Marktverkenningsverslag versterking SOC functie SVB

SVB Project team Versterken SOC

14/2/2022

Versie 1.0

Inleiding

Voor de bescherming van de SVB tegen de bedreiging van cyber criminaliteit heeft de SVB het voornemen een Security Operations Center (SOC) dienst van een Managed Security Service Provider (MSSP) aan te besteden ter aanvulling en versterking op het SOC, die de SVB zelf al actief heeft. Als onderdeel van dit voornemen is er rond de jaarwisseling 2021 – 2022 een marktverkenning uitgevoerd met vijf leveranciers. Doel van deze marktverkenning is om inzicht te krijgen in het aanbod van de markt en om enkele beoogde uitgangspunten voor de uiteindelijke uitvraag te toetsen met de marktpartijen.

Dit document bevat de samenvatting van de antwoorden van de leveranciers op de vragen van SVB. Als commercieel vertrouwelijk geclassificeerde informatie is daarbij weggelaten en conclusies zijn niet te herleiden naar specifieke partijen.

De SVB zal naar eigen inzicht de conclusies uit dit verslag verwerken in de definitieve aanbestedingsstrategie en de opvolgende aanbesteding. Aan dit verslag kunnen geen rechten worden ontleend.

Inhoud

Vragen 1 en 2: Introductie

Vraag 1

Kunt u uw organisatie introduceren?

Hierbij kunt u denken aan n.a.w. gegevens, een opgave van uw(kern) activiteiten, de personeelsopbouw / omvang van uw organisatie.

Samenvatting antwoorden op vraag 1

Leveranciers bieden de gevraagde diensten:

- Security Monitoring
- Incident Response
- Threat Intelligence
- Vulnerability Monitoring
- Threat Hunting
- Advies

Leveranciers bieden ook diensten die niet in de uitvraag stonden zoals:

- Red Teams
- Pentest Teams
- Crypto en Consultancy activiteiten
- Security Training
- Security Device Management
- Malware-analyse
- Verkoop van security producten als software en appliances
- Niet security gerelateerde IT diensten, zoals IT hosting, cloud computing etc.

Vraag 2

Kunt u de activiteiten van uw organisatie in relatie tot de scope van deze marktverkenning (zie paragraaf 3.3. van het marktverkenningsdocument) uiteenzetten?

Samenvatting antwoorden op vraag 2

De leveranciers konden alle NCSC model gevraagde diensten leveren.

- Intelligence
- Baseline Security

- Monitoring
- Pentesting
- Forensisch

Scope van de gevraagde dienstverlening

Vraag 3

Heeft de SVB een uitvoerbare en realistische scope afbakening voor ogen (zie paragraaf 3.3. van het marktverkenningsdocument)? Zijn er bepaalde onderdelen waarvoor u adviseert dit anders in te richten?

Samenvatting antwoorden op vraag 3

Het dominante beeld is dat de leveranciers het zien als een realistische en uitvoerbare scope. Hierbij zijn verschillende aandachtspunten meegegeven, zoals:

- Intelligence: voeg toe dat de dienst intelligence moet leveren specifiek gericht op de SVB.
- Baseline Security:
    - voeg toe risk management van derde partijen, zoals in de supply chain.
    - beschrijf de gewenste vulnerability management dienst duidelijker
- Forensisch: scheidt SOC diensten van de forensische dienstverlening, aangezien het forensische onderzoek ook het functioneren van de bij het incident betrokken partijen moet bevatten.
- Contract: borg contractueel dat de MSSP akkoord gaat dat bij red team oefeningen ook het functioneren van de MSSP in scope is.
- Monitoring:
    - voeg Endpoint, Detection and Response Service toe
    - de scope van 600GB per dag is veel
        - dit kan betekenen dat inefficiënt data wordt verzameld voor het doel security monitoring, maar dit is ook het gevolg van dat de data voor andere doelen wordt gebruikt.
        - De 600GB per dag die op dit moment in de Splunk omgeving binnenkomt is waarschijnlijk veel meer data dan dat er voor de MSSP nodig is om de dienst uit te kunnen voeren
        - Security logging vaak wordt verzameld met de gedachte dat later nog wel eens use cases hierop worden gemaakt, dit gebeurt in de praktijk te weinig, waardoor deze benadering inefficiënt is.
    - Sluit aan op de use cases die worden ontwikkeld en beheerd door de maker. Voorbeelden zijn een Endpoint Detection & Response tool (bijvoorbeeld MS Defender for Endoint) of een Web Application Firewall. Hierbij is het niet nodig om nog de rauwe logging data naar de SIEM te sturen.
    - In het partnership is het noodzakelijk dat ook SVB mensen op stand-by heeft staan voor een security incident buiten werktijden.

