Dreigingsanalyse Kaspersky Labs

Managementsamenvatting

Aanleiding voor deze analyse is berichtgeving in media omtrent verdenkingen van onbehoorlijk handelen van Russische antivirussoftwareontwikkelaar Kaspersky Labs. Dit mede in de context van bevindingen over de dreiging die uitgaat van statelijke actoren in het CyberSecurity Beeld Nederland en openbare jaarverslagen van de AIVD en MIVD. De analyse is gebaseerd op open bronnen.

Conclusie 1: Vanwege de aard van een AV-bedrijf en de producten en diensten kan misbruik een aantrekkelijk cybermiddel zijn voor een statelijke (of andere) actor. Of dit middel ook daadwerkelijk ingezet wordt, is afhankelijk van de intenties van de betreffende actor en de mogelijkheden voor misbruik.

Conclusie 2: Wanneer misbruik plaatsvindt van diensten en producten van AV-bedrijven, zoals Kaspersky, vormt dit een dreiging voor de Nationale Veiligheid door:

1. Aantasting van de cybersecurity van informatie en machines met als motief sabotage. Deze dreiging heeft de meeste impact.
2. Aantasting van de vertrouwelijkheid van informatie en machines met als motief spionage.
3. Ontwikkeling van geavanceerde aanvalstechnieken. Het motief is om op lange termijn aanvals- en verdedigingscapaciteit op te bouwen. Daadwerkelijk effect vindt pas plaats bij actieve inzet van de technieken.

Conclusie 3: Wat betreft de manifestatie van de geïdentificeerde dreigingen zijn verschillende scenario's voorstelbaar. Op dit moment is geen sluitend bewijs te vinden in open bronnen voor één of meerdere van de scenario's en kan er daarom geen uitsluitsel gegeven worden of Kaspersky op dit moment actief een dreiging vormt voor de Nationale Veiligheid. De dreiging van statelijke actoren in het digitale domein en de wetgeving met betrekking tot cryptografie en de samenwerking met de FSB moet beschouwd worden als een risico.

Conclusie 3A: Het is waarschijnlijk dat Kaspersky door de Russische overheid gedwongen wordt om samen te werken, maar dat eigenlijk niet wil (scenario bewust-ongewild).

Conclusie 3B: Het is waarschijnlijk dat Kaspersky geïnfiltreerd en gecompromitteerd is of wordt door een andere (dan de Russische) overheid (onbewust-ongewild).

Tot slot moet worden opgemerkt dat ook van andere AV-bedrijven dezelfde dreiging kan uitgaan als die van Kaspersky en soortgelijke scenario's denkbaar zijn. Andere AV-bedrijven hebben dezelfde middelen en kunnen ook door hun respectievelijke overheden in meer of mindere mate gedwongen worden tot samenwerking.

1 Inleiding

1.1 Aanleiding

Vooral sinds de eerste helft van 2017 wordt in de media gesproken over verdenkingen van spionage door Kaspersky Labs (hierna Kaspersky) bij hun klanten. Sindsdien heeft het Department of Homeland Security in de Verenigde Staten een bindende order uitgevaardigd dat Kaspersky producten uit de Amerikaanse overheid verbant. Deze order is in december 2017 bekrachtigd door president Trump. Het Britse National Cyber Security Centre heeft een advies afgegeven waarin het dringend verzoekt om binnen de overheid af te zien van Russische softwareproviders op systemen waarop gevoelige informatie staat. Tot dusver is er geen stuk gepubliceerd door een overheid of autoriteit waar daadwerkelijk verdenkingen of beschuldigingen in staan. Het Duitse cyber agentschap Bundesambt für Sicherheit in der Informationstechnik (BSI) heeft publiekelijk kenbaar gemaakt dat zij geen bewijs hebben kunnen vinden voor spionage door de Russische overheid via Kaspersky. Volgens open bronnen heeft een Israëlische inlichtingendienst Kaspersky gehackt en stelt deze dienst dat er wel bewijs is dat Kaspersky doelgericht en systematisch gespioneerd heeft op Amerikaanse inlichtingenoperaties. Ook stelt de berichtgeving dat Kaspersky relaties heeft met de Russische binnenlandse veiligheidsdienst, Federalnaja Sloezjba Bezopasnosti (FSB). Over de oorsprong en aard van deze relaties wordt gespeculeerd.

