Cybercheck: ook jij hebt supply chain risico's!

Een handreiking voor het inventariseren en beheersen van supply chain risico's voor producten en diensten uit landen met een offensief cyberprogramma

Doelgroep

Deze handreiking richt zich op publieke en private organisaties die over Te Beschermen Belangen (TBB) ten aanzien van de Nationale Veiligheid (NV) beschikken. Organisaties kunnen aan de hand van de bestaande richtlijnen zelf beoordelen of zij over een of meerdere TBB-NV beschikken.[28]

Deze handreiking is geschreven voor personen die binnen bovengenoemde organisaties op tactisch niveau werkzaam zijn en een rol hebben bij het beheersen van digitale risico's met betrekking tot de inzet van producten en diensten afkomstig uit landen met een offensief cyberprogramma.[29] Dit zijn in de eerste plaats de Chief Information Officer (CIO), de Chief Technology Officer (CTO) en de Chief Information Security Officer (CISO). Daarnaast kan deze handreiking ook gebruikt worden door inkoopafdelingen, cybersecurityspecialisten en ICT- en security-architecten.

Aan deze handreiking hebben bijgedragen

Bluebird & Hawk BV, De Nederlandse Vereniging van Banken, ICT Group, Nederlandse Spoorwegen en Technolution

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)
De NCTV dient de nationale veiligheid. Wij beschermen belangen, signaleren dreigingen en versterken weerbaarheid.

Nationaal Cyber Security Centrum (NCSC)
Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC draagt bij aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving. Daarnaast heeft zij als doel de vitale infrastructuur en Rijksoverheid van Nederland te beschermen door de digitale weerbaarheid van Nederland te vergroten en de gevolgen van cyberincidenten te beperken.

Algemene Inlichtingen en Veiligheidsdienst (AIVD)
De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) beschermt de democratie tegen nationale en internationale dreigingen, zodat we in vrijheid kunnen leven. We waken, vaak onzichtbaar, over Nederland en zijn bevolking. We doen daarvoor onderzoek in binnen- en buitenland. De AIVD doet wat nodig is om te voorkomen dat staten, organisaties of personen onze rechtsstaat tegenwerken, ondergraven of aanvallen.

CIO Rijk
CIO Rijk bevordert de continuïteit, kwaliteit, effectiviteit en efficiëntie van de digitalisering van de Rijksoverheid. Dit doet zij door ervoor te zorgen dat alle (rijks-)ambtenaren altijd en overal, veilig kunnen (samen-)werken. CIO Rijk verbindt de onderdelen van de Rijksoverheid door rijksbreed I-beleid en -kaders op te stellen, stuurt de doorontwikkeling en exploitatie van Rijksbrede ICT-Voorzieningen aan, borgt informatiebeveiliging en privacy en versterkt de I-functie van het rijksbrede CIO-stelsel. CIO Rijk coördineert, faciliteert en monitort.

Inhoud

Inleiding

De toenemende digitalisering biedt de Nederlandse samenleving voordelen, maar brengt ook risico's met zich mee. Zo gaat er de laatste jaren steeds vaker aandacht uit naar de risico's rondom de inzet van producten en diensten[1] uit landen met een offensief cyberprogramma dat gericht is tegen Nederland of Nederlandse belangen.

Landen met een offensief cyberprogramma kunnen tijdens de ontwikkeling of het onderhoud van producten en diensten invloed uitoefenen op de supply chain.[2] Voor deze landen kan gelden dat zij bedrijven en burgers in hun land op grond van wetgeving kunnen verplichten tot medewerking, waardoor deze bedrijven en burgers gedwongen worden om digitale achterdeuren in hun product of dienst in te bouwen.[3]

Dit biedt landen met een offensief cyberprogramma de mogelijkheid om via producten en diensten ongeoorloofd toegang te verkrijgen tot delen van de technische infrastructuur van een organisatie die gebruik maakt van deze producten of diensten. Deze toegang kan misbruikt worden voor spionage- en/of sabotagedoeleinden met gevolgen zoals heimelijke beïnvloeding, diefstal van gevoelige informatie, innovatieve kennis en technologieën of het verstoren van vitale infrastructuur.