- Het gebruik van verschillende leveranciers voor pentesten en monitoring is wenselijk, zodat de situatie 'slager die zijn eigen vlees keurt' voorkomen wordt.

Invulling van de gevraagde dienstverlening

Vraag 4

Eén van de onderdelen van de voorziene dienst is het bieden van ondersteuning aan het CSIRT (Computer Security Incident Response Team) in de afhandeling van grotere incidenten en cyber crisissen.

Wat is in het algemeen uw bijdrage aan de afhandeling van cyber incidenten? Hoe organiseert u in dit geval de afstemming met de klantorganisatie?

Samenvatting antwoorden op vraag 4

Alle leveranciers leveren ondersteuning in de afhandeling van grotere incidenten en cybercrisissen (CERT of CSIRT). Aandachtspunten hierbij zijn onder meer:

- De SOC van de MSSP moet aangesloten worden op de incident response processen van de SVB.
- CSIRT onder retainer of ad hoc beschikbaar tegen een hogere prijs
- Personeel
  - Personeel is aantoonbaar gekwalificeerd voor de taken door certificeringen.
  - Sommige medewerkers zijn ingeschreven in het Landelijk Register van Gerechtelijk Deskundigen voor de borging van de kwaliteit van rapportages voor indiening bij rechtzaken
- 24 x 7 telefonisch bereikbaar
- Goede voorbereiding door middel van o.a. on site service en jaarlijks oefenen
- Proactieve en reactieve incident response mogelijkheden

Vraag 5

Is het in uw ogen gangbaar/noodzakelijk om voor de betreffende dienstverlening on premise aanwezigheid te hebben bij de klantorganisatie? Zo ja, in welke omvang, welke criteria spelen hierbij een rol, en is dit op een kostenefficiënte wijze te organiseren?

Samenvatting antwoorden op vraag 5

Over het algemeen wordt een continue on premise aanwezigheid niet noodzakelijk geacht, bij enkele leveranciers is het wel mogelijk. Enkele aandachtspunten:

- Samenwerking en het elkaar leren kennen wordt wel belangrijk geacht
- Voor kennisoverdracht is het een optie om een security analist on premise te laten werken voor een aantal dagdelen per maand.
- Werkbezoeken door de SVB SOC medewerkers aan de locatie van de MSSP zijn een optie.

- Periodieke tactische en strategische overleggen zouden eventueel wel in persoon op kantoor kunnen plaatsvinden.

Vraag 6

Van de beschreven diensten, welke levert u (normaliter) in de Engelse taal of in de Nederlandse taal? Welke consequenties heeft het op het moment dat de SVB-eisen stelt aan de taalkeuze?

Samenvatting antwoorden op vraag 6

Meerdere leveranciers gaven aan dat alle diensten in het Nederlands en/of Engels geleverd kunnen worden soms m.u.v. een enkele dienst. De rapportage zijn vaak in het Engels aangezien de tooling in het Engels is. Het dominante beeld is dat leveranciers een harde taal eis op de Nederlandse taal niet noodzakelijk achten.

Vraag 7

Het landschap van de SVB beslaat diverse omgevingen welke wordt gehost door een ESP en door de SVB zelf. Zie hiervoor paragraaf 2.3 van het marktverkenningsdocument.

Is bekendheid met de platform technologie in uw optiek nodig om de MSSP-rol goed in te vullen? In welke mate heeft u in uw monitoringdienst en geautomatiseerde processen use case beschikbaar die in relatie tot deze platformen meerwaarde bieden?

