Het kabinetsbesluit over Kaspersky Lab

Reconstructie en analyse

```
// Scan features data by the current tree and return 0/1 (clean/detect).
int32_t tree_scan ()
{
    const Tree* tree = tp_fptr<Tree>();
    set_fptr(&tree->nodes[tree->num_nodes]); // skip the tree

    for (uint32_t node_ind = 1; ; )
    {
        // get current node and the corresponding compiled feature
        const Tree_Node& node = tree->nodes[node_ind - 1];

        const uint32_t prep_data_ind  = kl_get_unaligned_16_le(&node.feat_data_ind);
        const uint32_t node_param     = kl_get_unaligned_32_le(&node.param);
        const uint32_t node_left_ind  = kl_get_unaligned_16_le(&node.left_ind);
        const uint32_t node_right_ind = kl_get_unaligned_16_le(&node.right_ind);

        const Prep_Feat_Data_Ex& feat_data = m_prep_data[prep_data_ind];

        bool go_left = false;
```

Versie: 1, 14 november 2018, zaaknummer: 2018-0086

Auteur: Brenno de Winter, De Winter Information Solutions

brenno@dewinter.com, +31653536508

Advies: Hans de Raad, Barbara Bulten

Correctie: Rediscript & Marleen van Koetsveld

Status: Definitief

Inhoudsopgave

1. Over de rapportage 3
Aanleiding voor het rapport 3
Analyse 3
Aanvullende documentatie 4
Over Kaspersky Lab 4
2. Procedure naar risicoafweging toe 5
Compleetheid van het dossier 5
Gevolgde procedure 5
3. Observatie 1: Gevaar van software op de systeemlaag 7
Gebruikerslaag 7
Systeemlaag 8
Hardwarelaag 10
Niet één leverancier 11
Maatregelen tegen spionage en sabotage bij een product 11
4. Observatie 2: Verplichte juridische medewerking 14
Geen unieke wetgeving 15
5. Observatie 3: Cyberoperaties tegen Nederland en zijn belangen 17
6. Risiconiveau Kaspersky Lab 19
Malware is malware-beleid 20
Kwaliteitsindicatoren 20
Bug bounty 21
Penetratietest 21
Audit van de broncode 21
7. Kaspersky Security Network 23
8. Gevolgen van het kabinetsbesluit 26
10. Conclusies en aanbevelingen 28

1. Over de rapportage

Aanleiding voor het rapport

Op 14 mei 2018 draagt het Nederlandse kabinet de Rijksoverheid op de antivirussoftware van Kaspersky Lab niet langer te gebruiken en uit te faseren. Organisaties die vallen onder Algemene Beveiligingseisen Defensie Opdrachten (ABDO) of vallen onder vitale diensten en processen krijgen het advies hetzelfde te doen. Het advies geldt niet voor andere organisaties. Ook maakt het kabinet duidelijk dat het alleen gaat om de antivirussoftware, niet om de andere producten en diensten van Kaspersky Lab. Er zijn voor het kabinet drie redenen om deze keuze te maken:

1. Antivirussoftware heeft uitgebreide en diepgaande toegang tot een computer. Zulke toegang kan misbruikt worden voor spionage en sabotage.
2. Als Russisch bedrijf is Kaspersky Lab volgens Russische wetgeving verplicht om bij de overheid mee te werken als de Russische inlichtingendiensten hierom verzoeken.
3. De Russische Federatie heeft een offensief cyberprogramma. Dat laatste betekent dat het land met behulp van computers actief spionage en sabotage pleegt.

Het kabinet spreekt in een brief aan de Tweede Kamer[1] van een voorzorgsmaatregel met als reden te vrezen voor spionage en sabotage. Daarbij schrijft het kabinet een eigen, aangescherpte afweging in het kader van de nationale veiligheid te hebben gemaakt. In essentie komt de vrees van het kabinet erop neer dat de antivirussoftware van Kaspersky Lab, een bedrijf dat malware bestrijdt, zelf wordt ingezet als Trojaans paard ofwel malware.

Nederland beschikt niet over voorbeelden waaruit blijkt dat er misbruik is gemaakt van de antivirussoftware van Kaspersky Lab. Ook bij andere (Europese) landen en de Europese Commissie zijn er geen voorbeelden bekend. Als KRO-NCRV bij een journalistiek onderzoek met succes een beroep doet op de Wet openbaarheid van bestuur (Wob) komen nadere documenten beschikbaar.

Analyse

Brenno de Winter van De Winter Information Solutions is door Kaspersky Lab gevraagd een reconstructie te maken van de voorzorgsmaatregel van het kabinet en de drie observaties van het kabinet te analyseren. In een tijd van digitale operaties is het logisch en goed dat het kabinet alert is op de gevaren van spionage en sabotage. Dit rapport onderzoekt inhoudelijk en procedureel hoe de argumentatie vanuit het kabinet tot stand is gekomen, in hoeverre Kaspersky Lab op basis van deze argumentatie inderdaad een dreiging vormt en welke stappen noodzakelijk zouden zijn een dergelijke dreiging het hoofd te bieden.

Daarbij is gebruikgemaakt van beschikbare documentatie, relevante openbare bronnen en verificatie van bevindingen bij experts. Verder is een inspectie uitgevoerd bij het Transparancy Center van Kaspersky Lab in Zürich, Zwitserland waar de broncode van de antivirussoftware beschikbaar is. In het kader van het onderzoek heeft Kaspersky Lab zich gecommitteerd alle medewerking te verlenen, zich niet met de inhoud te bemoeien, geen

[1] Bijlage 1, Kamerbrief van de minister van Justitie en Veiligheid van 14 mei 2018 met kenmerk: 2268367.

druk uit te oefenen op de inhoud en observaties, en op voorhand akkoord te zijn dat het rapport openbaar wordt ongeacht de bevindingen.

Aanvullende documentatie

Met het rapport komen ook bijlagen beschikbaar met onderbouwing. In de voetnoten wordt naar deze onderbouwing verwezen. Waar mogelijk worden de onderliggende documenten bij het rapport gevoegd of wordt verwezen naar een vindplaats op internet om zo een zo accuraat mogelijke onderbouwing te bieden.

Over Kaspersky Lab

De onderneming Kaspersky Lab is in 1997 opgericht door onder andere Eugene Kaspersky. Hij begon het bedrijf nadat hij acht jaar eerder werd getroffen door het Cascade-virus en geïnteresseerd raakte in het bestrijden van malware. Het bedrijf is actief in tweehonderd landen, met 35 kantoren in 31 landen[2] en levert antivirussoftware, kennis en diensten op het gebied van informatiebeveiliging. Het bedrijf had in 2017 een omzet van 707,6 miljoen dollar[3] (ongeveer 624 miljoen euro[4]).

De vestiging in de Benelux is onder de naam Kaspersky Lab B.V. gevestigd in Utrecht. Dit is een volwaardige dochter[5] van het moederbedrijf Kaspersky Lab Limited[6] in het Verenigd Koninkrijk. Juridisch gezien is het bedrijf een Britse firma. Het hoofdkantoor zit in Moskou, Rusland. De assemblage van de software, de opslag van Europese klantgegevens vindt plaats in Zürich, Zwitserland.

In hoofdstuk 6 wordt nader ingegaan op de reputatie van Kaspersky Lab in het stuk ‘relaties met de Nederlandse overheid’

[2] https://www.kaspersky.nl/about/company - geverifieerd op 13 november 2018
[3] Bijlage 19 pagina 514 e.v.
[4] Berekend op 11 november 2018 met xe.com
[5] Afschrift Kamer van Koophandel van 11 november 2018 – Bijlage 18, pagina 508, 509
[6] https://beta.companieshouse.gov.uk/company/04249748 - geverifieerd op 11 november 2018

2. Procedure naar risicoafweging toe

Compleetheid van het dossier

In de brief aan de Tweede Kamer staan de overwegingen die bij het kabinet hebben geleid tot de voorzorgsmaatregel. Er is geen vertrouwelijke briefing over dit onderwerp geweest. Bij de weging van de maatregel is het uitgangspunt dat het kabinet het parlement correct heeft geïnformeerd en geen informatie heeft achtergehouden. Bij een Wob-verzoek verplicht de wet dat er gezocht wordt naar documenten[7] (dus memo's, rapporten, mails, brieven, verslagen, samenvattingen, notities enzovoort). Over alle documenten – ook de stukken die geweigerd worden – moet de overheid een besluit nemen. De documentenlijsten[8] maken duidelijk welke stappen er naar het besluit over het uitfaseren van de software van Kaspersky Lab toe zijn doorlopen. Uit het Wob-verzoek blijkt niet dat er reden is om aan te nemen dat andere overwegingen, buiten de ter beschikking gestelde documenten, een rol hebben gespeeld bij het besluit van het kabinet. De redenering van het kabinet valt op basis van de beschikbare informatie te reconstrueren en chronologisch te analyseren.

Gevolgde procedure

Uit de brief aan de Tweede Kamer en de bij het Wob-verzoek openbaar gemaakte documenten blijkt niet welke procedure het kabinet heeft gevolgd om een risico-inschatting te maken en welke besliscriteria vooraf zijn gedefinieerd om tot een gewogen besluit te komen. Uit de documenten van het Wob-verzoek is wel een aantal stappen en beslismomenten te herleiden:

1. 13 september 2017. Het Department of Homeland Security in de Verenigde Staten brengt 'Binding Operational Directive 2017-01'[9] uit. Hierin verplicht de Amerikaanse overheid de federale overheidsinstellingen binnen negentig dagen te beginnen met het stoppen van het gebruik van de producten van Kaspersky Lab.
2. 15 januari 2018. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) heeft een interne risicoanalyse geschreven.
3. 15 januari 2018. De CIO Rijk stuurt een verzoek uit om inzicht te krijgen in het gebruik van Kaspersky-software bij in ieder geval overheidspartijen. Dit bericht stuurt hij naar de Chief Information Officers (CIO's), Chief Technology Officers (CTO's) en Chief Information Security Officers (CISO's). Het verzoek aan de CISO's is om uiterlijk 19 januari 2018 te antwoorden.
4. 25 januari 2018. Kaspersky Lab heeft via partners begrepen dat er een uitvraag bezig is. In een brief[10] biedt de onderneming alle hulp aan bij het onderzoek en wijst op een beschikbare en in Nederland uitgevoerde penetratietest. Van die mogelijkheid wordt geen gebruikgemaakt.

[7] Een document is in de Wet openbaarheid van bestuur zeer ruim gedefinieerd als 'een bij een bestuursorgaan berustend schriftelijk stuk of ander materiaal dat gegevens bevat'
[8] Bijlagen 2, 3 en 4 bij dit rapport.
[9] Bijlage 10
[10] Bijlage 5

5. In de periode 2 februari 2018 tot 6 mei 2018 worden er een zevental documenten geschreven door de NCTV aan het Comité Verenigde Inlichtingendiensten Nederland (CVIN) en de Raad Veiligheid en Inlichtingen (RVI).
6. 14 mei 2018. Er volgen diverse aankondigingen van het aankomende besluit door het Nationaal Cyber Security Centrum (NCSC).
7. 14 mei 2018. De Tweede Kamer wordt in een brief geïnformeerd.

