Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 592

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 februari 2019

Hierbij stuur ik uw Kamer het advies van het Bureau ICT-Toetsing (BIT) over het Verwijzingsportaal Bankgegevens (VB) en mijn reactie daarop.

Ik dank het BIT voor dit advies. De bevindingen zijn helder en de aanbevelingen waardevol, ik neem deze dan ook ter harte.

Hieronder beschrijf ik kort wat het project VB behelst. Vervolgens geef ik een reactie op de kern van het BIT advies. Als laatste ga ik in op de aanbevelingen uit het BIT-advies.

Het Verwijzingsportaal Bankgegevens

De Politie, het Openbaar Ministerie, de Belastingdienst, de Financial Intelligence Unit (FIU) en de Bijzondere Opsporingsdiensten mogen identificerende persoonsgegevens bij banken en betaaldienstverleners vorderen of opvragen voor de uitoefening van bepaalde taken. Het VB is bedoeld om het proces voor het vorderen, opvragen en verstrekken van deze identificerende gegevens geautomatiseerd te laten plaatsvinden. Het huidige proces is arbeidsintensief: opsporingsdiensten vragen iedere individuele bank om gegevens die die bank vervolgens handmatig uit de eigen systemen haalt. Voor een grote bank gaat het om duizenden bevragingen per jaar. Het project VB wil dit proces efficiënter maken door het opsporingsdiensten mogelijk te maken om via het VB gegevens op te vragen, indien nodig bij meerdere banken tegelijkertijd. Het portaal wordt hiertoe gekoppeld aan de systemen van banken.

Banken worden wettelijk verplicht om bevragingen via het portaal geautomatiseerd te beantwoorden.[1] Het VB gaat gebruikt worden door de Politie, de Bijzondere Opsporingsdiensten en het Openbaar Ministerie. Ook de Belastingdienst krijgt toegang tot het VB om te controleren of

[1] Beschreven in het Concept Ontwerpbesluit Verwijzingsportaal Bankgegevens: https://www.internetconsultatie.nl/verwijzingsportaalbankgegevens/document/3707.

kst-26643-592
ISSN 0921 - 7371
's-Gravenhage 2019

opgegeven bankrekeningnummers overeenkomen met de gegevens van banken, om bijvoorbeeld fraude bij uitbetaling van toeslagen te voorkomen. De FIU gaat het VB gebruiken voor het opvragen van nadere gegevens in het kader van de analyse van ongebruikelijke transacties.

Met het VB wil Nederland voldoen aan de verplichting van de Europese Unie (EU) om te voorzien in een geautomatiseerd centraal opvraagsysteem voor identificerende gegevens van banken en betaaldienstverleners[2]. Vanaf augustus 2020 moeten alle EU-lidstaten hieraan voldoen.

BIT-advies

Het BIT onderschrijft het nut en de noodzaak van het VB. Het VB zoals het nu is ontworpen vindt zij echter nog geen robuuste oplossing om het huidige proces goed te vervangen. Ter onderbouwing hiervan heeft het BIT op vier onderdelen bevindingen gedaan:

- het ontbreken van inzicht voor opsporingsambtenaren of de door banken aangeleverde gegevens compleet zijn;
- het ontbreken van enkele noodzakelijke beveiligingsmaatregelen;
- de gewenste beschikbaarheid van het VB kan nog niet worden gegarandeerd;
- het VB is nog niet direct te gebruiken voor bevragingen bij alle banken, omdat banken waarschijnlijk niet allemaal op 1 juli 2019 zijn aangesloten.

Om het VB tot een succes te maken adviseert het BIT om vóór grootschalige inzet een aantal verbeteringen door te voeren ten aanzien van het ontwerp, de beveiliging, de beschikbaarheid en de bruikbaarheid van het VB. Voor de nadere uitwerking van de adviezen verwijs ik naar het bijgevoegde BIT-advies d.d. 10 december 2018[3].

Reactie

Sinds 2016 wordt vanuit mijn departement in nauwe samenwerking met mijn ambtsgenoot van Financiën en de toekomstig gebruikers van het VB (Politie, OM, FIU, Bijzondere Opsporingsdiensten, de vier grote banken en de NVB) intensief gewerkt aan de ontwikkeling en realisatie van het VB. In een gemeenschappelijk project is het technisch ontwerp van het VB tot stand gekomen en is de realisatie uitgevoerd. Daarbij is uitgebreid aandacht besteed aan de aspecten informatiebeveiliging en privacy. Onlangs heeft een succesvolle pilot met één van de vier grootbanken plaatsgevonden. Op dit moment wordt gewerkt aan de voorbereidingen van in gebruik name. Deze is beoogd vóór 1 januari 2020.

Parallel aan het ontwikkelproces is het wetsvoorstel VB tot stand gekomen waarin wordt voorgeschreven dat banken aansluiten op het VB. In dat verband is ook advies gevraagd aan de Autoriteit Persoonsgegevens. Ik verwacht het wetsvoorstel VB in het voorjaar aan uw kamer te kunnen aanbieden.