Samenvatting antwoorden op vraag 7

Bekendheid met de platformtechnologie wordt in meer en mindere mate belangrijk geacht:

- Alle leveranciers gaven aan dat zij een tool hebben met use cases voor de genoemde architectuur.
- Sommige leveranciers gaven aan specifieke kennis te hebben van de bij SVB gehanteerde platformen, anderen gaven aan dat kennis van SVB specifieke IT niet noodzakelijk was
- Er werd aangegeven dat voor generieke IT en voor specifieke applicaties een analyse advies zal moeten worden geschreven.
- Sommige leveranciers gaven aan dat hun technische oplossing zodanig is opgebouwd dat zij technologie onafhankelijk logbronnen kunnen aansluiten.

Vraag 8

Welke dienstverlening kan geleverd worden en is wenselijk/gebruikelijk in deze ten aanzien van ingrijpen en/of interventies plegen bij (acute) dreigingen bij de klant.

Samenvatting antwoorden op vraag 8

Antwoorden op ingrijpen door de MSSP variëren op het spectrum van geheel niet tot volledig geautomatiseerd. De scope varieert op het spectrum van user accounts, workstations tot servers. Vanuit een extern SOC automatisch en direct zonder overleg ingrijpen wordt niet door alle leveranciers aanbevolen,

tenzij onder strikte voorwaarden en bijna altijd beperkt tot host isolation (het afzonderen van een computer van het netwerk). Enkele aandachtspunten:

- Security Orchestration Automation Response (SOAR) is benoemd als een markt standaard voor automatisch ingrijpen (o.a. isoleren van werkstation/server).
- Het gebruik van een notificatie matrix werd beschreven, waarmee afspraken kunnen worden gemaakt tussen de SVB en de MSSP onder welke omstandigheden ingegrepen kan worden.
- Een mogelijkheid vormt het ingrijpen via de EDR tooling van de SVB (Microsoft 365 Defender).
- Meestal vereist ingrijpen tussenkomst door een analist (dus niet vol automatisch). Geautomatiseerd ingrijpen wordt niet gezien als een doel, maar runbooks kunnen het wel mogelijk maken om snel in te grijpen.
- Ingrijpen is nog niet gebruikelijk, maar het begint wel een trend te worden.
- Ingrijpen op een incident is bij sommige leveranciers een aparte optie boven op de standaard monitoring en voor andere leveranciers wel onderdeel van de standaard dienstverlening.

Siem oplossing

Vraag 9

De intentie is dat de MSSP de loginformatie van de SVB verkrijgt door middel van de SIEM oplossing van de SVB (Splunk). Dit houdt in dat de MSSP toegang zal krijgen tot een deel van deze data t.b.v. de uitvoering van haar werkzaamheden.

Is dit voor u een werkbare/gangbare wijze van het verkrijgen van loginformatie? Wat zijn de aandachtspunten om hierbij rekening mee te houden?

Samenvatting antwoorden op vraag 9

Het doorgeven van logdata vanuit een SIEM is meestal de gangbare manier van werken. Het verzamelen van de SVB log data voordat het naar het platform van de SOC MSSP gaat vindt plaats op een spectrum variërend van een app op de Splunk omgeving van de SVB, het plaatsen van een virtual machine met een sensor tot een appliance met een sensor.

Meerdere leveranciers zien SIEM technologie naar de cloud bewegen, waarbij soms een migratie van de business applicaties van on-premise naar de cloud de drijvende kracht is, aangezien het efficiënter is om de SIEM nabij de logsources te houden. Daarbij wordt zowel voor traditionele merken als Splunk, die voorheen on premise draaiden, gekozen als Cloud native challengers, zoals Microsoft (Sentinel) of eigen ontwikkelde software. Migratie naar de cloud heeft tevens als voordeel dat de bandbreedte geen beperking meer is.

Vraag 10

In de constructie waarbij de MSSP de loginformatie verkrijgt vanuit de SIEM van de SVB (Splunk), wat zijn in uw ervaring de daarvoor te treffen beveiligingsmaatregelen? Welke alternatieven, indien van toepassing, zijn voor u wenselijk?

Samenvatting antwoorden op vraag 10

Alle leveranciers benoemen diverse beveiligingsmaatregelen, waaronder

- Versturen van alerts over een beveiligde verbinding (TLS) van de klant naar de MSSP.
- Toegang tot Splunk door de MSSP-analisten op basis van een VPN.
- Een dubbele S2S VPN voor naar 2 verschillende locaties t.b.v. redundantie.