Wat bij deze verdenkingen opgemerkt moet worden is dat in het verleden vaker buitenlandse softwareproviders zijn buitengesloten. China heeft het gebruik van Microsoft Windows 8 in 2014 verboden op overheidscomputers. Vanwege mogelijke informatie-lekken werd in datzelfde jaar ook de Amerikaanse softwareprovider Symantec verboden, die vergelijkbare diensten aanbiedt als Kaspersky. Rusland streeft er sinds 2014 naar om onafhankelijker te worden van buitenlandse softwareproviders. Opvallend is dat deze veranderingen komen na de onthullingen door voormalig National Security Agency-medewerker (NSA) Edward Snowden.

1.2 Doel

Het verkrijgen van inzicht in hoeverre producten en diensten van Kaspersky een dreiging vormen voor de Nationale Veiligheid ten behoeve van besluitvorming in de RVI over de mate en wijze van eventuele mitigatie van mogelijke geïdentificeerde dreigingen.

1.3 Methode

De informatie weergegeven in dit stuk is vergaard via open bronnen, zowel media als rapporten. De gebruikte bronnen zijn geselecteerd omdat deze in het verleden overwegend juiste informatie en betrouwbare analyses hebben gepubliceerd.

1.4 Leeswijzer

Hoewel er situaties zijn beschreven die uniek zijn voor Kaspersky, geldt voor de meeste dreigingen en scenario's dat deze ook toepasbaar zijn op andere antivirusproducten en antivirusbedrijven. Daarnaast werken de meeste cybersecurity bedrijven, waaronder ook antivirusbedrijven, regelmatig samen met overheden om te assisteren bij misdrijven waarbij computers gebruikt zijn. Dit stuk gaat uit van een samenwerking tussen een antivirusbedrijf en een overheid buiten deze gebruikelijke kaders van assistentie verlenen aan een overheid. Tot slot, moet in acht genomen worden dat attributie van bijvoorbeeld aangetroffen malware aan een actor complex is.

2 Context

2.1 Kaspersky Labs

Het Russische Kaspersky Labs is een van de grootste antivirus (AV) en cybersecurity software bedrijven ter wereld (verder AV-bedrijf). Naar schatting heeft het ongeveer 400 miljoen gebruikers, waarvan de helft de AV-pakketten gebruikt. Enkele van de andere producten die het bedrijf aanbiedt zijn endpoint beveiliging, een vorm van cloudbeveiliging, een ondersteunend software pakket voor Security Operation Centres en een operating systeem voor vitale infrastructuur. Deze verschillende diensten worden aangeboden aan particulieren, midden- en kleinbedrijf en grote organisaties. Verder is het waarschijnlijk dat Kaspersky, net als andere AV-bedrijven, toeleverancier is van producten van andere fabrikanten, waar slecht tot geen zicht op is en zeer beperkte informatie over verstrekt wordt. Inmiddels bestaat het bedrijf van Yevgeni Kaspersky 20 jaar en heeft kantoren wereldwijd, inclusief een vestiging in Utrecht.

2.2 Rol van antivirus software

AV-software moet kwaadaardige software, ook wel malware[1], opsporen. Voor optimale bescherming heeft de software volledige toegang tot de bestanden en besturingssystemen op een computer of server (hierna machine) nodig. Het programma herkent dreigingen op basis van een signatuur of gedraging dat het vergelijkt met een dreigingen-bibliotheek die constant wordt geüpdatet. Wanneer er een dreiging is gedetecteerd op een machine, wordt de informatie opgestuurd voor diagnose en evaluatie (automatisch of na goedkeuring van de beheerder). Dit maakt het up-to-date houden van de bibliotheek mogelijk. Naast de verzending voor diagnose, wordt de kwaadaardige software onschadelijk gemaakt. Malware kan op veel verschillende soorten systemen voorkomen omdat niet alleen computers gevoelig zijn voor infectie, maar ook industriële systemen en mobiele apparaten.

