Bureau ICT-toetsing
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2511 AE Den Haag

Ministerie van Justitie en Veiligheid
De minister, de heer F.B.J. Grapperhaus
Postbus 20301
2500 EH Den Haag

Bureau ICT-toetsing
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Rijnstraat 50
Den Haag
Postbus 20011
2511 AE Den Haag
www.bureauicttoetsing.nl

Contactpersoon
BIT@rijksoverheid.nl

Kenmerk
2018-0000942828

Uw kenmerk
2190328/2190336

Datum: 10 december 2018
Betreft: Definitief BIT-advies project Verwijzingsportaal Bankgegevens

Geachte heer Grapperhaus,

U heeft het Bureau ICT-toetsing (BIT) verzocht een toets uit te voeren op het project Verwijzingsportaal Bankgegevens (VB). De opdrachtgever van dit project is de directeur van de Directie Rechtspleging en Criminaliteitsbestrijding van uw ministerie. In de inleiding vindt u een korte beschrijving van het project. Daarna geven we de conclusie van de toets, onze analyse en adviezen. We concentreren ons hierbij op de belangrijkste risico's van het project.

De politie, het Openbaar Ministerie, de Belastingdienst en bijzondere opsporingsdiensten mogen identificerende persoonsgegevens bij banken en betaaldienstverleners opvragen om te gebruiken voor hun opsporingstaken. Het project VB heeft als doel om het proces voor het opvragen en verstrekken van deze identificerende gegevens te automatiseren met behulp van een Verwijzingsportaal Bankgegevens.

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 opvragingen per jaar. Het project VB wil dit proces efficiënter maken door het opsporingsdiensten mogelijk te maken om via het Verwijzingsportaal 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 opvragingen via het portaal binnen een aantal seconden te beantwoorden[1].

Het aantal gebruikers van het toekomstige portaal is bij de meeste opsporings-diensten beperkt: van enkele tientallen tot honderden opsporingsambtenaren per dienst. Bij de politie gaat het om meer: circa 50.000 opsporingsambtenaren kunnen mogelijk toegang krijgen tot het VB. De Belastingdienst gaat het VB ook gebruiken om te controleren of opgegeven bankrekeningnummers overeenkomen met de gegevens van banken, om bijvoorbeeld fraude bij uitbetaling van toeslagen te voorkomen.

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

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.

Het project VB is gestart in 2015 en de planning is dat het portaal op 1 juli 2019 operationeel is. Dan moet het wetsvoorstel zijn goedgekeurd en moeten de banken zijn aangesloten op het VB. De bouw van het VB was ten tijde van onze toets technisch bijna klaar. In de tweede helft van 2018 vindt er een pilot plaats met twee banken en een aantal gebruikers bij opsporingsdiensten.

Voor de bouw van het VB heeft het project medewerkers ingehuurd van onder andere het Informatiepunt Bijzondere Opsporingsonderzoeken (IBO) en de Justitiële Informatiedienst (Justid) van uw ministerie. Het IBO is een onderdeel van Justid en gaat straks ook het beheer van het VB uitvoeren.

De kosten van het project zijn geraamd op € 9,1 miljoen. Deze raming is exclusief de kosten voor banken en opsporingsdiensten om aan te kunnen sluiten. JenV ontvangt voor 90% van de projectkosten een Europese subsidie. De overige 10% komen voor rekening van JenV en Financiën. Het beheer is geraamd op € 1,2 miljoen per jaar.

Wij hebben het project VB onderzocht in de periode van mei tot en met augustus 2018.

De conclusie van onze toets luidt als volgt:

Wij hebben geen twijfel over het nut en de noodzaak van het VB. Het VB zoals het nu is ontworpen is echter nog geen robuuste oplossing om het huidige proces goed te vervangen. Belangrijkste redenen hiervoor zijn het ontbreken van inzicht voor opsporingsambtenaren of de door banken aangeleverde gegevens compleet zijn, en het ontbreken van noodzakelijke beveiligingsmaatregelen. Daarnaast kan de gewenste beschikbaarheid van het VB nog niet worden gegarandeerd. Ook is het VB niet direct te gebruiken voor opvragingen bij alle banken, omdat banken waarschijnlijk niet allemaal op 1 juli 2019 zijn aangesloten.

Om het VB tot een succes te maken adviseren wij u 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.

Wij lichten onze conclusie hieronder toe.