Relatie SVB – MSSP

Vraag 11

De SVB acht het van belang dat een bepaalde mate van SVB-specifieke kennis door de MSSP wordt opgebouwd, en dat de MSSP zorgdraagt voor behoud van deze kennis en retentie van de direct bij de SVB betrokken medewerkers (specifiek de directe contactpunten naar de SVB).

Is dit aspect in uw ogen van belang? Hoe gaat u hier in de praktijk in algemene zin mee om?

Samenvatting antwoorden op vraag 11

Dit belang wordt in zijn algemeenheid onderschreven. Hierbij zijn benoemd:

- Een maand wordt gebruikt om een baseline te vormen en de oplossing van de MSSP te tunen voor de SVB-omgeving.
- Meedenken bij nieuwe applicaties en contracten aangezien de applicaties ook moeten worden aangesloten op de monitoring tool.
- Tijdelijk een SOC analist van de leverancier onsite bij de SVB met het SVB SOC laten samenwerken zodat de kennis goed geborgd wordt.
- De informatie over de klant (bijvoorbeeld contextuele data over de IT-omgeving en contactpersonen voor de runbooks) wordt vastgelegd in een systeem (knowledgebase) van de MSSP.
- Vaste mensen op het SVB account, die verantwoordelijk zijn voor de borging van SVB-kennis in de MSSP-organisatie.

Vraag 12

De SVB acht het van belang dat de MSSP voldoende prioriteit (bv management betrokkenheid) geeft aan de SVB. Is dit aspect in uw ogen van belang? Hoe gaat u hier in de praktijk in algemene zin mee om?

Samenvatting antwoorden op vraag 12

Dit belang wordt in zijn algemeenheid onderkent, de leveranciers verwijzen voor het belang van de prioriteit van de SVB voor de MSSP vooral naar het maken van goede afspraken over het governance model.

Vraag 13

De SVB acht het van belang dat de onafhankelijkheid geborgd is tussen de SOC-functie en de ESP's die operationele IT-diensten leveren aan de SVB. De MSSP dient voldoende objectief te opereren.

Is dit in uw ogen een relevant aspect? Zo ja, heeft u een suggestie hoe dit zou kunnen worden opgenomen in de aanbesteding?

Samenvatting antwoorden op vraag 13

Alle leveranciers achten (een bepaalde mate van) onafhankelijkheid van de MSSP van belang. De MSSP dient voldoende objectief te opereren. Enkele aandachtspunten:

- Er moet wel een goede samenwerking tussen MSSP en ESP zijn onder ander over het beschikbaar stellen van logdata vanuit de door de ESP beheerde omgevingen.
- Andersom moeten nieuwe ESP partners aansluiting met de SOC dienstverleners toestaan.
- Suggesties om dit in de aanbesteding te borgen zijn onder meer het uitsluiten van leveranciers die operationele diensten en het laten aantonen van de SOC dienstverlening als losse dienst via referenties.

Ontwikkelingen

Vraag 14

Vanuit de sourcing strategie SVB is de intentie om de Datacenter en hostingdiensten (tot en met het niveau van het technisch platform beheer) de komende jaren verder uit te besteden. Zo zullen de applicaties die nu binnen het eigen DMZ van de SVB draaien (op termijn) worden verplaatst naar een landingsplaats bij een ESP (ofwel als legacy hosting, ofwel private cloud hosting) ofwel verschuiven naar een publieke cloud. In deze bewegingen dient ook voor de uitbestede diensten de securityloginformatie aan te sluiten op het SOC (Splunk) welke weer informatie levert aan de MSSP ten behoeve van het integrale overzicht over alle diensten van de SVB.

Wat is uw ervaring met samenwerking met (andere) ESP's van de klantorganisatie of het verkrijgen van loginformatie van ESP's van de klantorganisatie? Wat zou de SVB hierover contractueel moeten regelen met deze ESP's?

Samenvatting antwoorden op vraag 14

De MSSP's geven aan dat het belangrijk is om goede afspraken te maken met de ESP's of Cloud leveranciers, en deze in een vroegtijdig stadium te betrekken. Te maken afspraken betreffen onder meer:

- Het beschikbaar stellen van a) log data, b) tooling (agents, etc.) en c) API's (voor automated response of allen binnenhalen van log uit de cloud).
- Het beschikbaar stellen van tijd voor het beantwoorden van vragen tijdens incidenten en algehele samenwerking.
- De reactietijd / prioriteit waarmee security vragen worden beantwoord.
- Change windows; in het bijzonder gerelateerd aan changes voor het mitigeren van hoge risico incidenten.