2.3 Dreiging statelijke actoren in het digitale domein

Het CyberSecurity Beeld Nederland (CSBN) en openbare jaarverslagen van de AIVD en MIVD gaan in op deze dreiging. Statelijke actoren vormen, samen met beroepscriminelen, de grootste dreiging en richten de meeste schade aan. Steeds meer landen hebben zich de afgelopen jaren de mogelijkheden verschaft om inlichtingen in te winnen via het digitale domein. Veel landen investeren in het opzetten van (militaire) offensieve digitale capaciteiten. Digitale middelen worden gebruikt voor beïnvloedings- en informatieoperaties. De Nederlandse inlichtingendiensten onderkennen dat veel landen investeren in het opzetten van digitale capaciteiten gericht op de (toekomstige) sabotage van vitale processen en deze ook daadwerkelijk inzetten. De inlichtingendiensten nemen ook waar dat meerdere statelijke actoren structureel particuliere ICT bedrijven als dekmantel gebruiken om hun digitale spionageactiviteiten te verhullen.

Volgens Nederlandse inlichtingendiensten ontwikkelen Russische inlichtingendiensten al jarenlang zeer aanzienlijke capaciteiten in het digitale domein. Naast een uitgebreid programma om digitale communicatie te onderscheppen, zijn er ook Russische hackers actief voor de Russische staat. Het defensie-, binnenland- en buitenlandbeleid van de Russische Federatie speelt een doorslaggevende rol bij de keuze van de doelwitten van de hackers. Rusland heeft ook toegang tot capaciteiten die

[1] Hoewel vaak in de volksmond antivirus genoemd, is een geschiktere naam voor deze software vaak antimalware. Een virus is slechts één categorie malware.

geschikt zijn om conventionele militaire inzet te ondersteunen in het digitale domein, bijvoorbeeld door middel van digitale aanvallen op kritieke infrastructuur in andere landen.

3 Dreigingen

3.1 Inleiding

Vanwege de aard van een AV-bedrijf en de producten en diensten kan misbruik een aantrekkelijk cybermiddel zijn voor een statelijke (of andere) actor. Of dit middel ook daadwerkelijk ingezet wordt, is afhankelijk van de intenties van de betreffende actor en de mogelijkheden voor misbruik.

Er zijn drie dreigingen die uitgaan van een AV-bedrijf wanneer misbruik plaatsvindt:

1. Aantasting cybersecurity ten behoeve van sabotage
2. Aantasting vertrouwelijkheid ten behoeve van spionage
3. Ontwikkeling van geavanceerde aanvalstechnieken

Deze dreigingen komen voort uit de eerder geschetste aard van AV-software die overal toegang toe moet hebben en direct verbinding moet kunnen maken met een machine wanneer nodig. Hierdoor kan misbruik eenvoudig plaatsvinden.

1. Aantasting cybersecurity ten behoeve van sabotage

De constante connectiviteit van het AV-bedrijf met zijn klanten zou uitgebuit kunnen worden door ongeoorloofde software te plaatsen op aangesloten machines. Deze software zou de systeeminstellingen van machines kunnen aanpassen. Op bestandsniveau zou het niet alleen de vertrouwelijkheid, maar ook de integriteit kunnen aantasten. Het aanpassen van bijvoorbeeld bestanden zou voor misleidende doeleinden gebruikt kunnen worden, maar ook om iets te verhullen. Ook zou het met deze strategie mogelijk zijn de toegang tot informatie te weigeren of de informatie te vernietigen. Een actor kan in eerste instantie alleen voorbereidingshandelingen treffen en pas later de daadwerkelijke operatie uitvoeren. Het motief voor deze strategie is overwegend sabotage.