Het onderzoek van het BIT heeft plaatsgevonden op basis van de situatie van het project in juni 2018. Op basis van zijn onderzoek heeft het BIT het nut en noodzaak van het VB bevestigd. Het BIT stelt echter ook dat het VB onvoldoende robuust is om het huidige proces te vervangen. Ik herken deze conclusies, die ten dele worden onderschreven door de resultaten

---

[2] Het VB is de invulling van de wijziging van de EU Richtlijn 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering en tot wijziging van Richtlijn 2009/101/EG.

[3] Raadpleegbaar via www.tweedekamer.nl.

van de pilot die in de periode september tot en met november is uitgevoerd. Het BIT geeft waardevolle adviezen die mij in staat stellen om de implementatie van dit systeem zo goed mogelijk voor te bereiden.

Mede gelet op de adviezen van het BIT is de planning van de implementatie van het VB een half jaar vooruitgeschoven. Het ontwerp is inmiddels op belangrijke punten aangepast en aanvullende maatregelen zijn gepland om de robuustheid van het VB te verbeteren. Deze licht ik hieronder toe voor elk van de vier delen van het BIT advies.

Ook ten aanzien van de overige twee door het BIT genoemde punten (duidelijkheid over kostenvergoedingen en capaciteit bij de beheerder) worden tijdig afdoende maatregelen getroffen door mijn Ministerie.

Aanbevelingen BIT

Binnen het project VB zijn gedurende het afgelopen jaar al concrete maatregelen genomen om het VB als systeem en de processen daaromheen te verbeteren en de aansluiting van banken goed voor te bereiden. De uitwerking daarvan heeft deels parallel gelopen met het onderzoek en de presentatie van de uitkomsten van het BIT. Om die reden is een belangrijk deel van de door het BIT geadviseerde maatregelen al geadresseerd of zelfs gerealiseerd. De door het BIT geadviseerde maatregelen staan hieronder vermeld. Per maatregel volgt hierop mijn reactie.

1. Pas ontwerp VB aan zodat nalevering gegevens mogelijk wordt

Zorg dat het voor opsporingsdiensten helder is of banken volledig zijn geweest in het beantwoorden van de onderzoeksvraag en of er nog informatie volgt. Hiervoor dient het ontwerp op twee punten te worden aangepast:

- *Gebruikers moeten kunnen zien welke gegevens missen in het antwoordbericht van banken en wat de oorzaak hiervan is. Bijvoorbeeld dat een bronsysteem met specifieke gegevens tijdelijk niet beschikbaar of nog niet aangesloten is. Wij adviseren om deze aanpassing door te voeren voordat het VB in productie gaat.*
- *Banken moeten gegevens na kunnen sturen als die niet binnen een aantal seconden beschikbaar zijn. Deze techniek kan ook gebruikt worden voor toekomstige uitbreidingen van het VB waarbij grotere hoeveelheden data, zoals financiële transacties in een specifieke periode, worden opgevraagd.*

Het ontwerp van het VB is inmiddels als volgt aangepast:

- Gegevens worden alleen geleverd door de bank als deze volgens de bank compleet zijn. Indien de bank niet binnen de vereiste reactietijd kan leveren of als één of meer van de systemen van de bank tijdelijk niet bereikbaar zijn, levert de bank geen gegevens. In het antwoordbericht van de bank is duidelijk waarom geen informatie wordt geleverd.
- Indien banken de gevraagde informatie niet tijdig kunnen leveren (binnen de voor het VB vastgestelde reactietijd van 30 seconden) wordt de vragende organisatie in de gelegenheid gesteld de gevraagde informatie op andere wijze op te vragen. In het antwoordbericht van de bank is duidelijk dat de informatie op andere wijze geleverd kan worden.
- Indien een bank nog niet is aangesloten op het VB en deze toch wordt bevraagd, geeft het VB daarvan een duidelijke melding.

2. Implementeer noodzakelijke beveiligingsmaatregelen

Gezien de gevoeligheid van de persoonsgegevens in zowel vraag- als antwoordberichten is het essentieel dat de gegevensstromen en de applicatie adequaat beveiligd zijn. Zorg voor minimaal de volgende beveiligingsmaatregelen:

- *Verleen toegang tot het VB op basis van verplichte «twee-factor-authenticatie», of bied het VB alleen aan vanaf een vertrouwd netwerk met authenticatie op een vergelijkbaar betrouwbaarheidsniveau.*

Ten tijde van de BIT toets werd het VB aangeboden op het besloten rijksbrede «Rijksweb». De vertrouwelijkheid van dit netwerk bleek onderwerp van discussie. Om die reden is besloten het VB alleen via het vertrouwde netwerk van het Ministerie van Justitie & Veiligheid aan te bieden. Deze verandering wordt in de eerste helft van 2019 geëffectueerd, voordat er gebruik gemaakt gaat worden van het VB.