Sommige leveranciers waarschuwden SVB er voor dat sommige ESP's niet in staat zijn om logging aan te leveren van componenten, die gedeeld worden met andere klanten.

Vraag 15

In algemene zin speelt geautomatiseerde monitoring met toepassing van kunstmatige intelligentie (AI) een steeds grotere rol in het detecteren van verdachte patronen en cyberincidenten. Acht u dit van belang voor uw dienstverlening? Wat is hierover uw visie/roadmap voor de toekomst? Welke randvoorwaarden worden verwacht van de klant om dit goed in te regelen?

Samenvatting antwoorden op vraag 15

Het dominante beeld is dat leveranciers voorspellen dat AI bij zowel de aanvallers als de verdedigers steeds belangrijker gaan worden. Hierbij wordt verwezen naar termen als User Behaviour Analytics (UBA) of User & Entity Behaviour Analytics (UEBA) en Machine Learning. AI dient met name om de onbekende dreigingen te deteceren waarvan we op dit moment nog niet weten dat ze bestaan. Er wordt wel op gewezen dat AI vaak een leerperiode nodig heeft en de analisten moet ondersteunen in het detectieproces, niet vervangen.

Contractueel

Vraag 16

Heeft u bepaalde suggesties omtrent de looptijd van de te sluiten overeenkomst met de MSSP?

Samenvatting antwoorden op vraag 16

Alle leveranciers geven de voorkeur aan een lange looptijd van minimaal 3 tot, optioneel, 5 jaar of langer. De dienstverlening heeft enige implementatietijd en aanlooptijd nodig en daarom is een wat langere looptijd nodig om de dienst goed uit te nutten.

Vraag 17

De MSSP krijgt toegang tot informatie van de SVB met een hoogst vertrouwelijk karakter (BBN2). Wat zijn de waarborgen die u voor vergelijkbare klanten heeft ingericht om geheimhouding en integriteit te borgen? Hoe wordt bv. omgegaan met screening van medewerkers?

Samenvatting antwoorden op vraag 17

Er worden organisatorisch maatregelen geïmplementeerd als:

- Medewerkers moeten een Verklaring Omtrent Gedrag (VOG) overleggen.
- Afhankelijk van de vertrouwelijkheid van de werkzaamheden worden medewerkers gescreend.
- Informatie Beveiligingsbeleid
- ISMS
- Certificeringen (o.a. ISO27001 en ISO9001)
- Derde Partij verklaringen over werking maatregelen bij processen (ISAE 3402 / SOC 2 Type 2)
- Strikt aanname / selectieproces

Tevens worden technische maatregelen toegepast als 2 factor authenticatie, versleutelde verbindingen en gebruik van certificaten voor authenticatie.

Vraag 18

Welke assurance / formele audit rapportage kan worden verstrekt waarmee de opzet, het bestaan en de werking van een passend stelsel van beveiligingsmaatregelen kan worden aangetoond (denk aan een ISAE 3000 rapportage).

Samenvatting antwoorden op vraag 18

Meerdere leveranciers kunnen een ISO9001 en ISO27001 certificaat overleggen.

Rapportage

Vraag 19

Wat zijn de kpi's die u normaliter hanteert om te rapporteren over dienstverlening zoals door de SVB geschetst? Welke rapportagevorm hanteert u?

Samenvatting antwoorden op vraag 19

Leveranciers hanteren verschillende kpi's aan de hand waarvan over de dienstverlening wordt gerapporteerd. Centraal hierin staan kpi's met betrekking tot beschikbaarheid en incident response maar ook zijn door een aantal leveranciers kpi's benoemd m.b.t. het percentage van binnen de tijd aangemaakte cases en het percentage binnen de tijd gehaalde onderzoeken per incident.

Leveranciers bieden rapportages met verschillende frequenties (wekelijks/maandelijks/per kwartaal) en meerdere leveranciers bieden raadpleegfuncties door middel van een portaalfunctie.

Vraag 20

Voorzien uw rapportages in een opsplitsing naar diverse organisatieniveaus (operationeel/tactisch/strategisch).