2. Aantasting vertrouwelijkheid ten behoeve van spionage

Het verzamelen van informatie vanaf een machine die AV-software draait, zonder dat de eindgebruiker hier wat van merkt, kan relatief eenvoudig zijn. Omdat de machine van de eindgebruiker structureel in verbinding staat met de servers van het AV-bedrijf vindt het uploaden en downloaden van informatie constant plaats via de legitieme software. Wanneer een actor in de machine van de eindgebruiker zou willen zoeken en de vertrouwelijkheid van bestanden zou willen aantasten, zou er geen verandering voor de gebruiker merkbaar zijn. Hierdoor zou een kwaadwillende partij langdurig op een machine actief kunnen zijn. Achterliggend motief achter deze strategie is overwegend spionage.

3. Ontwikkeling van geavanceerde aanvalstechnieken

Op basis van de informatie over malware die een AV-bedrijf op constante basis verzamelt, zou het kunnen werken aan het muteren van de geïdentificeerde malware, of onbekende kwetsbaarheden (zero-days) kunnen benutten voor nieuwe of gemuteerde malware. Op deze manier zouden geavanceerde aanvalstechnieken ontwikkeld kunnen worden, waarbij het niet nodig is een machine

te compromitteren. De bibliotheek van het AV-bedrijf wordt slechts gebruikt voor doeleinden anders dan bedoeld. Motief voor deze strategie is op lange termijn aanvals- en verdedigingscapaciteit te creëren.

3.2 Impact van de dreigingen

De dreiging met als motief sabotage zou de meeste impact hebben. Sabotage heeft bij ontdekking het gevolg dat alle machines en systemen die in verbinding stonden met het AV-bedrijf gewantrouwd moeten worden. Hierdoor zal die digitale omgeving opnieuw geëvalueerd moeten worden op vertrouwelijkheid, integriteit en beschikbaarheid. Mitigatie op overheidsniveau vindt deels plaats door aparte netwerken te gebruiken voor de toegang tot gerubriceerde informatie. De strategie van spionage is mogelijk aantrekkelijker omdat de kans op ontdekking kleiner is. De impact is nog altijd aanzienlijk omdat het gevoelige of geheime informatie kan compromitteren. De laatstgenoemde dreiging waarin geavanceerde aanvalstechnieken worden ontwikkeld zou een minder grote impact hebben zolang deze technieken niet daadwerkelijk worden ingezet. Daarnaast zijn er andere partijen dan een AV-bedrijf die deze aanvalstechnieken kunnen ontwikkelen. Ook is de machine van de klant niet gecompromitteerd.

4 Scenario's

4.1 Inleiding

Er zijn vijf verschillende scenario's voor misbruik van de producten en diensten van Kaspersky geïdentificeerd die op waarschijnlijkheid beoordeeld kunnen worden:

1. Bewust-gewilde betrokkenheid bij misbruik
2. Bewust-ongewilde betrokkenheid bij misbruik
3. Onbewust-ongewilde betrokkenheid – compromitteren door de Russische overheid
4. Onbewust-ongewilde betrokkenheid – compromitteren door een andere overheid
5. Beschuldigingen tegen Kaspersky zijn ongefundeerd

Per scenario volgt een beschrijving van de situatie zoals het zich voor zou kunnen doen, welke motivatie er achter zou kunnen zitten en wordt de berichtgeving dat het scenario onderschrijft dan wel tegenspreekt behandeld. Voor het conceptualiseren van de scenario's zijn de scenario's tegen twee assen uitgezet. De eerste as geeft de mate weer waarin Kaspersky zich bewust is van het ongewenste handelen richting klanten (bewust-onbewust), de andere as geeft weer de mate waarin Kaspersky bereid is mee te werken aan het ongewenste handelen (gewild-ongewild). Het scenario onbewust-gewild is niet uitgewerkt omdat deze analytisch als zeer onwaarschijnlijk bevonden is. Opgemerkt moet worden dat er tot op heden nog geen publiek toetsbaar bewijs is geleverd voor enig scenario (zowel voor als tegen). Ter verduidelijking van de scenario's volgt eerst een kort overzicht met betrekking tot Russische wetgeving die van toepassing is op Kaspersky.