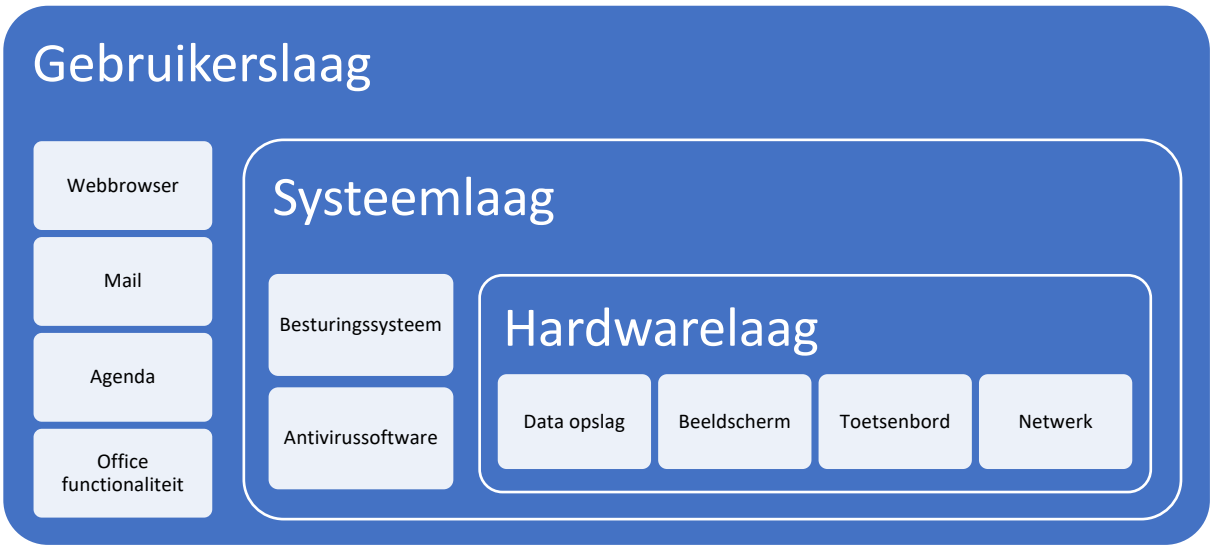
In het dossier (Kamerbrief met geopenbaarde documenten en de lijst van beschikbare documenten bij het Wob-verzoek) ontbreken een aantal zaken die bij een besluit van dit kaliber zouden mogen worden verwacht:

1. Er is niet duidelijk welke methodiek is gebruikt om de belangenafweging tussen potentiële risico's en maatregelen te maken. Ook ontbreken de beoordelingscriteria die vooraf gedefinieerd zijn tot het maken van een risico-inschatting. Dat is belangrijk om de weging bij een risico-inschatting te kunnen verklaren en om te kunnen controleren of deze afweging (in peerreview) wordt gedeeld. Ook blijft onduidelijk of er eventueel producten van andere leveranciers in vergelijkbare toepassingsgebieden risico's met zich meebrengen. De observaties van het kabinet horen aanleiding te zijn meer software en hardware te identificeren met eenzelfde of groter risicoprofiel.
2. Het ontbreekt aan een technisch onderbouwde analyse die aan de risico-inschatting ten grondslag ligt. Geen enkel document richt zich op techniek. De uitleg blijft daardoor beperkt tot de vaststelling dat antivirussoftware 'uitgebreide en diepgaande toegang tot een computer of netwerk heeft'. In Nederland zijn penetratietesten op de antivirussoftware van Kaspersky Lab uitgevoerd, waarvan de uitkomst aan de overheid ter beschikking is gesteld[11]. Deze kennis is aangeboden, maar uit het dossier blijkt niet dat deze informatie is meegewogen.
3. De juridische redenering, waarom Kaspersky Lab een verhoogd risico zou vormen, is enkel gestoeld op de Amerikaanse documenten. Nergens blijkt uit dat ook in Nederland een controleonderzoek is gedaan naar de juistheid van deze documenten, is gekeken naar de relevantie in de Nederlandse context of dat contact is geweest met de opstellers ervan. Uit eigen onderzoek blijkt dat er op zijn minst sprake is van een discussie hoe de Russische wetgeving geïnterpreteerd moet worden.
4. Er heeft geen wederhoor, of (voor zover uit de documenten blijkt) een onafhankelijke peerreview, plaatsgevonden. Kaspersky Lab is niet in staat gesteld te reageren op de observaties van het kabinet en de observaties zijn ook niet ter validatie voorgelegd aan een derde partij.
5. Het (dringende) advies specificeert niet de omstandigheden of toepassingsgebieden wanneer de software van Kaspersky Lab wel of geen risico vormt. De Europese Commissie onderzocht[12] de bestaande toepassingsgebieden wel naar aanleiding van vragen uit het Europees Parlement. Dat blijkt de antivirussoftware te gebruiken op systemen die niet direct met internet verbonden zijn. 'The risk of data exfiltration therefore would be minimal even if the software was in fact malicious. However, the Commission has no indication for any danger associated with this anti-virus engine', schrijft Eurocommissaris Mariya Gabriel.

[11] In de brief van Kaspersky (Bijlage 5) wordt verwezen naar onderzoeken (penetratietesten of 'hackerstesten') die zijn gedaan door meerdere marktpartijen. Een daarvan wordt aangemerkt als kritieke sector. [911911]
[12] http://www.europarl.europa.eu/doceo/document/P-8-2018-000603-ASW_EN.html - geverifieerd op 10 november 2018

3. Observatie 1: Gevaar van software op de systeemlaag

De eerste observatie van het kabinet stelt dat antivirussoftware uitgebreide en diepgaande toegang tot een computer of netwerk heeft. Het kabinet onderscheidt daarbij twee niveaus: het 'systeemgedeelte' en het 'gebruikersgedeelte'. Om een compleet beeld van een computer, netwerkonderdeel, mobiele telefoon of ander apparaat te schetsen, vallen er simpel gezegd drie lagen te onderscheiden: het gebruikersgedeelte, het systeemgedeelte en de daaronder actieve hardware. Op iedere laag functioneert een onderdeel van een systeem (computer, telefoon, netwerkapparaat enzovoort).



Naarmate we dieper afdalen in het systeem wordt de dreiging bij misbruik groter en wordt het lastiger een kwaadaardige code te ontdekken. De keerzijde is dat het plegen van een aanval dan ook lastiger wordt. Om de dreiging juist te kunnen plaatsen, lopen we de gevaren laag voor laag langs.

Gebruikerslaag

De gebruikerslaag is de laag waar de programmatuur functioneert waar een gebruiker mee communiceert. Dit is bijvoorbeeld een webbrowser, tekstverwerker, e-mailpakket en andere functionaliteit. Enkele voorbeelden zijn Apple Mail, Google Chrome, Microsoft Office, Microsoft Outlook, Mozilla Firefox of op een smartphone bijvoorbeeld apps als Facebook, LinkedIn, Twitter, een weerapp, NS Reisplanner Xtra, een nieuwsapp, Apple/Google Maps, Waze enzovoort.

Veel aanvallen vinden in eerste instantie op dit niveau plaats. Als een gebruiker iets downloadt, een kwaadaardige site bezoekt of reageert op een e-mail, is het voor aanvallers al snel mogelijk malware af te leveren of is een zwakheid in gebruikte software te misbruiken. Via andere zwakheden in een systeem kan een aanval op dit eerste niveau via een *privilege escalation* als het ware 'upgraden' naar een aanval op systeemniveau. De software is dan als het ware beheerder op het systeem.

Om dit tegen te gaan, beperkt het besturingssysteem wat software mag doen. Dit merkt de gebruiker als het systeem expliciet om toestemming vraagt om als beheerder iets uit te voeren. Bij veel besturingssystemen en op veel telefoons moet de gebruiker toestemming

geven voor rechten, zoals bijvoorbeeld toegang tot het adressenboek, opslaan van bestanden of het versturen van sms-berichten. Aanvallers omzeilen dat door de gebruiker te verleiden om hen alsnog systeemtoegang te geven of door zwakheden op systeemniveau te misbruiken. Veel antivirussoftware is erop gericht om dit soort schadelijk, afwijkend gedrag tussen gebruikers-, en systeemniveau te herkennen en te stoppen. Om dat effectief te kunnen, moet het dieper dan de gebruikerssoftware opereren.

Systeemlaag

Onder de gebruikerslaag zit de systeem-laag. Het kabinet stelt dat deze laag 'uitgebreide en diepgaande toegang tot ICT-systemen geeft'. Hier wordt alle verwerking gedaan die nodig is om de hardware van één systeem aan te sturen en de software te faciliteren waarmee de gebruiker interactie heeft. Dit is de plaats waar signalen van een aanraakscherm, muis of toetsenbord binnenkomen, een beeldscherm wordt aangestuurd, de temperatuur van hardware in de gaten wordt gehouden, het netwerkverkeer wordt geregeld, de resterende lading van de batterij wordt bijgehouden en het opslaan of ophalen van bestanden wordt geregeld.

Om als antivirussoftware echt effectief te zijn, richten de meeste leveranciers zich op deze laag. Wanneer een bestand wordt geopend of er netwerkverkeer langskomt, kan het gelijk scannen op malware en zo nodig ingrijpen op een aanval. Verder neemt het op dit schakelpunt afwijkend en onwenselijk gedrag op het systeem waar en grijpt in als dat nodig is. Zulke ingrepen geven weerbaarheid tegen aanvallen op de gebruikersslaag en andersom weerbaarheid tegen zwakheden in bijvoorbeeld een besturingssysteem. Gevonden afwijkingen kan antivirussoftware daarop bij monitoringsystemen melden. Zo weet de beheersorganisatie dat er een probleem speelt. Voorbeelden van besturingssystemen zijn Android OS, iOS, Linux, Microsoft Windows en MacOS. Voorbeelden van leveranciers van antivirussoftware

WannaCry- & NotPetya-infecties

In april publiceert de hackersgroep 'Shadow Brokers' een aantal aanvallen op basis van zwakheden in het besturingssysteem Microsoft Windows. De zwakheden zouden afkomstig zijn van de Amerikaanse National Security Agency (NSA). Een maand voor de bekendmaking heeft Microsoft de zwakheden gedicht.

Er volgen diverse uitbraken met malware. De meeste zijn ransomware. Opvallend is dat na infectie via bijvoorbeeld e-mail de malware misbruik maakt van de onthulde lekken. De aanval vindt op dat moment plaats gericht tegen de systeemlaag van de software.

Tijdens een van de uitbraken van ransomware wordt bijvoorbeeld de Britse National Health Service getroffen. Deze aanval krijgt de naam 'WannaCry'. Sommige experts wijzen Noord-Korea als verspreider aan.

Enkele weken later volgt een uitbraak van een virus dat al snel wordt geduid als een variant op de ransomware Petya. De infectiehaard blijkt in dit geval verplichte boekhoudsoftware in Oekraïne. Ook deze software misbruikt het lek op systeemniveau bij Windows. De uitbraak raakt ook een containerterminal in de Rotterdamse haven.