Producten en diensten bereiken Nederlandse organisaties inmiddels vanuit de hele wereld. Als de inzet van deze producten en diensten bijvoorbeeld leidt tot een incident binnen organisaties die vitale processen ondersteunen dan raakt dat niet alleen de organisatie zelf, maar kan ook de nationale veiligheid van Nederland geraakt worden. Het inventariseren en beheersen van supply chain risico's is in die gevallen van groot belang voor het digitaal veilig functioneren van zowel organisaties als de Nederlandse samenleving.

Aan de slag: maak supply chain risico's voor producten en diensten afkomstig uit landen met een offensief cyberprogramma inzichtelijk

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD), Chief Information Office-Rijk (CIO Rijk), het Nationaal Cyber Security Centrum (NCSC) en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) brengen deze gezamenlijke publicatie uit om organisaties bewust te maken van supply chain risico's als gevolg van de inzet van producten en diensten afkomstig uit landen met een offensief cyberprogramma.

Deze handreiking biedt concrete handvatten voor:
- Het inventariseren van mogelijke supply chain risico's met behulp van de Cybercheck[4];
- Het uitvoeren van een aanvullende risicoanalyse om mogelijke supply chain risico's te beheersen. Dit wordt toegelicht aan de hand van een fictief voorbeeld.[5]

De resultaten uit de aanvullende risicoanalyse hebben betrekking op een specifiek supply chain scenario en vormen een aanvulling op het bredere en bestaande risicomanagementproces van jouw organisatie. Als jouw organisatie niet over een risicomanagementproces beschikt, dan adviseren we om hier eerst een proces voor in te richten.[6]

Let op! Deze handreiking geeft geen advies met betrekking tot de vraag of producten en diensten wel of niet ingezet zouden moeten worden binnen jouw organisatie. Het management van jouw organisatie is zelf eindverantwoordelijk voor het nemen van een besluit over de inzet van de betreffende producten en diensten uit landen met een offensief cyberprogramma. De Cybercheck in deze handreiking is bedoeld als een hulpmiddel en biedt jouw organisatie een structuur voor het inventariseren van mogelijke risico's die betrekking hebben op een specifiek supply chain scenario.

1 De Cybercheck

De Cybercheck is een hulpmiddel om te inventariseren of de inzet van een bepaald product of dienst afkomstig uit een land met een offensief cyberprogramma mogelijk tot een verhoogd beveiligingsrisico leidt en daarmee aanleiding geeft om een aanvullende risicoanalyse uit te voeren.
Dit hoofdstuk licht toe waarvoor en hoe je de Cybercheck binnen jouw organisatie kunt gebruiken, en geeft een overzicht van de belangrijkste begrippen en termen om de vragen in de Cybercheck te kunnen beantwoorden.

Wat is de toegevoegde waarde van de Cybercheck voor jouw organisatie?

De vragen in de Cybercheck zijn opgesteld op basis van een aantal technologie-lagen, de zogeheten *technology stack*. Deze lagen bestaan in deze handreiking uit de software, het besturingssysteem (OS), de firmware en fysieke hardware. Landen met een offensief cyberprogramma kunnen via de supply chain op één of meerdere van deze lagen misbruik maken van de digitale componenten waar producten of diensten uit bestaan. Door voor elk van deze lagen een aantal vragen te beantwoorden, kan doelgericht onderzocht worden of het mogelijk is om de technologie op deze laag te misbruiken.

Welke producten en diensten kies je voor de Cybercheck?

Deze handreiking is geschreven voor organisaties die over een of meerdere TBB-NV beschikken. Met behulp van een risicomanagementproces heeft jouw organisatie doorgaans al vastgesteld om welke belangen dit gaat of kunnen deze belangen snel inzichtelijk gemaakt worden.