4.2 Russische wetgeving van toepassing op Kaspersky

Er bestaat een zeer strenge wetgeving in Rusland met betrekking tot bedrijven die met cryptografie werken. Licenties die het gebruik toestaan, moeten bij het FSB Bureau voor Licenties, Certificering en de Beveiliging van Staatsgeheimen (FSB-TSLSZ) aangevraagd worden. Kaspersky heeft een licentie nodig omdat een klein deel van de producten data-encryptie mogelijkheden biedt, waardoor het

hele bedrijf onder de wetgeving valt. In de wetten met betrekking tot FSB-TSLSZ staan de volgende verplichtingen voor bedrijven met een dergelijk certificaat:

- uitvoeren van operationele zoekopdrachten om spionage [...] tegen te gaan;
- binnendringen van buitenlandse inlichtingendiensten [...] die een bedreiging vormen;
- assisteren van de FSB in het uitvoeren van FSB verantwoordelijkheden;
- leveren van extra hard- of software of anderzijds technische ondersteuning voor de FSB;
- toestaan van FSB medewerkers binnen de eigen organisatie.[2]

Wettelijk bestaan er dus verplichte banden tussen Kaspersky en de FSB. De certificaten afgegeven door de FSB zijn beschikbaar op de Russische Kaspersky-website. Het is op dit moment niet met publieke bronnen te toetsen op welke wijze en hoe vaak de FSB zich beroept op deze wetgeving.

1. Bewust-gewild

In dit scenario zou Kaspersky vrijwillig samenwerken met de Russische overheid. Dit zou door het AV-bedrijf aangeboden kunnen zijn, of dit zou hen gevraagd kunnen zijn. Het is mogelijk dat Kaspersky actief werkt met de Russische overheid uit loyaliteit en vaderlandsliefde, ook aangeboden gunsten kunnen meewegen. De Russische overheid zou in dit scenario niet alleen toegang kunnen hebben tot informatie van Kaspersky zelf of van hun klanten, maar ook tot medewerkers die voor verschillende doeleinden ingezet zouden kunnen worden. Vrijwillig meewerken door Kaspersky zou voor de medewerkers ook veiligheidsrisico's beperken. Een reden voor Kaspersky om deze samenwerking niet te willen, zou kunnen zijn dat het de geloofwaardigheid en integriteit van het bedrijf zou aantasten ten overstaan van internationale klanten.

Er zijn ongeveer even veel media berichten die voor als tegen het scenario spreken. Yevgeni Kaspersky heeft zich in de media verscheidene keren uitgesproken om verdenkingen te weerleggen en onafhankelijk functioneren van het bedrijf Kaspersky te benadrukken. Ook het Kremlin stelt geen bijzondere relatie met het AV-bedrijf te hebben. Door marktwerking binnen de AV industrie zou grootschalig ongericht misbruik waarschijnlijk opvallen. De aanbieders vergelijken elkaars producten regelmatig waardoor afwijkingen in de code of signaturen en/of gedragingen ontdekt zouden worden. Een in december 2017 op Facebook gepubliceerd document zou een 'ongewone nauwe samenwerking' tussen Kaspersky en het Kremlin bewijzen. Ondanks de media-aandacht wordt aan de authenticiteit van het document getwijfeld. Verdenkingen tegen Kaspersky worden volgens media verder aangewakkerd door een Israëlische inlichtingendienst. Deze zou Kaspersky in 2015 geïnfiltreerd hebben en er werd geconstateerd dat er actief op lopende inlichtingenoperaties van de NSA gezocht werd. Verder wordt in de media gewezen op een reorganisatie die in 2012 plaatsvond, waarbij veel nieuwe hooggeplaatste managers aangesteld zijn met een Russische inlichtingenachtergrond, en zouden bestuurs- en aandeelhoudersvergaderingen niet langer in het Engels gevoerd worden maar in het Russisch. Ook worden de wekelijkse *Banya* (badhuis, red.) bezoeken van Yevgeni Kaspersky met verschillende Russische ambtenaren verdacht gevonden, net als Kaspersky's KGB (voorloper van de FSB) opleiding. Tot slot wordt Kaspersky's voormalige functie bij de voormalige militaire inlichtingendienst in de media als verdacht aangemerkt.