De Verenigde Staten, het Verenigd Koninkrijk en Denemarken wijzen Rusland als dader aan. Kaspersky Lab onderzoekt de malware en concludeert dat het een ander virus is en noemt de malware NotPetya. Dit staat onder andere in bijlage 14 op pagina 304.

op deze laag zijn Avast, AVG, Avira, Bitdefender, Dr. Web, ESET, F-Secure, G-Data, Kaspersky Lab, McAfee, Microsoft, Nano Security, Qihoo 360, Symantec, VirusBlokAda, Webroot enzovoort.

Wie op de systeemlaag malware weet te installeren, kan zowel het besturingssysteem als software op de gebruikerslaag beïnvloeden. Bij toegang tot de systeemlaag is er overigens niet automatisch sprake van 'uitgebreide en diepgaande toegang tot ICT-systemen', zoals het kabinet stelt. Hooguit toegang tot één specifiek systeem. Er is bij een succesvolle aanval toegang tot die mobiele telefoon of dat desbetreffende werkstation, maar niet automatisch tot omliggende systemen in een netwerk. Die zouden namelijk dan ook op hun beurt één voor één gecompromitteerd moeten worden.

De manier van denken die het kabinet aangeeft, gaat uit van een enkele laag in beveiliging. De norm[13] voor overheidsdiensten – voor andere organisaties zijn er vergelijkbare – is echter om in gevoelige omgevingen de risico's op escalatie tussen systemen te beperken door netwerken te segmenteren. Daarbij behoren netwerken te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen[14]. Een stap is het opdelen[15] van netwerken in losse stukken (bijvoorbeeld via VLAN's). Zo blijft een grote aanval, zoals een virusuitbraak (of ransomware), manuele hackerinbraak of andere opzettelijk kwaadwillende actie, beperkt tot het kleinere segment. Daarom moet er continu monitoring op het netwerk aanwezig zijn[16]. Al het verkeer dat binnenkomt of eruit gaat en wat er zich aan data binnen het netwerksegment zelf beweegt, wordt zo gecontroleerd. Dat monitoren gebeurt met Security Information and Event Management-systemen (kortweg: SIEM) waar alle gebeurtenissen in een netwerkomgeving worden gecontroleerd en bewaakt[17]. Daarnaast betekent bredere toegang tot een enkel systeem niet automatisch bredere toegang tot bijvoorbeeld documenten.

Documenten worden in de regel altijd bewaard in een Document Management Systemen (DMS) en een gebruiker krijgt enkel toegang tot een tijdelijke kopie van een document. Die toegang is – bij normale en deugdelijk ingerichte systemen – beperkt tot de rechten van een specifieke gebruiker, waardoor een systeem ook niet bij meer documenten mag dan waar die gebruiker op dat moment zelf bij kan.

[13] De norm voor de Rijksoverheid is de 'Baseline Informatiebeveiliging Rijksdienst' – Bijlage 11
[14] BIR 2017, 13.1.1 – 1 (pagina 230 van de bijlagen)
[15] BIR 2017, 13.1.3 – 1 (pagina 230 van de bijlagen)
[16] BIR 2017, 13.1.2 – 1 (pagina 230 van de bijlagen)
[17] BIR 2017, 12.4.1 (pagina 228 van de bijlagen)

Hardwarelaag

Nog dieper in een systeem functioneert de hardware. Dit is het diepste niveau van een ICT-systeem. Hier ligt letterlijk de regie over alles wat er op technisch vlak aan commando's wordt uitgevoerd. Deze regie gaat zover dat zelfs een opdracht vanuit de systeemlaag genegeerd kan worden, verkeerde resultaten worden teruggestuurd of het mogelijk is iedere handeling heimelijk naar een derde partij te sturen. In de hardware zit ook programmatuur, die we firmware noemen. Voorbeelden van leveranciers van hardware voor computers, mobiele telefoons, beveiligingsapparaten en netwerkapparaten zijn: Acer, Apple, Aruba, Asus, Cisco, Dell, HP, Huawei, Lenovo, LG, Medion, Motorola, Netgear, Nokia, Samsung, Sony, Synology of WatchGuard.

Verborgen firmwarefunctionaliteit in de auto

Een bekend voorbeeld van verborgen software in hardware is het emissie-schandaal omtrent verschillende (voornamelijk Duitse) dieselauto-fabrikanten. In de boordcomputer bleek op firmwareniveau functionaliteit te zitten om een officiële emissietest te detecteren en dan de motor anders te laten functioneren. De uitstoot op de weg was tien- tot veertigmaal hoger dan uit de tests bleek.

Detectie op dit niveau is lastig. De sjoemel-software activeert slechts onder bepaalde operationele omstandigheden. De zaak werd pas aan het rollen gebracht toen er een vermoeden was dat er iets niet klopte en doelgericht, intensief op de openbare weg werd getest. Als de uitkomsten van dat gerichte onderzoek naar buiten komen, ontstaat er ophef.

Waar bij software in de meeste gevallen met inspanning te achterhalen is wat de programmatuur exact doet, is dat bij firmware in hardware moeilijk of soms zelfs onmogelijk. De logica kan verborgen zitten in de fysieke circuits van chips. Al zijn de ontwerpen van de hardware beschikbaar dan is het, zonder diepgaand en continu toezicht op het fabricageproces, lastig te toetsen of precies die hardware ook gebouwd is. Wie kwaadaardige code in de hardware kan verstoppen, is in staat zeer effectief te spioneren of sabotage te plegen.

Een aanvaller die firmware kan aanpassen of toevoegen is daarmee heer en meester. Voor spionagedoeleinden is een aanval op dit niveau extra effectief en subtiel juist omdat het zo lastig te detecteren en te mitigeren is. De hardware gedraagt zich immers geheel normaal. Het uitvoeren van een dergelijke aanval is echter ook lastiger. De aanvaller moet een kwetsbaarheid introduceren in het ontwerp van de fysieke hardware of in een firmwareupdate. Zo'n update kan bij de distributie van die firmware mogelijk toch opvallen. In zo'n geval moet de gebruiker (bijvoorbeeld een ICT-beheerder, of een laptopeigenaar) worden verleid om zelf nieuwe firmware te laten installeren. Antivirussoftware kan in sommige gevallen zo'n aanval detecteren. Ook veel makers van besturingssystemen hebben maatregelen genomen om zo'n installatie lastig te maken of om de impact van een dergelijke hardware-hack op systeemniveau te beperken. Pijnlijke recente voorbeelden hiervan in centrale processing units (CPU's, de kern van ieder computersysteem), zijn de kwetsbaarheden die toen ze ontdekt werden de naam Spectre en Meltdown[18] kregen. De namen reflecteren hoe groot de impact is en hoe moeilijk de risico's te bestrijden zijn.

De 'God'-modus bij Intel-processoren

In december 2017 toonden twee beveiligingsonderzoekers hoe zij misbruik konden maken van een fout in de Intel Management Engine. Door de brede toegang tot ieder aspect van de computer (bestanden, netwerk en hardware) noemden zij dit de 'God'-modus. De hardware blijkt voor wie het lek kan vinden een verborgen achterdeur te zijn.

Het pijnlijke is dat de beveiligings-onderzoekers ook concluderen dat het probleem teruggaat tot chips die sinds 2007 op de markt zijn gekomen.

Niet één leverancier

Door alleen te kijken naar een leverancier van antivirussoftware gaat het kabinet voorbij aan vele andere risico's voor spionage en sabotage. Er zou veel breder gekeken moeten worden naar de toegang tot systemen en naar de systemen zelf. Een achterdeur hoeft niet eens opzettelijk gebouwd te worden. Deze kan ontstaan door fouten in de software of hardware. Wie vreest voor operaties van een vijandige inlichtingendienst kan dit risico niet negeren. Daarbij horen we niet alleen antivirussoftware, maar ook besturingssystemen en hardware als risico te wegen. Door in deze zaak niet breder te kijken naar aanpalende beveiligingsdomeinen, ontstaat een te beknopt, incorrect en vooral onvolledig beeld. Dat roept een beeld van selectieve beargumentering op waarbij enkel naar de casus Kaspersky Lab is gekeken.

Maatregelen tegen spionage en sabotage bij een product

Achterdeuren in software voor spionage of sabotage komen op twee manieren voor. De eerste is een platform dat onbedoeld voor misbruik door fouten in de software kan worden ingezet. Een zwakheid geeft bijvoorbeeld toegang tot bestanden of logingegevens. Vooral nog niet bekende lekken, zogenaamde *zero days*, zijn dan instrumenteel. Er is vaak geen verdediging tegen de aanval, omdat deze nog niet bekend, geanalyseerd (en gedeeld) is binnen de securitygemeenschap waar Kaspersky Lab onderdeel van is. De tweede manier is het opzettelijk aanbrengen van kwetsbaarheden in software, of een bredere infrastructuur

[18] https://meltdownattack.com/ - geverifieerd op 8 november 2018

om aanvallen (spionage en sabotage) uit te voeren. Deze laatste vorm is lastig te detecteren, omdat dan de softwareleverancier in het complot zit. Voor het ontdekken is meer inzicht nodig in de software. De benaming voor deze aanvalsmethodiek heet een Advanced Persistent Threat (APT).

Er zijn een aantal maatregelen mogelijk om spionage en sabotage via een achterdeur in ingekochte software te beperken:

1. Onderzoek naar de leverancier van een softwareproduct of -dienst. Is eerder meegewerkt aan spionage? Of is de leverancier juist betrokken bij het detecteren en bestrijden van aanvallen? Omdat er veel externe partijen een rol spelen in de systemen van organisaties, speelt het vertrouwen in een speler een grote rol. Of een antivirusleverancier te vertrouwen is, kun je bijvoorbeeld toetsen aan de hand van de volgende vragen:
    a. Zijn er veel zwakheden in het product te vinden? Wanneer er zwakheden in software worden gevonden, dan worden deze publiekelijk bekendgemaakt op een standaardmanier via een Common Vulnerability Exposure (CVE). Hierdoor is te volgen wat de problemen met de software zijn, welke aanvallen door de kwetsbaarheid mogelijk zijn en daarmee ook hoe ernstig dit is. Nagenoeg alle veelgebruikte softwareproducten zijn in deze lijst wel aanwezig. Maar het aantal meldingen per product in combinatie met de ernst van de gemelde incidenten maken per product duidelijk in hoeverre er verhoogd risico op misbruik van de software mogelijk is.
    b. Zijn er bekende en bewuste beperkingen in de beschermende werking van de software? Is er malware die bewust niet wordt gedetecteerd of wordt gestopt?
    c. Is eerder duidelijk geworden dat het bedrijf – anders dan het plaatsen van een wettelijk verplichte afluistertap – ingezet wordt voor het uitvoeren van spionagetaken?
2. Uitvoeren van penetratietesten – ook hackertesten genoemd. Bij een dergelijk onderzoek wordt de software op veel verschillende manieren aangevallen en wordt gezocht naar bekende (en vaak onbekende) lekken. Zijn er veel bevindingen, dan kan dat een aanwijzing zijn dat de kwaliteit van de software tekort schiet. Het probleem bij deze vorm van inspectie is dat wordt gewerkt met een black box, waardoor de tester niet alle relevante scenario's of situaties kan doorgronden of testen. Het blijft een momentopname van het systeem, waarbij alleen de input (wat je als tester erin stopt) en de output (de resultaten die je ziet) worden gemeten.
3. Uitvoeren van een codereview. Bij het maken van bruikbare software schrijven ontwikkelaars programmeercode, die leesbare tekst noemen we broncode. Deze wordt omgezet in uitvoerbare systeemcode, die een computer begrijpt (die stap heet compileren). De kwaliteit van de software blijkt uit een inspectie op de broncode. Dan kan er naar zwakheden worden gezocht waaronder (onopzettelijke) achterdeuren. Deze vorm van verificatie geeft op hoog niveau vertrouwen, de leverancier geeft hierbij letterlijk al zijn geheimen prijs. Tegelijkertijd geeft de toegang op dit niveau kwaadwillenden de mogelijkheid om geconstateerde zwakheden voor zichzelf te houden en later te misbruiken. Een leverancier moet zeker van zijn zaak zijn om dit niveau van transparantie te bieden.