De TBB's vormen het startpunt om specifieke producten en diensten te selecteren voor de Cybercheck. Bepaal van welke producten en/of diensten deze belangen momenteel afhankelijk zijn, dan wel zelf een TBB vormen omdat deze bijvoorbeeld altijd beschikbaar moeten blijven. Hierbij geldt het advies om producten en diensten die een grotere rol spelen ten aanzien van het vastgestelde TBB te prioriteren.

De producten en diensten die uit deze analyse volgen vormen in eerste instantie het uitgangspunt voor de Cybercheck in deze handreiking. Denk hierbij bijvoorbeeld aan een bedrijfskritieke dienst voor het verwerken van gevoelige informatie of operationele technologie die productieprocessen ondersteunt, zoals een Programmable Logic Controller (PLC) of Human Machine Interface (HMI) in OT-omgevingen.

Wie voert de Cybercheck uit?

De Cybercheck is bedoeld voor personen binnen jouw organisatie die een rol hebben bij het beheersen van digitale risico's. Het eigenaarschap van deze risico's ligt bij het management (bijvoorbeeld de proces-eigenaar). Het management is eindverantwoordelijk (accountable). Het management wordt hierbij doorgaans ondersteund door de Chief Information Security Officer (CISO) (verantwoordelijk voor de uitvoering: responsible). De CISO kan ook zorgen dat een vertrouwde partner deze risico's inzichtelijk maakt. Deze uitvoerder hoeft geen inhoudelijk expert te zijn, maar moet het primaire proces goed kennen en moet weten bij welke personen de juiste informatie opgehaald kan worden om de vragen in de Cybercheck te kunnen beantwoorden. Het gaat hierbij bijvoorbeeld om het intern bevragen van inhoudelijk deskundigen, maar ook om externe leveranciers van het betreffende product of dienst.

Wanneer gebruik je de Cybercheck?

De Cybercheck kan zowel voor producten en diensten die al in gebruik zijn, als voor producten en diensten waarvan wordt overwogen die te gaan inkopen uitgevoerd worden.[7] Voor iedere aanschaf van nieuwe producten of diensten adviseren we om ruim van tevoren de Cybercheck uit te voeren. Zo kan er tijdig een inkoopbeslissing genomen worden. Het is van belang om een zo goed mogelijk beeld te krijgen en houden van de afkomst van partijen in de supply chain van deze producten en diensten. Hierbij kunnen veranderingen in overnames of nieuwe eigendomsconstructies voor jouw organisatie een aanleiding vormen om de Cybercheck uit te voeren.[8]

Voor de Rijksoverheid geldt het staande kabinetsbeleid dat risico's ten aanzien van bijvoorbeeld spionage, beïnvloeding of sabotage door statelijke actoren bij digitale producten of diensten op case-by-case-basis worden beoordeeld aan de hand van de zogenaamde C2000-criteria.[9] De Cybercheck kan door organisaties die deel uitmaken van de Rijksoverheid worden betrokken bij de beoordeling die zij aan de hand van de C2000-criteria al moeten uitvoeren.

Aan de slag met de Cybercheck

We adviseren om de Cybercheck aan de hand van de volgende stappen te doorlopen:

Selecteer producten en/of diensten voor de Cybercheck

Bepaal vooraf de reikwijdte van deze producten en diensten

Voer de Cybercheck uit en beantwoord de vragen

Voer bij een 'ja' in de Cybercheck een aanvullende risicoanalyse uit

1. Selecteer producten en/of diensten voor de Cybercheck[10]
2. Bepaal vooraf de reikwijdte van deze producten en diensten om in de Cybercheck te toetsen[11]
3. Voer de Cybercheck uit en beantwoord de vragen[12]
4. Voer bij een 'ja' in de Cybercheck een aanvullende risicoanalyse uit

Hieronder worden de belangrijkste begrippen en termen in de Cybercheck toegelicht.