HET VB IS NOG GEEN ROBUUSTE OPLOSSING

Het automatiseren van het vorderen van bankgegevens voor opsporings-doeleinden vinden wij een logische stap die bovendien vanuit Europa verplicht wordt gesteld. De aanpak van het project is het afgelopen jaar verbeterd en zit op het juiste spoor. Echter, de gekozen oplossing voor het VB is bij ingebruikname nog niet robuust genoeg om het huidige proces goed te kunnen vervangen. De redenen daarvoor zetten we hieronder uiteen.

[2] Het VB is de invulling van de aanstaande 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.

A. Opsporingsdiensten hebben geen zekerheid dat gegevens uit VB compleet zijn

Het huidige VB-ontwerp gaat uit van 'synchrone' uitwisseling van gegevens, waarbij een bank binnen een aantal seconden een antwoordbericht moet terugsturen naar het VB met de gevraagde gegevens. Er is geen rekening gehouden met situaties waarin banken niet binnen een aantal seconden alle gevraagde gegevens kunnen aanleveren. Wij verwachten dat deze situatie zich regelmatig voor zal doen:

- Banken kunnen bij de aansluiting op het VB veelal nog niet alle gegevens vanuit de eigen bronsystemen aanleveren. Met name historische gegevens (bijv. gemachtigden) en zakelijke klantgegevens zullen vaak niet direct op te leveren zijn.
- Een bancair bronsysteem kan tijdelijk niet beschikbaar zijn, bijvoorbeeld door storingen of onderhoudswerkzaamheden. Bij de primaire systemen zal dat niet vaak gebeuren, maar bij bijvoorbeeld systemen met historische gegevens kan dit wel voorkomen.

Het moet voor opsporingsdiensten glashelder zijn of de gevorderde gegevens volledig zijn aangeleverd of dat er nog specifieke informatie ontbreekt. In het ontwerp van het VB is er geen mogelijkheid voor banken om in het antwoordbericht aan te geven dat slechts een deel van de gevraagde gegevens is geleverd. Bovendien biedt het VB geen mogelijkheid om ontbrekende gegevens na te leveren. In het huidige handmatige proces treedt dit probleem niet op, omdat banken meer tijd hebben om de benodigde informatie op te zoeken. Het risico is daarom groot dat opsporingsambtenaren ervoor gaan kiezen om gegevens via het oude proces op te vragen, zodat ze meer zekerheid hebben over de volledigheid van de gegevens.

B. Er ontbreken noodzakelijke beveiligingsmaatregelen

Vraag- en antwoordberichten die via het VB lopen, bevatten gevoelige persoonsgegevens in het kader van opsporingsonderzoeken. Bovendien is het VB niet uitsluitend te benaderen vanuit vertrouwde netwerkomgevingen. Vandaar dat adequate beveiliging van de applicatie, de verbindingen en de berichten essentieel is. Wij constateren dat noodzakelijke beveiligingsmaatregelen ontbreken:

- Anders dan gesteld in de documentatie en geëist door de Baseline Informatiebeveiliging Rijksdienst wordt toegang tot het VB vanuit opsporingsdiensten niet verleend op basis van 'twee-factor authenticatie'. Het project heeft ervoor gekozen om toegang tot het VB te verlenen op basis van een gebruikersnaam en wachtwoord, in combinatie met beperking van de netwerkadressen vanaf waar het VB te benaderen is. Deze combinatie voldoet niet aan de gestelde eis. Een netwerkadres kan niet gebruikt worden als tweede factor omdat dit niet gekoppeld is aan een persoon, zoals dat wel geldt voor een bezits- of biometrisch kenmerk.
- Er is geen sprake van volledige (*end-to-end)* versleuteling van het berichtenverkeer van het VB tot aan de bank. In het voorgestelde ontwerp wordt de versleuteling onderbroken bij de tussenliggende berichtenmakelaar[3] binnen JenV. Reden hiervoor is dat JenV eerder heeft gekozen om berichten van applicaties bij de berichtenmakelaar te controleren op mogelijke schadelijke software. Ook zijn geen aanvullende maatregelen getroffen waardoor een bank kan vaststellen dat de vraag daadwerkelijk van het VB afkomstig is. Hierdoor bestaan onnodige risico's dat iemand met toegang tot