Niet iedere leverancier staat open voor het bestuderen van de broncode. Andere laten slechts een beperkt deel van de broncode toetsen. Die laatste stap is niet heel zinvol, omdat in het gedeelte waar geen inspectie heeft plaatsgevonden alsnog een achterdeur kan zitten. Het is dus zaak om zeker te weten dat de getoetste broncode daadwerkelijk die is waarmee het uiteindelijke product wordt gemaakt dat actief is op de computers/telefoons van jouw organisatie.

Het uitvoeren van een inspectie op de broncode van gebruikte software is een belangrijke (of onmisbare) stap voor gevoelige omgevingen. Het is een vorm van due diligence die ervoor zorgt dat er een hogere mate van zekerheid is over de werking van de programmatuur. Voor diverse producten die bijvoorbeeld worden gebruikt voor de bescherming van departementaal vertrouwelijke documenten beschikt de AIVD over de mogelijkheid de kwaliteit te toetsen en een goedkeuring te verlenen[19].

4. Het voortdurend diepgaand controle uitvoeren op operationele processen van de leverancier. Door te kijken naar de processen, systemen en maatregelen aan de zijde van de dienstverlener, wordt duidelijk of wat er in de dagelijkse praktijk met gegevens gebeurt overeenkomt met de “papieren realiteit” van, bijvoorbeeld ISO, certificaten en andere, periodiek gecontroleerde, kwaliteitslabels.

[19] https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/goedgekeurde-producten - geverifieerd op 10 november 2018

4. Observatie 2: Verplichte juridische medewerking

De tweede observatie van het kabinet is dat Kaspersky Lab op basis van Russische wetgeving verplicht is medewerking te verlenen aan een operatie van de Russische inlichtingendiensten. “Kaspersky Lab is een Russisch bedrijf met haar hoofdkantoor in Rusland en valt daarmee onder Russische wetgeving”, schrijft het kabinet in de Kamerbrief. Dat is incorrect. Kaspersky Lab is een Britse onderneming, waarvan inderdaad het hoofdkantoor in Rusland staat[20].

Uit het Wob-verzoek blijkt dat de rapportages[21] waarop deze beslissing gebaseerd is, leunen op documentatie die ten grondslag lag aan de Amerikaanse ‘Binding Operational Directive 2017-01’. De documenten leggen uit waarom er vrees bestaat dat er spionage en sabotage via de software van Kaspersky Lab plaatsvindt. Uit de stukken blijkt niet waarom Kaspersky Lab anders is dan een andere antivirus-, of softwareleverancier uit de Russische Federatie. Evenmin blijkt hieruit waarom Kaspersky Lab anders is geclassificeerd dan een leverancier van andere software op deze systeemlaag (of hardwarelaag), die ook onder Russische wetgeving valt zonder dat een bedrijf zijn primaire vestiging in de Russische Federatie heeft.

Bij het Amerikaanse besluit speelt het rapport van de Amerikaanse professor gespecialiseerd in Russisch recht Peter B. Maggs[22]een sleutelrol. Hij stelt – simpel gezegd – dat een bedrijf dat persoonsgegevens in Rusland opslaat en transporteert een aanbieder van een communicatiedienst is. Daarom is het bedrijf verplicht mee te werken met inlichtingendiensten van de Russische Federatie. Probleem daarbij is de verplichting op basis van privacywetgeving om data van Russische burgers in Rusland te bewaren. Hierdoor is er al vrij snel sprake van het aanbieden van een telecommunicatiedienst. Een bedrijf als Kaspersky Lab zou verplicht zijn mee te werken aan verzoeken van de Russische inlichtingendiensten bij het uitvoeren van operaties en het tappen of verstrekken van gegevens die in de Russische Federatie zijn opgeslagen.

Het rapport van Maggs is niet onomstreden. Kaspersky Lab stelt niet onder de tapverplichting van aanbieders van telecommunicatiediensten te vallen. Ongeacht wie er gelijk heeft, kan vastgesteld worden dat er discussie is over deze juridische verplichtingen. In de uitleg van het Nederlandse besluit is geen heldere toelichting gegeven op de positie die het kabinet hierbij kiest. Dat hoort te leiden tot nader onderzoek of wederhoor. Dit rapport behandelt nadrukkelijk niet de vraag wie er in deze discussie gelijk heeft.

Waar wel nadrukkelijk naar is gekeken, is de historische reputatie, en het gedrag, van Kaspersky Lab en de vraag of de komaf van de onderneming aanwijsbaar leidt tot een verhoogd risico om als middel te worden ingezet voor spionage en sabotage. Zou een Nederlands, Amerikaans, Chinees bedrijf met vergelijkbare dienstverlening in de Russische Federatie aan dezelfde wetgeving moeten voldoen? Is Kaspersky Lab anders dan deze bedrijven? Om hierover helderheid te krijgen, is contact gezocht met professor Maggs[23]. Hij stelt dat ook andere bedrijven met vergelijkbare dienstverlening in de Russische Federatie net als Kaspersky Lab onder dezelfde verplichtingen vallen:

[20] Zie hiervoor het kopje ‘Over Kaspersky Lab’ in het hoofdstuk ‘Over de rapportage’
[21] Bijlagen 7, 8 en 9
[22] Bijlage 7, pagina 95 en verder
[23] Bijlage 13, pagina 204

"Kaspersky Lab is verplicht om te voldoen, omdat het informatie in Rusland opslaat en informatie door Rusland transporteert. Een niet-Russisch bedrijf dat dezelfde activiteiten uitvoert moet ook aan dezelfde wetten voldoen, net als een vrachtwagen van een Nederlands bedrijf in Moskou zich aan de Russische verkeersregels dient te houden."

Belangrijk in het onder de spionagewetgeving vallen is dat Kaspersky Lab gegevens van Russische gebruikers opslaat in de Russische Federatie. Ook deze verplichting geldt voor alle bedrijven die actief op zijn op de Russische markt:

"Inderdaad, zoals ik het begrijp – ik heb de zaak zorgvuldig bestudeerd – is Rusland bezig om bedrijven die zakendoen in Rusland, te verplichten om data over Russische burgers op servers in Rusland op te slaan. Het beleid is min of meer de tegenhanger van de Europese wetgeving rond de bescherming van de privacy, die probeert data over EU-burgers veilig binnen de EU te houden. Rusland wil de data toegankelijk houden in Rusland."

De problematiek van de veronderstelde verplichte medewerking met Russische inlichtingdiensten geldt niet alleen voor Kaspersky Lab. Iedere marktpartij die relaties met Russische burgers aanknoopt en een kantoor in Rusland voert, heeft met deze wetgeving te maken. Daarmee is het aantal risicovolle partijen aanzienlijk. Zo blijken alle grotere leveranciers van besturingssystemen voor zowel computers als mobiele telefoons, maar bijvoorbeeld ook telecommunicatiediensten, een vestiging in Moskou te hebben. Voor de grotere antivirusleveranciers is het niet anders. Er zijn veel meer bedrijven die gedwongen kunnen worden om bij te dragen aan de (contra)spionageoperaties van de Russische inlichtingendiensten.

Er zijn bij deze brede interpretatie van de wetgeving veel verschillende softwareleveranciers die exact dezelfde risico's voor de Nederlandse Rijksoverheid en gevoelige sectoren opleveren als Kaspersky Lab. Onduidelijk is waarom dan in de beoordeling van de casus van Kaspersky Lab niet is gekeken naar leveranciers die een ogenschijnlijk vergelijkbaar risicoprofiel opleveren.

Geen unieke wetgeving

De wetgeving in de Russische Federatie staat niet op zichzelf. China kent sinds eind juni 2017 ook voorzieningen in de wetgeving[24] met de verplichting voor bedrijven en personen om

[24] https://www.chinalawtranslate.com/%e4%b8%ad%e5%8d%8e%e4%ba%ba%e6%b0%91%e5%85%b1%e5%92%8c%e5%9b%bd%e5%9b%bd%e5%ae%b6%e6%83%85%e6%8a%a5%e6%b3%95/?lang=en de medewerking staat onder andere in de artikelen 11, 12 en 15 en de wet kent ook strafbepalingen. - geverifieerd op 10 november 2018

inlichtingen- en veiligheidsdiensten te helpen. Daarbij is de focus duidelijk offensief[25] gericht. De Verenigde Staten hebben de Foreign Intelligence Surveillance Act[26] met allerhande aanpassingen (bijvoorbeeld de Patriot Act) die medewerking verplicht stelt. Ook Nederland kent de verplichting om aan spionage mee te werken, versleuteling ongedaan te maken of een voorziening te plaatsen op basis van bepalingen van de Wet op de inlichtingen- en veiligheidsdiensten 2017[27]. Dat is natuurlijk niet direct een vrijbrief voor Russische partijen, maar schept wel enige behoefte voor nuance in de toepasbaarheid van dit specifieke argument.

Overigens wijst ook de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) in het Cybersecuritybeeld Nederland 2018[28] op de problematiek van verplichte medewerking met inlichtingendiensten en geeft aan dat het meerdere landen betreft:

> *"Door de afhankelijkheid van (buitenlandse) partijen groeit de kwetsbaarheid voor spionage, verstoring en sabotage. Buitenlandse partijen kunnen in specifieke landen wettelijk verplicht worden mee te werken aan het ondersteunen van operaties zoals spionage of voorbereidingen voor sabotage."*

Dat de problematiek breder speelt bevestigt professor Maggs:

> *"Zo'n beetje ieder land behoudt zich het recht voor om de communicatie van andere landen te bespioneren. Natuurlijk kunnen er diplomatieke repercussies zijn, zoals in het geval van het aftappen van Angela Merkels mobiele telefoon."*

De Russische wetgeving wijkt in hoofdlijnen niet noemenswaardig af van diverse andere landen.