[2] ,,Russian Laws and Regulations: Implications for Kaspersky," *Wired Magazine*, Engels, zomer 2012, hxxps://www[.]wired[.]com/images_blogs/dangerroom/2012/07/Russian-Laws-and-Regulations-and-Implications-for-Kaspersky-Labs.pdf. Benaderd op 15 december 2017.

2. Bewust-ongewild

Voor het scenario bewust-ongewild wordt er van uitgegaan dat Kaspersky niet buiten de afgesproken kaders als AV-bedrijf wil functioneren, maar hiertoe wordt gedwongen door de Russische overheid. Reden voor Kaspersky om niet mee te willen werken zou angst kunnen zijn voor reputatieschade en een verlies van klanten buiten Rusland. Het is echter onwaarschijnlijk dat een weigering vanuit Kaspersky door de Russische overheid zou worden geaccepteerd. De wetten rondom bedrijven met het FSB-TSLSZ certificaat zullen dan zeker aangehaald worden en pressiemiddelen op de persoonlijke levens van medewerkers zouden dan mogelijk niet geschuwd worden.

De meeste berichtgeving onderschrijft dit scenario; er zijn weinig publicaties die het tegenspreken. Volgens de media zou bewijs voor een ongewenste maar gedwongen inmenging van de Russische overheid binnen Kaspersky gevonden kunnen worden in de organisatorische veranderingen die zijn doorgevoerd in 2012. Ook de gepubliceerde informatie over de vermeende zoekopdrachten naar inlichtingenonderzoeken zou aangemerkt kunnen worden als bewijs voor dit scenario. Er zijn op dit moment geen berichten die het scenario tegenspreken. Ook de wetten zoals eerder in dit hoofdstuk beschreven zouden op ieder moment gebruikt kunnen worden en de in die wet beschreven verplichtingen onderschrijven het scenario eveneens.

3. Onbewust-ongewild – compromitteren door de Russische overheid

Het scenario onbewust-ongewild illustreert een situatie waarin Kaspersky geïnfiltreerd is door de Russische overheid, die het bedrijf zou gebruiken en misbruiken ter bevordering van de eigen agenda. Kaspersky zou in dit geval eventuele eerdere aanvragen tot samenwerking om moverende redenen hebben afgewezen, maar het is ook mogelijk dat Kaspersky niet gevraagd is samen te werken. Er is dan geen keuze of motivatie van Kaspersky. Voor de Russische overheid zou het binnendringen van Kaspersky toegang bieden tot een grote hoeveelheid informatie en een omvangrijk netwerk. Daarnaast zou het infiltreren zonder medeweten van Kaspersky geen publiek spoor achterlaten, waardoor het bedrijf minder gewantrouwd zou worden en dus langer beschikbaar blijft als informatiebron. En de Russische overheid kan dit scenario altijd ontkennen.

Binnen de huidige berichtgeving zijn er geen publicaties die voor of tegen het scenario spreken. Het enige dat in overweging genomen zou moeten worden is een verklaring van het BSI (Duits cyberagentschap), waaruit op te maken is dat onderzoek niet heeft uitgewezen dat Kaspersky ingezet is door Russische hackers.

4. Onbewust-ongewild – compromitteren door een andere overheid

Een andere situatie voor onbewust-ongewild is de mogelijkheid dat het bedrijf door een andere overheid dan de Russische wordt misbruikt. De motivatie van deze (onbekende) overheid zou kunnen zijn dat er een besef is van de hoeveelheid informatie en systemen waartoe Kaspersky toegang heeft en deze wil uitbuiten. Een andere motivatie zou kunnen zijn dat Kaspersky als bedrijf niet vertrouwd wordt en er onderzoek gedaan wordt naar onbehoorlijke gedragingen door het AV-bedrijf, of naar de inmenging van de Russische overheid in het bedrijf. Ook is het mogelijk dat Kaspersky als middel wordt ingezet door een overheid om een derde partij te compromitteren. Deze overheid kan dit scenario altijd ontkennen.