Samenvatting antwoorden op vraag 20

Alle leveranciers geven aan dat ze verschillende rapportage mogelijkheden hebben, maar niet allemaal maakten ze een duidelijk onderscheid in organisatieniveaus.

Implementatie

Vraag 21

Welke aanpak adviseert u de SVB ten aanzien van de implementatie van de dienstverlening zoals omschreven? Welke doorlooptijd ervaart u bij dergelijke implementatietrajecten? Welke verwachtingen zijn er over de bemensing bij SVB en beschikbaarheid in uren?

Samenvatting antwoorden op vraag 21

De verschillende leveranciers gaven verschillende indicatieve doorlooptijden aan, variërend van 4 – 6 weken vanaf de start van de installatie tot 6 tot 12 maanden. De verschillende leveranciers stelden ook diverse samenstellingen voor de benodigde bemensing bij SVB voor, met onder andere betrokkenheid van een Projectmanager, diensteigenaren, architect en SOC specialisten.

De leveranciers benadrukten een gefaseerde uitrol van de diensten.

Aanbesteding en Kosten

Vraag 22

Kunt u een indicatieve bandbreedte aangeven voor het budget dat de SVB zou moeten reserveren voor de implementatie van de dienstverlening zoals omschreven?

Samenvatting antwoorden op vraag 22

De antwoorden van de leveranciers op deze vraag worden niet gedeeld.

Vraag 23

Welke soorten vaste kosten (per maand) en welke variabele kosten zullen er voor deze dienstverlening in rekening worden gebracht? Met andere woorden, wat is een gangbaar afrekenmodel voor deze dienstverlening uitgaande van de scope zoals deze beschreven is in de uitnodiging van de marktverkenning?

In welke mate speelt het aantal servers/nodes hierbij een rol?

Voegt u eventueel een prijsmodel toe zoals u dit voor deze dienstverlening hanteert.

Samenvatting antwoorden op vraag 23

De leveranciers hanteren afrekenmodellen met verschillende parameters. Het meest dominant zijn de verrekening op basis van de hoeveelheid GB logging data per maand en de verrekening op basis van het aantal aangesloten databronnen of servers / nodes. Leveranciers maken over het algemeen onderscheid tussen variabele kosten en vaste kosten. Vaste kosten zijn onder meer gericht op de implementatie en de retainer functie waarbij vervolgens een uurloon geldt voor de ingezette medewerkers bij forensich onderzoek.

Vraag 24

Welke informatie heeft u van de SVB nodig in de Europese aanbesteding om tot een offertestelling (financiële inschrijving) te komen? Denk hierbij aan omvang van gebruikers, systemen, e.d.

Samenvatting antwoorden op vraag 24

Dominant wordt hierbij genoemd de hoeveelheid logging en/of het aantal essentiële log bronnen. Daarnaast worden verschillende kenmerken gevraagd over de omgeving zoals het aantal/type appliances die aan het SIEM zijn gekoppeld, aantal VM’s, aantal gebruikers etc.

Vraag 25

Kunt u een niet bindende indicatieve bandbreedte aangeven voor het budget dat de SVB zou moeten reserveren voor de geschetste dienstverlening?

Samenvatting antwoorden op vraag 25

De antwoorden van de leveranciers op deze vragen worden niet gedeeld.

Vraag 26

Welke vraag hebben we niet gesteld maar zou volgens u wel gesteld moeten worden? Wat zou uw antwoord dan zijn op deze vraag?

Samenvatting antwoorden op vraag 26

Hierbij zijn verschillende suggesties benoemd, onder andere:

Met betrekking tot de aanbesteding:

- hanteer een niet-openbare procedure.
- Leg de focus op de kwaliteit (niet op de prijs).
- Geef een duidelijke situatieschets en scope omschrijving.
- Hanteer objectieve kwalitatieve gunningscriteria.
- hanteer eventueel een demo bij de aanbesteding.
- Hanteer referentie gesprekken om de kwaliteit duidelijk te maken.

Met betrekking tot de dienstverlening

- Maak Deep Packet Inspection onderdeel van Intrusion Detection Management
- Overweeg om beheer van de SIEM omgeving over te laten nemen
- Dwing mogelijkheid tot doen van externe audits af
- Creëer een partnership waarbij SVB ook kennis heeft van security.

www.svb.nl

15/16

voor het leven
Sociale Verzekeringsbank