[25] https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense - geverifieerd op 10 november 2018
[26] Bijvoorbeeld: https://www.law.cornell.edu/uscode/text/50/chapter-36 - geverifieerd op 10 november 2018
[27] https://wetten.overheid.nl/BWBR0039896/2017-09-01 - Bijvoorbeeld artikel 45, lid 9 en artikel 52 en artikel 57 - geverifieerd op 10 november 2018
[28] Bijlage 14, pagina 310

5. Observatie 3: Cyberoperaties tegen Nederland en zijn belangen

De derde en laatste observatie van het kabinet die heeft geleid tot de voorzorgsmaatregel is dat Rusland operaties uitvoert tegen Nederland en Nederlandse belangen. Er is weinig nodig om vast te stellen dat er inderdaad operaties tegen Nederland en Nederlandse belangen worden uitgevoerd. In het Cybersecuritybeeld Nederland 2018[29] wijst de NCTV dat staten de grootste bedreiging vormen:

> *"Staten voeren digitale aanvallen uit op andere landen, organisaties of individuen uit primair geopolitieke motieven. Zij hebben als doel de verwerving van strategische informatie (spionage), beïnvloeding van de publieke opinie of democratische processen (beïnvloeding) of verstoring van vitale systemen (verstoring) of zelfs de vernietiging daarvan (sabotage). Er zijn het afgelopen jaar verscheidende digitale aanvallen door staten waargenomen. Deze hadden impact op de nationale veiligheid."*

In het jaarverslag 2017 van de AIVD wijst de inlichtingendienst op de bijzondere positie van Nederland als hub, lid van de VN Veiligheidsraad in 2018, de NAVO en de EU[30]. Het gaat bij digitale spionage om een groeiend probleem, waarbij er diverse actoren zijn:

> *"Digitale spionage met een economisch motief blijft een bron van zorg en de AIVD onderkent een lichte toename van economische spionage in Europa in vergelijking met vorig jaar. Diverse staten maken zich hieraan schuldig. Wij hebben in 2017 digitale spionage vastgesteld bij diverse Europese multinationals en onderzoeksinstellingen in de energie-, hightech-, en chemische sector. Hieronder bevinden zich diverse organisaties die intensieve samenwerkingsrelaties hebben met Nederland of vestigingen hebben in Nederland. Bij deze digitale inbraken zijn terabytes aan vertrouwelijke gegevens gestolen die een substantiële economische waarde vertegenwoordigen."*

De AIVD wijst daarbij op vooral de inzet vanuit Rusland en China als statelijke actoren die ons land aanvallen. Overigens zijn de offensieve capaciteiten onderdeel van een bredere wapenwedloop. Na de onthullingen van Edward Snowden is duidelijk geworden dat omvangrijke nationale programma's actief zijn om proactief en offensief aanvallen uit te voeren, achterdeuren in software te introduceren (of juist na ontdekking te verzwijgen) en dat maatwerk-malware wordt verspreid.

[29] Bijlage 14, pagina 320
[30] Bijlage 15, pagina 374, 375

In januari 2018[31] wordt duidelijk dat medewerkers van de Joint Sigint Cyber Unit (JCSU)[32] in 2014 hebben ingebroken op de netwerken van de Russische hackersgroep Cozy Bear, ook bekend als APT29. Zij stellen vast dat deze groep gelieerd is aan een Russische inlichtingendienst. Juist Kaspersky Lab was als eerste actief in het waarschuwen voor deze groep.

De ernst van dreiging van offensieve programma's mag niet onderschat worden. Juist voor leveranciers van allerhande programmatuur, waaronder antivirussoftware en besturingssystemen, groeit de druk om mee te werken aan deze operaties. Daarbij is niet het meest zorgwekkende de inzet bij losse operaties, maar het actief creëren van een permanente infrastructuur om operaties mogelijk te maken[33].

[31] https://www.volkskrant.nl/nieuws-achtergrond/hackers-aivd-leverden-cruciaal-bewijs-over-russische-inmenging-in-amerikaanse-verkiezingen~b32c6077/ - geverifieerd op 9 november 2018
[32] De Joint Sigint Cyber Unit is een samenwerkingsverband tussen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
[33] https://www.theverge.com/2018/9/3/17815196/five-eyes-encryption-backdoors-us-uk-australia-nz-canada - geverifieerd op 12 november 2018

6. Risiconiveau Kaspersky Lab

Het inzichtelijk maken van het risico op spionage en sabotage bij antivirussoftware is in de zaak van Kaspersky Lab goed mogelijk. Er is veel informatie te vinden over het bedrijf en het uitvoeren van audits is goed mogelijk. Hierdoor is een realistisch beeld van de handel en wandel van het bedrijf te schetsen.

Relaties met de Nederlandse overheid

Kaspersky Lab is voor de Nederlandse overheid geen onbekende partij. De onderneming ondersteunt op het moment van het besluit van het kabinet de Nationale Politie bij diverse onderzoeken. Dat hebben ze in het verleden vaker gedaan, zoals bij de Carbanak[34]-aanvallen waarbij is ingebroken bij diverse financiële instellingen. De aanvallen waren de grootste digitale bankroof in de geschiedenis en aanleiding voor Europol om met spoed Europese banken bij elkaar te roepen en Kaspersky Lab uitleg te laten geven.

Bij ransomware-aanvallen is intensief samengewerkt met de politie om sleutels voor het ontcijferen van versleutelde bestanden te achterhalen, zodat slachtoffers weer bij hun bestanden kunnen komen zonder losgeld te betalen. Een bekend voorbeeld is de Coinvault-malware. Kaspersky Lab heeft naar aanleiding hiervan samen met de politie, Europol en antivirusleverancier McAfee het No More Ransom-initiatief gestart. Hierdoor kunnen zeker 30.000 mensen hun computers na een infectie met ransomware toch ontcijferen. In 2016 is oprichter Eugene Kaspersky prominent aanwezig als keynotespreker op de NCSC One Conference. Op dezelfde conferentie geeft Kaspersky Lab in 2016 en 2017 gezamenlijke presentaties met Team High Tech Crime van de Landelijke Eenheid van de Nationale Politie.

Verder werkt de organisatie onder andere mee aan diverse bewustwordingscampagnes, zoals bijvoorbeeld Alert Online[35] en ‘Maak het ze niet te makkelijk’. Kortom, het bedrijf werkt op verschillende gebieden intensief samen met de Nederlandse overheid als het gaat om beveiliging.

Het ontbreekt aan ieder bewijs dat de software van Kaspersky Lab daadwerkelijk ingezet wordt voor het uitvoeren van spionage of sabotage. Bij het communiceren van het besluit schrijft de minister in de Kamerbrief[36] dat er in Nederland geen concrete gevallen van misbruik bekend zijn. De Binding Operational Directive (afgekort BOD) in de Verenigde Staten ontbeert bewijs dat Kaspersky Lab een probleem met de producten heeft of iets niet goed zou doen. In de civiele procedure tussen Kaspersky Lab en de Amerikaanse overheid schrijft de rechter in zijn vonnis[37] ook: “The BOD was not based on a determination that Kaspersky Lab was disloyal or guilty of any wrongdoing”. De Belgische premier Charles Michel stelt[38] dat zijn Centrum voor Cybersecurity ‘geen objectieve technische informatie heeft en niet beschikt over onafhankelijke studies die aantonen dat de toepassingen van Kaspersky Lab kwaadaardig zijn of een dreiging betekenen’. Het Duitse Bundesamt für

[34] https://en.wikipedia.org/wiki/Carbanak -
[35] https://www.alertonline.nl/overzicht-partners - geverifieerd op 13 november 2018
[36] Bijlage 1, pagina 3 eerste alinea
[37] Bijlage 12, pagina 258
[38] https://www.tijd.be/nieuws/archief/Belgie-bant-Russische-antivirussoftware-niet/10064355 - geverifieerd op 10 november 2018

Sicherheit in der Informationstechnik, het overheidsexpertisecentrum, stelt[39] niet met een waarschuwing te komen 'omdat het geen aanwijzingen heeft voor malafide praktijken of softwarekwetsbaarheden'. In antwoord op vragen uit het Europees Parlement schrijft[40] de Europese Commissie 'geen indicatie voor enig gevaar te hebben'. Ook het Zwitserse Federale Stuurorgaan stelt ook geen bewijs te hebben dat Kaspersky Lab bij welke aanval ook betrokken is geweest[41].

Malware is malware-beleid

Kaspersky Lab voert een beleid met als uitgangspunt 'malware is malware' ongeacht de maker ervan. Het ontkent mee te werken aan spionageoperaties in welk land ook. Het bedrijf schroomt er dan ook niet voor malware bloot te leggen[42] waar de herkomst zeer waarschijnlijk Russisch is en militaire objecten van NATO-landen het doelwit[43] zijn of bijvoorbeeld het Witte Huis een doelwit[44] is. Ook wijst het bedrijf op basis van de kennis die zij hebben welke actoren een continue dreiging vormen voor Nederland[45], een Advanced Persistant Threat (APT). Daarbij wordt gekeken naar alle spelers, ongeacht hun afkomst.
Bij de uitbraak van het NotPetya -virus, dat door de Amerikaanse overheid wordt toegedicht als afkomstig van de Russische overheid, analyseert[46] Kaspersky Lab de malware. Het virus blijkt afkomstig uit boekhoudsoftware in de Oekraïne en raakt ook Nederlandse belangen. Een containerterminal in de Rotterdamse haven moet worden gesloten. De virusbestrijder waarschuwt dat betalen zinloos is, omdat de makers de schade niet ongedaan kunnen maken. Het bedrijf betoogt waarom dit geen Petya-virus is en noemt het daarom NotPetya, wat daardoor ook die naam kreeg. Het gevolg van het 'malware is malware'-beleid is dat ook malware van westerse origine wordt blootgelegd, zoals bijvoorbeeld gebeurde bij de bekende Stuxnet-malware[47]. Hier was het doelwit het Iraanse nucleaire programma, waarbij naar verluidt zowel Israël als de Verenigde Staten in de aanval een rol hadden.

Kwaliteitsindicatoren

Kaspersky Lab scoort bij gezaghebbende onderzoeksinstellingen hoog. Zo bleek het bedrijf in augustus[48] de maximale scores (6 uit 6) te halen voor de detectie van malware, de performance en de bruikbaarheid. Dit geldt voor zowel de persoonlijke als de zakelijke edities bij de tests van AV Tests. Bij de test van AV Comparatives van malware die op

---

39 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/BSI_Stellungnahme_Kapersky_11102017.html - geverifieerd op 10 november 2018

40 http://www.europarl.europa.eu/doceo/document/P-8-2018-000603-ASW_EN.html - geverifieerd op 10 november 2018

41 https://www.nzz.ch/schweiz/westliche-regierungen-werfen-der-russischen-it-firma-kaspersky-lab-spionage-vor-sie-eroeffnet-im-november-in-zuerich-ein-neues-transparenzzentrum-ld.1430956

42 https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/ - geverifieerd op 10 november 2018

43 https://securelist.com/a-slice-of-2017-sofacy-activity/83930/ - geverifieerd op 10 november 2018

44 https://securelist.com/the-cozyduke-apt/69731/ - geverifieerd op 10 november 2018

45 https://securelist.com/threats-in-the-netherlands/88185/ - geverifieerd op 10 november 2018

46 https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ - geverifieerd op 10 november 2018

47 https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet - geverifieerd op 10 november 2018

48 https://www.av-test.org/en/antivirus/home-windows/windows-10/august-2018/kaspersky-lab-internet-security-19-183111/ - geverifieerd op 10 november 2018

internet is aangetroffen[49] is dat beeld niet anders. In de test hoe effectief leveranciers zijn in het verwijderen van kwaadaardige software scoort het bedrijf als enige 99 van de 100 punten[50]. Kaspersky Lab is daarmee aantoonbaar een van de koplopers in het detecteren van malware en leidend in het verwijderen ervan. Onderzoeksbureau IDC[51] geeft aan niet te twijfelen aan de kwaliteit. Er is op basis van publiek beschikbare onderzoeken geen reden om aan de kwaliteit van de software van Kaspersky Lab te twijfelen.