- *Neem maatregelen zodat een bank kan vaststellen dat de vraag daadwerkelijk van het VB afkomstig is.*

Het VB heeft inmiddels een technische voorziening beschikbaar die banken kunnen gebruiken om te zien dat een vraag afkomstig is van het VB.

- *Zorg dat de toegang tot berichten tot een minimum wordt beperkt. Voer hiertoe een risicoanalyse uit om een afweging te maken tussen het belang van optimale, preventieve beveiliging middels end-to-end beveiliging versus betere detectie door de berichtenmakelaar JUBES op schadelijke software. Neem daarbij ook in overweging dat de VB berichten typisch kort zijn en alleen leesbare teksten bevatten zodat het verstoppen van schadelijke software daarin niet eenvoudig is.*

De door het BIT voorgestelde risicoanalyse wordt in de eerste helft van 2019 uitgevoerd.

- *Voer een penetratietest uit, kort voor het in productie brengen van het VB, op een omgeving die representatief is voor de definitieve productieomgeving.*

Een penetratietest op een omgeving die representatief is voor de productieomgeving van het VB heeft al met goed resultaat medio 2018 plaatsgevonden. Deze zal worden herhaald kort voor de in productie name.

- *Implementeer bij het IBO SIEM-software zodat beveiligingsincidenten snel kunnen worden gesignaleerd en afgehandeld.*

Voorbereidingen voor de aanschaf en installatie van SIEM-software zijn inmiddels gestart. Deze zal zijn ingericht vóórdat het VB operationeel in gebruik wordt genomen.

3. Zorg dat het IBO de gevraagde beschikbaarheid kan garanderen

- *Breng de dienstverlening van het IBO in lijn met de – door de opsporingsdiensten en Belastingdienst – gewenste beschikbaarheid van het VB. Zorg hiertoe dat het IBO voor de systemen van het VB een uitwijkmogelijkheid creëert in een tweede datacenter en een calamiteitenplan beschikbaar heeft. Hierdoor is de maximale uitvaltijd bij ernstige calamiteiten beperkt.*

De toekomstig beheerder van het VB, de Justitiële Informatiedienst (Justid/IBO) beheert al twee systemen die vergelijkbaar zijn met het VB. Daarvoor worden al enige tijd plannen ontwikkeld voor een uitwijkvoor-

ziening. In deze plannen wordt nu ook een uitwijkvoorziening voor het VB opgenomen. In het verlengde daarvan wordt door de beheerder vóór de inbeheername van het VB een calamiteitenplan opgeleverd.

4.Ontzorg de opsporingsdiensten tijdens de beginperiode

– Indien u ervoor kiest om het VB op 1 juli 2019 in gebruik te stellen, adviseren wij u gebruikers te ontzorgen zodat ze zo min mogelijk last ondervinden van banken die niet aangesloten zijn. De opsporingsdiensten kan de mogelijkheid geboden worden om via het VB gegevens uit te vragen bij alle banken via een tijdelijke workaround. Deze workaround kan georganiseerd worden door de gevraagde gegevens handmatig uit het VB naar de betreffende banken te versturen overeenkomstig het bestaande proces. Dus ook bij banken die nog niet zijn aangesloten.

Zoals gemeld is de planning van het project VB met een half jaar verlengd. Hierdoor hebben banken meer tijd om de aansluiting op het VB vóór de inwerkingtreding van de wet te realiseren. Mijn verwachting is dat de meeste banken vóór 1 januari 2020 zijn aangesloten.

- *Om het gebruik van deze werkwijze zoveel mogelijk te beperken is het van belang dat zoveel mogelijk banken voor 1 juli 2019 zijn aangesloten. Neem hiervoor de volgende maatregelen:*
  - *Zorg dat er voor banken een standaard aansluitproces wordt ontwikkeld met een heldere tijdslijn. Maak daarover tijdig afspraken met de banken.*
  - *Maak een planning voor de gefaseerde aansluiting van banken, rekening houdend met de beperkte capaciteit van het IBO. Laat de grote banken als eerste aansluiten omdat deze de meeste bevragingen krijgen.*

Binnen het project VB is een standaardproces voor aansluiting op het VB ontwikkeld. Dit proces is inmiddels met alle banken afzonderlijk besproken. Met elke bank afzonderlijk worden de komende maanden afspraken gemaakt over aansluiten en planning. Daarbij wordt rekening gehouden met de beschikbare capaciteit van Justid/IBO en tijdelijke extra capaciteit binnen het project VB. In dit verband zijn inmiddels concrete planningsafspraken gemaakt met de grote banken.

Tot slot

Gelet op het advies van het BIT, de reeds genomen maatregelen binnen het project VB en de op korte termijn te nemen maatregelen zoals hiervoor beschreven, heb ik er alle vertrouwen in dat het Verwijzingsportaal Bankgegevens tijdig en met alle noodzakelijke waarborgen, operationeel in gebruik genomen kan worden.

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