Wat is een product of dienst?

Met een product wordt in deze handreiking het geheel aan fysieke en digitale componenten bedoeld. Zo bestaat een smartphone bijvoorbeeld uit fysieke hardware, maar ook uit firmware, een besturingssysteem (OS) en software in de vorm van applicaties. Een dienst voorziet in een specifieke behoeftestelling van de organisatie waarbij de betreffende dienstverlening van meerdere producten gebruik kan maken. Voorbeelden van diensten zijn antivirusoplossingen of identiteits- en toegangsbeheeroplossingen.

In deze handreiking wordt met een product niet alleen een fysiek product bedoeld waar de gebruiker direct interactie mee heeft, maar ook de digitale omgeving waarmee het product in verbinding staat. Een voorbeeld hiervan is een bewakingscamera. Deze bestaat uit de fysieke bewakingscamera zelf, maar is ook gekoppeld aan een cloudomgeving waar de camera de bewakingsbeelden naar verzendt. In dit voorbeeld maakt de cloudomgeving dus ook onderdeel uit van het product en moet deze omgeving worden meegenomen bij het beantwoorden van de vragen in de Cybercheck.

Wanneer een dienst wordt onderzocht, moet worden vastgesteld van welke onderliggende producten of diensten de dienst gebruik maakt. Deze producten en diensten zijn ook onderdeel van de dienst en daarmee relevant voor het beantwoorden van de vragen in de Cybercheck. Het is aan de organisatie zelf hoe diepgaand zij de supply chain wil en kan onderzoeken. Zo kunnen componenten uit meerdere componenten bestaan en kunnen diensten ook weer uit meerdere diensten bestaan waarvoor producten gebruikt worden.

Software

Software is het geheel van programma's dat computers of andere apparatuur een taak kan laten vervullen. Software kan vele vormen aannemen. Denk hierbij aan de applicaties op je telefoon, kantoorautomatisering zoals softwarepakketten voor boekhouding en voorraadsystemen of games.[13]

Het OS

Het Operating System (OS), of besturingssysteem in het Nederlands, is de laag tussen de applicaties en de firmware die de hardware aanstuurt. Het besturingssysteem wordt na het opstarten in het geheugen geladen. Bekende voorbeelden van een OS zijn Microsoft Windows, Android, iOS, Linux en UNIX. Ook uitbreidingen van een besturingssysteem, zoals Ubuntu (voor Linux) of One UI voor Android, vallen onder de definitie OS.

Firmware

Firmware is specifieke software die in de hardware geprogrammeerd is en het besturingssysteem faciliteert bij de aansturing van hardware. De firmware zorgt ervoor dat de hardware bepaalde basisfuncties kan uit voeren, zoals opstarten en afsluiten. Een voorbeeld van firmware is het Basic Input Output System (BIOS).

Hardware

Hardware duidt op de fysieke componenten die onderdeel zijn van een digitaal product. Hardware kan zowel in IT- als OT-omgevingen ingezet worden. Voorbeelden van hardware zijn: Random Access Memory (RAM), Central Processing Unit (CPU), Solid State Drive (SSD), een Printed Circuit Board (PCB) of een Programmable Logic Controller (PLC). Maar ook printers, servers en netwerkapparatuur vallen onder hardware.