In de software van Kaspersky Lab zijn de afgelopen vijf jaar (in de periode 4 november 2013 tot en met 4 november 2018) negentien lekken gevonden, waarbij de gemiddelde ernst 5.8 op een schaal van 1 tot 10 is. Dit is relatief weinig gezien de omvang van ruim 2 miljoen regels broncode. Ook hier is geen sprake van een significante afwijking ten opzichte van andere marktpartijen. Er zijn een paar partijen die minder fouten hebben gehad, maar die in ernst gemiddeld hoger scoren. Ook zijn er gerenommeerde partijen die meer fouten hebben gehad en hoger scoren. Dit beeld is geen aanleiding te twijfelen aan de software van Kaspersky Lab.

Bug bounty

Het bedrijf biedt beloningen voor het vinden van zwakheden in de software. Voor grote fouten worden beloningen tot 100.000 dollar (ruim 89.013 euro[52]) geboden[53].

Penetratietest

De software van Kaspersky Lab heeft in Nederland ten minste één bekende penetratietest ondergaan en die goed is doorstaan. De test is uitgevoerd door telecombedrijf KPN in samenwerking met een van de grootste beveiligingsbedrijven ter wereld. In de brief voorafgaand aan het besluit van het kabinet heeft Kaspersky Lab hierop gewezen[54].

Audit van de broncode

Kaspersky Lab opent drie Transparency Centers waar het bedrijf inzage geeft in de producten, de werking van diensten en de broncode van de software. Het eerste centrum bevindt zich in Zürich, Zwitserland. Hierdoor is het voor gebruikers mogelijk een diepgaande audit uit te voeren op de broncode van de programma's. Zo is onafhankelijk onderzoek mogelijk naar het risico op spionage en sabotage en naar de kwaliteit en effectiviteit van de software. Het bedrijf biedt niet alleen de mogelijkheid om de huidige softwareversie te laten toetsen, maar ook aankomende (beveiligings)updates en nieuwe versies. Voordat een organisatie nieuwe programmatuur toelaat tot de eigen omgeving is het daardoor mogelijk gemaakt om deze vooraf te toetsen op deugdelijkheid.

Op 12 november 2018 is in het kader van dit rapport door Brenno de Winter een verificatiebezoek aan het Transparency Center in Zürich, Zwitserland gebracht. Daar is de

[49] https://www.av-comparatives.org/tests/real-world-protection-test-august-2018-factsheet/ - geverifieerd op 10 november 2018
[50] https://www.av-comparatives.org/tests/malware-removal-test-2018/ - geverifieerd op 10 november 2018
[51] https://www.linkedin.com/pulse/until-theres-some-evidence-dont-kick-out-kaspersky-dominic-trott/ - geverifieerd op 12 november 2018
[52] Berekend op 13 november 2018 via xe.com
[53] https://www.kaspersky.com/blog/bug-bounty-boost-2018/21477/ - geverifieerd 13 november 2018
[54] Bijlage 5 pagina 56

broncode van de antivirussoftware getoetst. Op onderdelen is middels een steekproef vastgesteld dat de aanwezige broncode daadwerkelijk omzet naar exact dezelfde code die op de referentiecomputer draait. Er zijn geen verschillen aangetroffen, waardoor het aannemelijk is te veronderstellen dat het bedrijf echt alle broncode inzichtelijk maakt. Ook is vastgesteld dat bij een audit er geen wijzigingen in de broncode kunnen worden geïntroduceerd. De broncode is goed gedocumenteerd. Zo is bijvoorbeeld duidelijk welke medewerker welke veranderingen heeft doorgevoerd en is er een goed versiebeheer. Dit waarborgt ook om snel updates te kunnen toetsen. De broncode is geschreven in de programmeertaal C++ en ziet er netjes en schoon uit. Dat maakt het houden van een audit goed mogelijk.

Het bedrijf verplaatst de assemblage van de software naar Zwitserland, alsmede de opslag van persoonsgegevens van in ieder geval inwoners van de Europese Unie, Zwitserland en het Verenigd Koninkrijk na de Brexit. Dat betekent dat er geen data in de Russische Federatie worden bewaard. Hiermee geeft Kaspersky Lab effectief invulling aan de Algemene Verordening Gegevensbescherming (AVG). Zwitserland heeft een hoog niveau van gegevensbescherming dat sterk lijkt op de AVG. Kaspersky Lab voldoet daarom aan zowel Zwitserse als EU-regelgeving voor de bescherming van persoonsgegevens.

Om de maatregel van het Nederlandse kabinet echt op waarde te schatten heeft Kaspersky Lab voor dit onderzoek toegang tot de broncode verschaft. De waarde van een dergelijke toegang staat of valt met de vraag of toegang is verschaft tot alle broncode. Wanneer een klein gedeelte niet geïnspecteerd kan worden, zou daar ook de mogelijkheid zitten om een achterdeur in te bouwen. Via een steekproef zijn modules van de broncode in uitvoerbare software omgezet en vergeleken met een versie die op een losse computer actief is. Samenvattend geeft Kaspersky Lab inzicht in de broncode, laat verificaties toe en verschaft daarmee openheid waarmee auditors kunnen toetsen op risico's. Daarmee bestaat vanaf november 2018 daadwerkelijk de mogelijkheid voor het bedrijfsleven en overheden om zelf de kwaliteit te toetsen of dit door experts te laten doen.

Een andere vraag is of het voor Nederland inhoudelijk mogelijk is om de software kwalitatief te toetsen nu het Transparency Center geopend is. Deze vraag kan bevestigend worden beantwoord. De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) beschikt over het Nationaal Bureau Verbindingsbeveiliging (NBV). Zij hebben voldoende expertise in huis om een dergelijke test uit te voeren, beschikken over kwaliteitscriteria waar producten aan moeten voldoen en voeren dergelijke tests regelmatig uit. Het toetsen van complexe producten geeft deze dienst de juiste expertise in het zoeken naar achterdeuren in software. NBV doet dit niet alleen voor gerubriceerde[55] informatie voor Nederland, maar ook voor onder andere de European Space Agency, de EU en NATO[56]. Op dit moment is geen enkel besturingssysteem of antiviruspakket goedgekeurd. Dat is opmerkelijk, omdat het kabinet in de maatregel van dergelijke software stelt dat juist deze diepgaande en brede toegang tot netwerken en systemen heeft. Wie dat zo ervaart, moet voor systemen in vitale sectoren en de Rijksoverheid opteren voor een hoog niveau van zekerheid en daarom controles moeten afdwingen.

[55] Afhankelijk van de keuring gaat dat van departementaal vertrouwelijke informatie tot gegevens die het predicaat 'staatsgeheim zeer geheim' hebben.
[56] Bijlage 15, pagina 377

7. Kaspersky Security Network

Voor het uploaden van malware samples moet de gebruiker toestemming geven.

De strijd tegen malware is een voortdurende wapenwedloop. Dagelijks verschijnt er nieuwe malware en passen aanvallers bestaande malware aan. Zo spelen ze in op nieuwe detectiemogelijkheden, zwakheden in besturingssystemen of gebruikersapplicaties. Het doel is om deze kwetsbaarheden actief te misbruiken voor diefstal, spionage of sabotage. Kaspersky Lab detecteert dagelijks circa 360.000 kwaadaardige malwaresamples[57]. Antivirussoftware detecteert vaak afwijkend gedrag of ongeïdentificeerde malware. Diverse leveranciers bieden de mogelijkheid om deze malware geautomatiseerd naar het bedrijf op te sturen voor nadere analyse. De antivirusbedrijven kunnen zo sneller inspelen op actuele dreigingen en de kennis omzetten in regels voor de software om de nieuwe malware sneller te herkennen en te stoppen. Deze informatie wordt in de regel gedeeld met andere partijen om zo gezamenlijk effectiever hiertegen te kunnen optreden en dubbel werk te voorkomen. Kaspersky Lab beschikt ook over een dergelijke dienst: het Kaspersky Security Network (KSN). Wie dat wil gebruiken, moet daarvoor bij installatie of op een later moment expliciete toestemming geven. De deelname kan ook op ieder moment in de tijd weer worden beëindigd.

Bij het KSN activeert de dienst op het moment dat de antivirussoftware vreemd gedrag of malware herkent. Op dat moment zoekt het systeem naar het stukje software waarvan het meent dat het malware is. Het stuurt een digitale handtekening van de malware (maar niet de malware zelf) op. Het KSN geeft aan of de malware bekend is. Is dat niet het geval dan stuurt de antivirussoftware de malware naar het KSN op, zodat het onderzocht kan worden. Het document waar de malware in zit genesteld wordt niet verzonden. Wel gaat mee wat voor document (programma, tekstverwerkingsbestand, enzovoort) betreft.

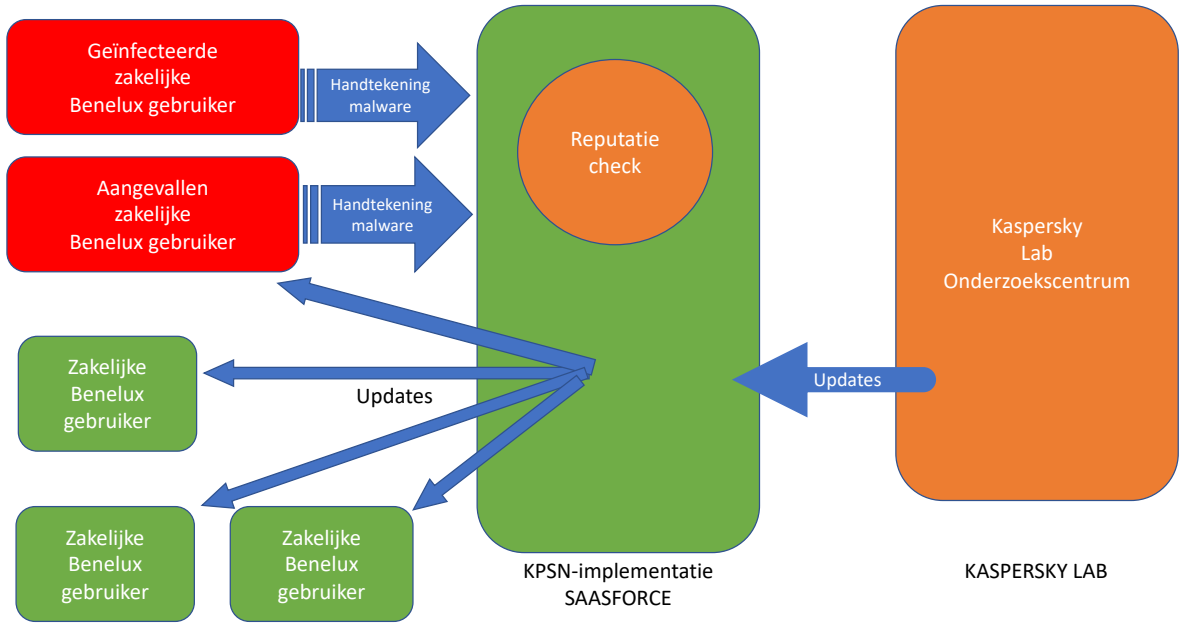
Een aantal maatregelen beschermen gebruikers en organisaties tegen het mogelijk stelen van documenten of het spioneren via antivirussoftware:

