uitgebreid aandacht besteed aan datalekken teneinde te bewerkstelligen dat medewerkers zijn toegerust om privacy bewust te werken. Dat betekent onder meer dat zij datalekken kunnen signaleren en weten waar en wanneer ze datalekken dienen te melden.

Bij de ontwikkeling van de app en de DPIA is onvoldoende expertise ingezet om te toetsen of de verstrekte informatie over de beoogde werking van de app correct en volledig was. De vastgestelde DPIA had geactualiseerd moeten worden op het moment dat daartoe aanleiding was. Daarom worden binnen mijn ministerie maatregelen genomen om de kennis van medewerkers over DPIA's te vergroten.

[3] Kamerstukken 29 668 en 26 643, nr. 55.

Tevens is – in afstemming met de AP – een onderzoek ingesteld naar in 2019 en 2020 uitgevoerde relevante DPIA's waarvoor ik de verwerkingsverantwoordelijke ben, waarbij zal worden beoordeeld of de praktijk van gegevensverwerking in lijn is met de inhoud van de DPIA's, en of de naar aanleiding van de DPIA's getroffen maatregelen voldoende zijn gebleken om de vastgestelde risico's te mitigeren.

Er zal tevens voor worden gezorgd dat in voorkomende gevallen het ontwikkelen van vergelijkbare producten binnen mijn ministerie volgens een projectmatige aanpak plaatsvindt, waarbij informatiebeveiliging en privacy belangrijke pijlers zijn. Bij deze aanpak wordt gebruik gemaakt van projectleiders met ervaring in ICT-projecten en gegevensbeschermingsexperts die gedurende het traject betrokken blijven. Naast *privacy by design* en *privacy by default* wordt extra rekening gehouden met de benodigde technische en organisatorische maatregelen. Welke maatregelen moeten worden genomen is afhankelijk van de aard en type van de verwerking. Goede voorbeelden zijn versleuteling, maar ook het inrichten van procedures voor de controle van systemen. Hiermee wordt het risico op kwetsbaarheden, datalekken en andere inbreuken verkleind. Tevens moet waar mogelijk gebruik worden gemaakt van beschikbare interdepartementale expertise en moet opgedane kennis worden uitgewisseld. Tot slot worden binnen het ontwikkelproces voldoende momenten ingebouwd om het product – indien nodig ook extern - te toetsen op de naleving van geldende eisen op het gebied van informatiebeveiliging en privacy.

**Toekomstige voorziening**
De app was een aanvullend middel op NL-Alert, het alarmmiddel van de overheid in het geval van een noodsituatie. De NL-Alert app was ontwikkeld om twee specifieke doelgroepen te bedienen. De eerste doelgroep betreft mensen met een communicatieve beperking die met een regulier NL-Alert bericht niet altijd worden bereikt. De app is om die reden in goede samenwerking met belangengroepen voor mensen met een visuele en/of auditieve beperking ontwikkeld. De tweede doelgroep betreft bewoners van de grensregio's die met hun telefoon soms (automatisch) gebruik maken van Belgische en Duitse mobiele netwerken en daardoor niet altijd een regulier NL-Alert bericht ontvangen.

De app bevond zich nog in een pilotfase toen deze in maart 2020 in de appstores werd geplaatst. Personen die betrokken waren bij de ontwikkeling van de app zijn destijds actief gevraagd om de app te downloaden en hun ervaringen te delen. De app werd goed ontvangen door deze personen en bleek in een grote behoefte te voorzien.

Gezien de geconstateerde behoefte heb ik besloten om opnieuw een voorziening te gaan ontwikkelen. Bij dit traject worden de geleerde lessen en de aanbevelingen uit de verschillende onderzoeken ter harte genomen. De voorziening komt pas beschikbaar voor het publiek als een zorgvuldige (externe) doorlichting op onder andere privacy-eisen en informatiebeveiliging heeft plaatsgevonden.

De minister van Justitie en Veiligheid,
F.B.J. Grapperhaus