Er zijn op dit moment overwegend media berichten die dit scenario onderschrijven. Volgens berichtgeving gepubliceerd in oktober 2017 heeft een Israëlische inlichtingendienst de software ontwikkelaar geïnfiltreerd zonder medeweten van het bedrijf en heeft tijdens deze periode data van het bedrijf en operationele elementen ervan kunnen inzien. Kaspersky heeft onderkend dat er in de genoemde periode een intrusie heeft plaats gevonden en dat deze snel is gedetecteerd en gestopt. Volgens mediaberichten heeft de VS zonder medeweten van Kaspersky gebruik gemaakt van producten van het bedrijf voor inlichtingenoperaties. De Central Intelligence Agency zou informatie hebben toegevoegd aan Kaspersky-software om verschillende personen te kunnen volgen. Daarnaast stelt de media dat een voormalig FSB cybersecurity specialist die bij Kaspersky is gaan werken door de Russische overheid opgepakt op verdenking van spionage voor de Amerikaanse overheid.

5. Ongefundeerde beschuldigingen

Tot slot is het mogelijk dat de beschuldigingen en verdenkingen aan het adres van Kaspersky onterecht zijn. Dit zou betekenen dat Kaspersky niet onbehoorlijk met de Russische overheid samenwerkt en hun systemen ook niet gecompromitteerd zijn. Mogelijk heeft de Russische overheid het bedrijf niet nodig heeft of wil het bedrijf niet schaden met (gedwongen) samenwerking. Vanuit het oogpunt van Kaspersky zou men de integriteit van het bedrijf niet willen aantasten ten overstaan van hun (internationale) klanten.

Het is voorstelbaar dat de beschuldigingen aan het adres van Kaspersky waar zijn, maar er is weinig concreet bewijs. Yevgeni Kaspersky heeft herhaaldelijk in de pers aangegeven dat de software van het AV-bedrijf door buitenstaanders onderzocht mag worden om te bewijzen dat het bedrijf niet verkeerd handelt. Ook zou het bedrijf bereid zijn om het hoofdkantoor in een ander land te plaatsen om zijn onafhankelijkheid te bewijzen. Daarnaast kunnen de banden met de FSB door achtergrond van Kaspersky-werknemers (inclusief Yevgeni Kaspersky zelf) niet als redelijk vermoeden dienen, omdat binnen de private cybersecurity industrie een inlichtingenachtergrond regelmatig voorkomt. Verder heeft Kaspersky internationaal een goede naam, onder andere door het onderzoek dat ze doen, waarbij ook Russische actoren veelvuldig beschreven zijn. Volgens een woordvoerder van het Kremlin zijn er geen banden met Kaspersky. Kaspersky heeft echter ook erkend heeft dat het in enkele gevallen niet-geïnfecteerde bestanden heeft gedownload van de machines van klanten. Daarnaast maakt de wetgeving met betrekking tot bedrijven die met cryptografie werken het ongeloofwaardig dat het bedrijf de Russische overheid zal weigeren bij een onredelijk verzoek.

4.3 Waarschijnlijkheid van de scenario's

De scenario's bewust-ongewild en onbewust-ongewild zijn de twee scenario's die als waarschijnlijk zijn aangemerkt. **Bewust-ongewild** is aangemerkt als **waarschijnlijk** omdat de wetgeving in Rusland het voor de overheid mogelijk maakt gebruik te maken van het AV-bedrijf, maar Kaspersky vanwege reputatieschade zo min mogelijk wil mee werken. De waarschijnlijkheid in dit scenario zit vooral in de potentie van misbruik voor de Russische overheid. Het is niet bekend op welke wijze en hoe vaak de Russische overheid zich beroept op de wetgeving, maar er moet worden aangenomen dat het gebeurt. Het andere scenario dat als **waarschijnlijk** is aangemerkt is **onbewust-ongewild- door een andere overheid** omdat er al onderbouwde berichten zijn die laten zien dat het infiltreren en compromitteren van Kaspersky heeft plaatsgevonden. Zowel het internationale wantrouwen tegen Kaspersky, als de hoeveelheid informatie die Kaspersky bezit, maken het bedrijf tot een interessant doelwit.