1. Transparency Center. In het Transparency Center kan de broncode worden gecontroleerd. De lopende audit door een van de ‘Big Four’-bedrijven toetst of de antivirussoftware alleen iets naar het KSN stuurt als hiervoor is gekozen door de gebruiker.
2. Procedurele audits. Een van de ‘Big Four’-bedrijven voert een audit naar de procedurele aspecten van het KSN uit. Hierdoor wordt inzichtelijk of het bedrijf daadwerkelijk zo met de data omgaat als ze stellen.
3. Awareness en instructies aan gebruikers. Door verplichte[58] training aan gebruikers worden mensen opgeleid om goed en correct om te gaan met de hulpmiddelen die

[57] Cijfers over 2017 - https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-detects-360000-new-malicious-files-daily - geverifieerd op 9 november 2018
[58] Bijlage 11 BIR 2017 - 6.2 pagina 213 en 7.2.2/7.2.3 pagina 215

aan hen worden verstrekt en een geïnformeerde keuze te maken om deze functionaliteit wel/niet te gebruiken.

4. Het belangrijkst is een nieuwe waarborg die Kaspersky Lab heeft gemaakt voor zakelijke gebruikers in de Benelux. Bij het Nederlandse bedrijf SaaSForce wordt een kopie van de beveiligingsinformatie afkomstig van Kaspersky Lab opgeslagen[59]. Er vloeit echter vervolgens geen data naar Kaspersky Lab, waardoor procedureel is uitgesloten dat deze technologie buiten de EU te misbruiken is voor spionage. Dit is het Kaspersky Private Security (KPSN).



De KPSN-oplossing bestaat als concept al langer. In Nederland heeft KPN een dergelijke oplossing geïmplementeerd. Al voor de discussie over spionage en sabotage was het mogelijk dat ook de Rijksoverheid deze oplossing installeert in de Rijks-datacentra. Het is voor de overheid dus mogelijk om het wegvloeien van informatie onder eigen regie te voorkomen.

Het nadenken over het gebruik van functionaliteit, zoals het Kaspersky Security Network, is noodzakelijk. In 2017 onthult de *Wall Street Journal*[60] dat een inlichtingendienst met succes heeft ingebroken bij Kaspersky Lab. Na het bekijken van de software stelt de krant dat de inlichtingendienst beweert dat het mogelijk is voor de Russische inlichtingendiensten om documenten te zoeken. Kaspersky Lab zou een 'tool voor spionage' zijn. Het bedrijf onderzocht de inbraak al in juni 2015[61] en komt naar aanleiding van de berichtgeving met een rapportage[62].

[59] https://saasforce.eu/benelux-klanten-van-kaspersky-lab-profiteren-van-unieke-real-time-bescherming-zonder-dat-data-de-eu-verlaten/ - geverifieerd 11 november 2018
[60] https://www.wsj.com/articles/russian-hackers-scanned-networks-world-wide-for-secret-u-s-data-1507743874 - geverifieerd op 11 november 2018
[61] https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/ - geverifieerd 12 november 2018
[62] https://securelist.com/investigation-report-for-the-september-2014-equation-malware-detection-incident-in-the-us/83210/ - geverifieerd op 9 november 2018

Als Kaspersky Lab de bewering van de *Wall Street Journal* onderzoekt, komt het wel iets bijzonders tegen: Het ontdekt een computer die veel malware meldde. Het zit in een illegale versie van Microsoft Office, losse malware en zelfs broncode van de Equation Group-malware. In een zip-bestand zitten meerdere malware bestanden en vier gerubriceerde Word documenten. De malware betreft nieuwe variaties van de Equation Group-malware. De samples worden naar het KSN verstuurd. In een van de gerubriceerde Word-documenten herkent de antivirussoftware broncode van malware. Op basis van de broncode, de unieke samples vermoeden analisten van Kaspersky Lab dat de Kaspersky-gebruiker een maker van malware kan zijn. De verdenking ontstaat dat de in het artikel genoemde NSA-medewerker zijn werk mee naar huis heeft genomen. Verder vermoeden de onderzoekers dat de computer van de persoon zelf gehackt is, omdat er een achterdeur(malware) in de illegale Microsoft Office-versie zit. Kaspersky Lab verdenkt Russische hackers van deze hack. Gedurende een langere periode is de antivirussoftware op deze computer niet gebruikt, waardoor de computer geïnfecteerd kon raken.

Een dergelijk scenario kan zich in de situatie van de SaasForce Benelux niet voordoen. Kaspersky Lab krijgt informatie over malware niet doorgestuurd. Het bedrijf kan niet bij de bestanden komen, Russische wetgeving heeft geen enkele invloed op het in Nederland en België gevestigde SaasForce. Deze beveiligingsslag maakt het scenario dat een Russische inlichtingendienst Kaspersky Lab dwingt tot een succesvolle medewerking aan een spionage- of sabotageoperatie zeer onwaarschijnlijk.

8. Gevolgen van het kabinetsbesluit

De voorzorgsmaatregel van het kabinet heeft nadelige gevolgen voor zowel de Nederlandse overheid, het bedrijfsleven, burgers, als uiteraard het bedrijf Kaspersky Lab. Kaspersky Lab steekt veel energie in het kosteloos bijdragen aan de bestrijding van cybercrime. Met de Nederlandse politie was een goede werkrelatie opgebouwd. Door de maatregel van het kabinet is die samenwerking stilgevallen. Uit gesprekken met Kaspersky Lab wordt duidelijk dat ten minste drie grote strafzaken worden getroffen. Een zaak was net opgestart, een andere zaak betreft een langer lopend onderzoek en een derde was tijdelijk on hold gezet. Voor deze zaken geldt dat van expertise door Kaspersky Lab geen gebruik meer kan worden gemaakt. Expertise van vergelijkbare kwaliteit is mogelijk te vinden, maar zulke expertise is doorgaans kostbaar. Na het voorbeeld van Kaspersky Lab is het de vraag hoe aantrekkelijk het is voor bedrijven om diensten aan te bieden aan een relatief klein land als Nederland.

Het National Cyber Security Center (NCSC) verwijst[63] al in maart 2014 in het Cybersecuritybeeld Nederland nadrukkelijk naar de kwetsbaarheid van ons land voor spionage via een gerichte, geavanceerde en aanhoudende aanval, bekend als een Advanced Persistent Threat: “Nederland is met zijn open samenleving en grote technische en wetenschappelijke kennis en zijn economische positie een aantrekkelijk doelwit voor spionage. Bovendien kan het maanden en soms zelfs jaren duren voordat een Advanced Persistent Threat (APT) wordt ontdekt.” Een belangrijke expertise van Kaspersky Lab is het intensief onderzoek doen naar dergelijk APT’s. Precies dit soort tijdkritische informatie, kennis en ondersteuning is belangrijk bij incidenten, in de strijd tegen spionage en sabotage en voor het veiligstellen van kennis noodzakelijk voor onze digitale ambities.

Nu is de realiteit dat contacten tussen Nederlandse overheden en Kaspersky Lab (en in de toekomst mogelijk ook andere globale bedrijven) na het kabinetsbesluit stroever verlopen. Dat betekent bijvoorbeeld bij grote uitbraken van malware, offensieve spionage en sabotageacties in de richting van Nederland dat Kaspersky Lab weliswaar waarschuwt, maar dat het ontbreekt aan een slagvaardige samenwerking. Bij grotere globale incidenten is er opeens heel veel vraag naar schaarse kennis en kunde. Een slechte werkrelatie helpt dan niet. Bij de uitbraak van de NotPetya-malware was het onder andere Kaspersky Lab, die snel en accuraat informatie kon aanleveren. Het gevolg van dit incident dat een containerterminal in de Rotterdamse haven verstoorde is enorm. Los van de verstoring van het bedrijfsleven betreft de schade op basis van conservatieve schattingen van alleen NotPetya [64] meer dan een miljard dollar[65].

Een van de samenwerkingsverbanden tussen de overheid (voornamelijk de politie) en Kaspersky Lab en McAfee is het No More Ransomware-initiatief. Dit initiatief is een samenwerkingsverband om de cryptografie van ransomware zo te kraken, dat burgers en bedrijfsleven zonder losgeld te betalen hun versleutelde bestanden terug kunnen krijgen.

---

[63] Bijlage 17, pagina 446 en 447.

[64] Maritiem bedrijf Maersk tussen de € 200 en € 300 miljoen – Bijlage 14, pagina 334, Nuance Communications € 92 miljoen dollar, farmabedrijf Merck €135 miljoen - https://www.security.nl/posting/552421/Nuance+Communications+schat+schade+NotPetya+op+92+miljoen+dollar – geverifieerd 10 november 2018

[65] Rapportage van het bedrijf Cyber Reason: https://www.cybereason.com/hubfs/Content%20PDFs/Paying-the-Price-of-Destructive-Cyber-Attacks.pdf?t=1541798173918 – geverifieerd 10 november 2018

Om dit goed te kunnen doen, is hoogwaardige expertise op zowel het gebied van malware als cryptografie nodig. Deze kennis is beperkt en in onvoldoende mate aanwezig bij de Nederlandse overheid. Nu de werkrelatie tussen de overheid en Kaspersky Lab tot stilstand is gekomen, betekent dit dat slachtoffers van digitale aanvallen een kleinere kans hebben om hun bestanden terug te krijgen.

Voor Kaspersky Lab is het besluit schadelijk. Al schrijft het kabinet in de voorzorgsmaatregel dat er geen incident speelt, toch ontstaat een beeld dat er 'iets mis is' met het bedrijf. Het is een idee van 'waar rook is, is vuur'. Voor een bedrijf dat zich richt op bescherming tegen malware, spionage en sabotage is juist de beschuldiging dat het juist voor dat soort doelen wordt ingezet – ook al is daar geen voorbeeld van bekend – schadelijk. De procedure waar geen enkele vorm van wederhoor is geweest of waar het signaal is geweest dat er een vorm van overleg heeft plaatsgevonden, kan een beeld oproepen dat het 'wel zo erg is dat er iets heel groots moet zijn'. Dat beeld komt niet in de laatste plaats door de brede communicatie van de voorzorgsmaatregel via bijvoorbeeld een Kamerbrief en een televisieoptreden van de minister van Justitie en Veiligheid bij *Pauw*.