Ontwikkeling

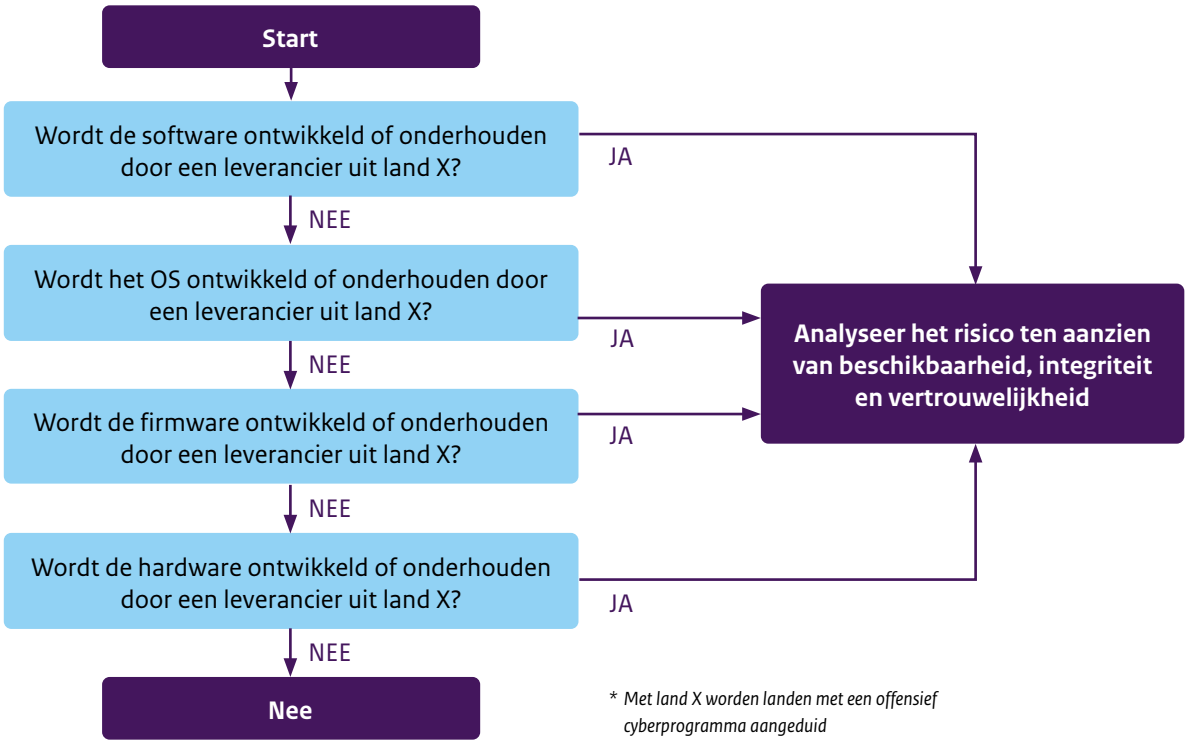
Voordat de gebruiker producten en diensten daadwerkelijk kan inzetten moeten deze eerst geproduceerd en/of ontwikkeld worden. In het geval van de software, het OS en de firmware gebeurt dit doorgaans door middel van het ontwerpen en schrijven van de programma-code. Tijdens het ontwikkelen van de code kunnen er bewust (of onbewust) fouten worden gemaakt of aangebracht die een kwaadwillende actor kan misbruiken. In het geval van hardware worden componenten fysiek in fabrieken geproduceerd, waardoor het mogelijk is om tijdens de productie bewust digitale achterdeuren in het product aan te brengen die op een later moment misbruikt kunnen worden.

Onderhoud

Nadat een product of dienst is opgeleverd, moet deze ook onderhouden worden. In het geval van software, het OS en firmware vindt onderhoud plaats door middel van updates. Een update introduceert vaak nieuwe of verbeterde functionaliteiten. Ook worden eventuele kwetsbaarheden als gevolg van fouten in de code verholpen. Kwaadwillende actoren kunnen deze updates echter ook misbruiken om (nieuwe) kwetsbaarheden te introduceren. Een bekend voorbeeld is het incident dat zich heeft voorgedaan bij een product van het bedrijf SolarWinds.[14]

In het geval van hardware en firmware is het soms nodig om fysiek onderhoud uit te voeren. In sommige gevallen kan een beheerder van de organisatie dit zelf doen, maar vaak wordt het onderhoud uitbesteed aan de leverancier van de hardware. Kwaadwillende actoren kunnen deze fysieke toegang misbruiken door de leverancier kwetsbaarheden aan te laten brengen.