Bewust-gewild is een **onwaarschijnlijk** scenario. Vrijwillig medewerken van Kaspersky met de Russische overheid zou internationaal tot grote reputatieschade kunnen lijden, wat nadelig is voor het AV-bedrijf. Het is ook **onwaarschijnlijk** dat alle geuite **beschuldigingen onterecht** zijn. Hoewel het bedrijf zich probeert te presenteren als een ethisch bedrijf, kan een volledig onafhankelijk functioneren van de Russische overheid — mede door de FSB-TSLSZ wetgeving — niet als realistisch worden ingeschat. Tot slot is het **onwaarschijnlijk** dat er sprake is van het scenario **onbewust-ongewild- door de Russische overheid** omdat deze voldoende middelen heeft om in te zetten om medewerking van Kaspersky af te dwingen, waardoor zij niet zonder medeweten van Kaspersky het bedrijf hoeft binnen te dringen.

Hoewel het uitwerken van deze scenario's zich heeft beperkt tot Kaspersky, zijn deze scenario's ook van toepassing op andere AV-bedrijven in hun nationale context. Wat het AV-bedrijf Kaspersky Labs onderscheidt van ieder ander AV- of cybersecuritybedrijf, is de wetgeving die in Rusland geldt voor bedrijven die met cryptografische producten werken.

5 Conclusie

Conclusie 1: Vanwege de aard van een AV-bedrijf en de producten en diensten kan misbruik een aantrekkelijk cybermiddel zijn voor een statelijke (of andere) actor. Of dit middel ook daadwerkelijk ingezet wordt, is afhankelijk van de intenties van de betreffende actor en de mogelijkheden voor misbruik.

Conclusie 2: Wanneer misbruik plaatsvindt van diensten en producten van AV-bedrijven, zoals Kaspersky, vormt dit een dreiging voor de Nationale Veiligheid door:

1. Aantasting van de cybersecurity van informatie en machines met als motief sabotage. Deze dreiging heeft de meeste impact.
2. Aantasting van de vertrouwelijkheid van informatie en machines met als motief spionage.
3. Ontwikkeling van geavanceerde aanvalstechnieken. Het motief is om op lange termijn aanvals- en verdedigingscapaciteit op te bouwen. Daadwerkelijk effect vindt pas plaats bij actieve inzet van de technieken.

Conclusie 3: Wat betreft de manifestatie van de geïdentificeerde dreigingen zijn verschillende scenario's voorstelbaar. Op dit moment is geen sluitend bewijs te vinden in open bronnen voor één of meerdere van de scenario's en kan er daarom geen uitsluitsel gegeven worden of Kaspersky op dit moment actief een dreiging vormt voor de Nationale Veiligheid. De dreiging van statelijke actoren in het digitale domein en de wetgeving met betrekking tot cryptografie en de samenwerking met de FSB moet beschouwd worden als een risico.

Conclusie 3A: Het is waarschijnlijk dat Kaspersky door de Russische overheid gedwongen wordt om samen te werken, maar dat eigenlijk niet wil (scenario bewust-ongewild).

Conclusie 3B: Het is waarschijnlijk dat Kaspersky geïnfiltreerd en gecompromitteerd is of wordt door een andere (dan de Russische) overheid (onbewust-ongewild).

Tot slot moet worden opgemerkt dat ook van andere AV-bedrijven dezelfde dreiging kan uitgaan als die van Kaspersky en soortgelijke scenario's denkbaar zijn. Andere AV-bedrijven hebben dezelfde

middelen en kunnen ook door hun respectievelijke overheden in meer of mindere mate gedwongen worden tot samenwerking.