Schadelijk is ook de communicatie door het NCSC "Advies aan vitaal: stop met antivirus-software Kaspersky Lab"[66] zonder enige nuance in het bericht. Juist het NCSC is het centrale punt waar veel adviezen vandaan komen. De Rijksoverheid en de vitale sectoren hebben rechtstreeks contact met het NCSC en er zijn directe, niet-publieke kanalen beschikbaar. Door juist publiekelijk dit advies – dat geen algemene werking zou hebben – naar buiten te brengen, wekt de overheid de indruk verkapt een algemeen advies uit te brengen. Dit beeld wordt versterkt door in de communicatielijn op juridische consequenties te wijzen[67].

In communicatie stelt het kabinet dat andere organisaties een eigen afweging dienen te maken. Veel overheden en bedrijven zijn niet in staat zo'n ingewikkelde risicoanalyse goed uit te voeren. De vrees dat inlichtingendiensten mogelijk meer kennis hebben en zo publiekelijk naar buiten wordt getreden, helpt niet. Bij het maken van een afweging voor dreigingen als 'spionage' en 'sabotage' zal iedere zichzelf respecterende organisatie zichzelf als potentieel doelwit zien. Deze combinatie van factoren maakt dat de reikwijdte van de voorzorgsmaatregel veel breder opvolging krijgt dan de Rijksoverheid en vitale sectoren.

Naast het voorgaande punt is de maatregel langdurig schadelijk voor Kaspersky Lab. De maatregel gaat formeel over alleen de antivirussoftware. Maar die komt in veel producten voor. Zo stuurt de CIO Rijk een lijst[68] van vijftien pagina's naar partijen in het kader van de uitvraag welke Kaspersky Lab-producten in gebruik zijn. De lijst bestaat uit partners die de oplossing van Kaspersky Lab in hun oplossing hebben verwerkt. Met het advies treft het kabinet die spelers ook gedeeltelijk. Door die stap te zetten, is het niet ondenkbaar dat sommige spelers om die reden een samenwerkingsverband met Kaspersky Lab opzeggen. Dat is opnieuw schadelijk voor het bedrijf.

[66] https://www.ncsc.nl/actueel/nieuwsberichten/advies-aan-vitaal-stop-met-antivirussoftware-kaspersky-lab.html - geverifieerd 10 november 2018 en Bijlage 18 pagina 506
[67] Bijlage 6 pagina 70, overweging 21 en 22
[68] Bijlage 5 pagina 37 t/m 51

10. Conclusies en aanbevelingen

De documenten uit het Wob-verzoek en de brief van het kabinet tonen dat Amerikaanse documenten bepalend zijn voor de maatregel. De Europese situatie is niet de Amerikaanse. Zo kennen wij EU-wetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG/GDPR). In Nederland bepalen normenkaders, zoals Baseline Informatiebeveiliging Rijksdienst, hoe organisaties beveiliging inregelen. Inmiddels verplicht de Wet beveiliging netwerk- en informatiesystemen het houden aan normen. Uit de reconstructie en analyse van de besluitvorming ontstaat een beeld van selectieve beargumentering. Het is onduidelijk welke methodiek voor risicoanalyse is gehanteerd. Ook ontbreken vooraf gestelde beoordelingscriteria voor antivirussoftware.

Soms zijn feiten incorrect weergegeven. “Kaspersky Lab is een Russisch bedrijf met haar hoofdkantoor in Rusland en valt daarmee onder Russische wetgeving”, schrijft het kabinet bijvoorbeeld aan de Tweede Kamer. Dat is incorrect. Kaspersky Lab is een Britse onderneming, waarvan inderdaad het hoofdkantoor in Rusland staat.

Het beeld van selectieve beargumentering wordt versterkt door:

- het niet wegen van verschillen tussen ons land en de situatie in de VS;
- het niet wegen van normenkaders;
- het niet wegen van kwaliteitsaudits van Kaspersky Lab die proactief zijn aangeboden;
- het niet wegen van informatie vanuit België, Duitsland, Zwitserland en de Europese Commissie;
- het ontbreken van technische duiding rond antivirussoftware;
- het ontbreken van eigen weging rond het Russische wetgevend kader;
- het ontbreken van omstandigheden wanneer het risico wel of niet speelt;
- het niet houden van wederhoor.

Het kabinet stelt geen kennis te hebben van spionage of sabotage waar Kaspersky Lab op enige wijze bij is betrokken. De drie observaties van het kabinet gaan uit van algemeenheden, die onvoldoende aansluiten bij de situatie Kaspersky Lab:

1. Dat antivirussoftware diep in een systeem zit, betekent niet automatisch dat er uitgebreide toegang is voor spionage en sabotage. Verplichte controlemaatregelen bij overheden en bedrijven en de uitgebreide toetsing van de software en allerhande procedures van Kaspersky Lab maken de risico’s zeer beheersbaar.
2. Het Russisch wetgevend kader voor inlichtingen- en veiligheidsdiensten geldt nadrukkelijk niet alleen voor het onder een Britse holding functionerende Kaspersky Lab. Iedere softwaremaker op systeemniveau (antivirus- en besturingssystemen) met vestigingen in de Russische Federatie heeft dit probleem. Overigens zijn er meer landen, zoals bijvoorbeeld China, de Verenigde Staten en Nederland waar spionage-wetgeving bedrijven kan vragen om medewerking. De wetgeving is daarmee niet heel uniek.
3. De Russische Federatie voert operaties van spionage en sabotage uit. Uit jaar-verslagen van inlichtingendiensten blijkt dat veel landen hiermee bezig zijn. Juist Kaspersky Lab laat zich kwalificeren als een effectieve stoorzender bij veel operaties door ongeacht de afkomst van de aanval en zonder schroom Russische operaties bloot te leggen. Het bedrijf hanteert een ‘malware is malware’-beleid ongeacht de afkomst.

Met de introductie van het Transparency Center in Zürich is zet Kaspersky Lab een effectieve stap in de weerbaarheid tegen spionage en sabotage. Het kunnen toetsen van de broncode maakt risico's beheersbaar. Kaspersky Lab laat zelf een audit door een Big Four-bedrijf uitvoeren. De theoretische mogelijkheid is daarmee praktijk. Dit is een effectieve stap in het hinderen bij het uitvoeren van spionage en sabotage via de software van Kaspersky Lab. Door de verwerking van gegevens voor Europese klanten en de software-assemblage te verplaatsen naar Zwitserland, wordt het lastiger voor de Russische Federatie om software van Kaspersky Lab te misbruiken. Samenvattend: De stap is effectief.

De berichtgeving over de inbraak bij Kaspersky Lab door een inlichtingendienst en de beschuldiging dat gerubriceerde documenten bij het bedrijf terechtkwamen, heeft wel impact gehad op Kaspersky Lab. Het is de vraag of het voldoende is om te wijzen dat deelname aan het Kaspersky Security Network altijd vrijwillig is, de antivirussoftware precies deed wat het moest doen: malware detecteren en samples opsturen en detecteren van de achterdeur in Microsoft Office. De oplossing van het Kaspersky Private Security Network (KPSN), zoals ook toegepast met SaasForce voor de Benelux, voorkomt dat data naar Kaspersky Lab gaat. Maar het verhaal rond de vermoedelijke NSA-medewerker rechtvaardigt niet de conclusie dat data gestolen kan worden via het KSN. Het inzetten van de antivirussoftware door inlichtingendiensten voor spionage en sabotage is met het KPSN moeilijk voorstelbaar. Ondertussen blijft het mogelijk nieuwe malware in seconden te detecteren. De maatregel is effectief.

Het besluit rond Kaspersky Lab is voor alle partijen schadelijk. De (gratis) geboden hoogwaardige expertise rond malwarehulp bij drie strafzaken is komen stil te liggen. Met schaarste aan goede kennis is dat kwalijk. Kaspersky Lab heeft bewezen bij grote malware-incidenten snel, slagvaardig en accuraat informatie te kunnen leveren. De verstoorde vertrouwensrelatie maakt het voor Kaspersky Lab lastig Nederland te waarschuwen. Het stoppen van de samenwerking tussen de overheid en Kaspersky Lab betekent voor slachtoffers van gijzelvirussen dat zij minder kans maken op het terugkrijgen van hun data. Voor Kaspersky Lab zijn de maatregel en de communicatie erover ronduit schadelijk. Door hard te stellen dat de software een hulpmiddel voor spionage en sabotage is, ontstaat ten onrechte het beeld dat de malwarebestrijder zelf malware levert.

De Amerikaanse overheid besluit op 13 september 2017 de software van Kaspersky Lab te verbannen. Nederland neemt op 15 mei 2018 eenzelfde besluit op basis van het Amerikaanse dossier. Dat is acht maanden en twee dagen later. Gaat het hier om zorgvuldige of ambtelijke trage besluitvorming? Dit is een relevant vraagstuk voor het kabinet als het slagvaardig wil omgaan met de ernstige dreiging van spionage en sabotage.

De stelling dat software op systeemniveau brede en diepe toegang heeft, roept in de Nederlandse situatie de vraag op of de vitale sectoren de geldende normen voldoende naleven. De maatregelen in die normen wapenen tegen risico's van te brede toegang tot informatie en juiste detectie van incidenten.

De CIO Rijk moest uitvragen welke software van Kaspersky Lab in gebruik is. Dat roept de vraag op of er voldoende zicht is op gebruikte software. Is op de juiste plaats bij de overheid

bekend welke software er in gebruik is (en daarmee welke risico's er spelen)? Onder software op het systeemniveau zit hardware, die ook in netwerkcomponenten zit. Is inzichtelijk welke risico's daar spelen? Vergelijkbare vragen zijn ook gerechtvaardigd voor de inzet van clouddienstverleners in de vitale sectoren, omdat bij hen veel data bij elkaar komt en vaak onduidelijk is naar welke landen die gegevens gaan.

De algemene redenering in de voorzorgsmaatregel van het kabinet rechtvaardigt de vrees voor andere bedrijven dat zij ook zonder enige wederhoor volledig worden uitgesloten en er publiekelijk voor het bedrijf wordt gewaarschuwd. De kwaliteit van producten, bijdragen aan de veiligheid in Nederland en waarborgen in het Europees en Nederlands regelgevend kader doen er immers niet toe.

Nederland heeft forse ambities op het gebied van innovatie en informatiebeveiliging. Dat legt de lat hoog om zware beslissingen zeer zorgvuldig en goed gemotiveerd te nemen. Kaspersky Lab gaat serieus met angsten van spionage en sabotage om. Het Transparency Center is een effectieve manier om zowel op basis van feiten als emotie zorgen weg te nemen. Er kan daadwerkelijk worden getoetst. De Benelux-specifieke oplossing met SaasForce voegt nog een extra beveiligingslaag toe aan de software van Kaspersky Lab. Het bedrijf bewijst bij herhaling en voortduring dat software en procedures – wat beveiliging betreft – in de haak zijn. Het loopt daarmee op veel leveranciers voor. Toch is dat op zichzelf niet bijzonder, want toetsbare kwaliteit hoort bij inkoop van software de norm te zijn. Alles bij elkaar genomen zou een heroverweging van het genomen besluit rechtvaardig en in ieders belang zijn.