[3] JenV maakt gebruik van een zogenaamde 'message broker' (berichtenmakelaar), die JUstitie BErichten Service (JUBES) wordt genoemd. Dit is een Justitiebrede voorziening, die het elektronische berichtenverkeer tussen JenV en haar ketenpartners buiten JenV faciliteert.

de berichtenmakelaar inzage krijgt in de opvragingen van opsporingsdiensten of zelfstandig informatie opvraagt. Het ontbreken van volledige berichtenversleuteling is bovendien niet in lijn met gangbare beveiligingsnormen en het uitgangspunt van minimale gegevensverwerking vanuit de Algemene Verordening Gegevensbescherming.
- Beoogd beheerder IBO heeft nog niet de middelen om de beveiliging van het VB goed te kunnen monitoren. Zo voorziet het IBO niet in *Security Information en Event Management* (SIEM)–software om direct mogelijke beveiligingsincidenten te constateren en maatregelen te treffen.

C. Beheerder IBO kan gewenste beschikbaarheid niet garanderen

Beoogd beheerder IBO kan de gewenste beschikbaarheid van het VB voor de opsporingsdiensten en de Belastingdienst niet garanderen. Het IBO heeft geen mogelijkheid om bij ernstige calamiteiten uit te wijken naar een ander datacenter. Dit heeft als gevolg dat het VB in dit soort situaties zeker twee weken niet beschikbaar is. Het ontbreekt bovendien aan een calamiteitenplan. Het IBO onderkent de noodzaak om op dit punt te professionaliseren zodat een hogere beschikbaarheid kan worden gegarandeerd, maar er zijn hiervoor nog geen concrete plannen en benodigde budgetten beschikbaar.

D. Banken waarschijnlijk niet allemaal in juli 2019 aangesloten

De kans is groot dat banken niet allemaal op 1 juli 2019 zijn aangesloten, waardoor een opsporingsambtenaar via het VB maar een gedeelte van de banken kan bevragen. Oorzaken voor het niet tijdig aansluiten zijn:
- Voor banken is de impact om aan te sluiten op het VB groter dan verwacht. Momenteel hebben twee banken een deel van de benodigde functionaliteit gebouwd voor deelname aan de pilot. De inspanning van deze banken was groter dan vooraf ingeschat. Wij verwachten dat dit ook voor veel andere banken zal gelden.
- Banken zullen wachten met voorbereidende werkzaamheden totdat het wetgevingstraject is afgerond. Het is onzeker wanneer dit exact gebeurt. Banken weten waarschijnlijk pas enkele maanden van tevoren de definitieve ingangsdatum van de wet.
- Onduidelijkheid over de vergoeding voor de banken leidt tot weerstand en mogelijk tot onnodige vertraging in het wetgevingstraject. In de huidige situatie krijgen de banken een operationele vergoeding per opsporingsverzoek. Het is onduidelijk of deze vergoeding in de nieuwe situatie blijft bestaan.
- Beheerder IBO heeft beperkte capaciteit en kan slechts een beperkt aantal banken per maand aansluiten. Vanuit het project is er nog geen implementatieplan met (gefaseerde) aansluitplanning beschikbaar.

ADVIES: VERBETER HET VB VÓÓR GROOTSCHALIGE INZET

Om het VB tot een succes te maken, adviseren wij om een aantal maatregelen te treffen zodat het VB een betrouwbare oplossing wordt die in alle situaties bruikbaar is voor de opsporingsdiensten en de Belastingdienst.

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.

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.
- Neem maatregelen zodat een bank kan vaststellen dat de vraag daadwerkelijk van het VB afkomstig is.
- 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.
- Voer een penetratietest uit, kort voor het in productie brengen van het VB, op een omgeving die representatief is voor de definitieve productieomgeving.
- Implementeer bij het IBO SIEM-software zodat beveiligingsincidenten snel kunnen worden gesignaleerd en afgehandeld.

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.

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.

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 opvragingen krijgen.

Bureau ICT-toetsing
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum
10 december 2018

Kenmerk
2018-0000942828

***

Wij danken het ministerie van JenV, opsporingsdiensten en banken voor hun openheid en medewerking bij deze toets. Wij hopen dat wij met dit advies een bijdrage leveren aan een succesvolle introductie van het VB.

Met de meeste hoogachting,
namens het Bureau ICT-toetsing,

prof. dr. Cokky Hilhorst
hoofd BIT