De Cybercheck



* *Met land X worden landen met een offensief cyberprogramma aangeduid*

De Cybercheck in de praktijk: het voorbeeld van TechnologyS

Het Nederlandse bedrijf TechnologyS is producent en leverancier van hoogwaardige en innovatieve digitale componenten. Deze componenten zijn uniek in hun soort en maken TechnologyS een wereldwijde marktleider. TechnologyS levert daarmee een belangrijke bijdrage aan het verdienvermogen van de Nederlandse economie. Deze bijdrage bestaat niet alleen uit de directe omzet, maar ook uit een indirecte bijdrage in de vorm van werkgelegenheid, kennisontwikkeling en digitale onafhankelijkheid van Nederland. In het geval van een cyberincident zou daarom niet alleen TechnologyS zelf, maar ook de economische en daarmee nationale veiligheid van Nederland geraakt kunnen worden.

TechnologyS beschikt over een risicomanagementproces waarin de belangrijkste TBB's beschreven zijn. Hoewel TechnologyS over meerdere TBB's beschikt, is met name één belang als meest kritiek aangemerkt: het behoud van het intellectueel eigendom van de organisatie. TechnologyS is door jarenlange investeringen in het ontwikkelen van hoogwaardige en innovatieve componenten marktleider geworden. Momenteel is het bedrijf wereldwijd de enige die deze componenten kan maken, waardoor de marktpositie van TechnologyS (en indirect die van Nederland) afhankelijk is van het unieke intellectueel eigendom van het bedrijf. Het beschermen van dit intellectueel eigendom heeft voor het management en de CISO van TechnologyS dan ook de hoogste prioriteit.

TechnologyS denkt na over de aanschaf van nieuwe laptops voor bestuurders. De risico's rondom de inzet van producten en diensten uit landen met een offensief programma zijn de afgelopen tijd steeds vaker in de media benoemd. Dit zet de CISO van TechnologyS aan het denken. Is er in eerdere risicoanalyses ook rekening gehouden met het specifieke supply chain scenario waarin landen met een offensief cyberprogramma via producten of diensten mogelijk ongeoorloofd toegang kunnen verkrijgen tot de technische infrastructuur van de organisatie? Dit roept de vraag bij de CISO op of de geplande aanschaf van laptops mogelijk beveiligingsrisico's met zich meebrengt ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van het intellectueel eigendom.

De CISO besluit om met behulp van de Cybercheck te inventariseren of de aanschaf van deze laptops een mogelijk risico vormt:

Wordt de software ontwikkeld of onderhouden door een leverancier uit land X?	De CISO vraagt de interne IT-afdeling en inhoudelijk deskundigen om hulp en neemt contact op met een aantal externe leveranciers die specifieke softwareoplossingen voor TechnologyS hebben ontwikkeld. De CISO vraagt de leverancier om inzichtelijk te maken op basis van welke software deze oplossingen zijn gebouwd en door wie deze onderhouden wordt. Uit deze analyse blijkt dat de software die op de laptop geïnstalleerd zou worden, niet ontwikkeld of onderhouden wordt door een leverancier uit een land met een offensief cyberprogramma.	**NEE**
Wordt het OS ontwikkeld of onderhouden door een leverancier uit land X?	Voor de aanschaf van de laptops kan gekozen worden voor een type OS waarvan bekend is dat deze niet ontwikkeld of onderhouden wordt door een leverancier uit een land met een offensief cyberprogramma.	**NEE**
Wordt de firmware ontwikkeld of onderhouden door een leverancier uit land X?	De CISO stelt deze vraag aan de interne IT-afdeling en inhoudelijk deskundigen. Zij onderzoeken met behulp van device management tooling welke firmware versie op de laptops gebruikt zou worden en door welke leverancier deze ontwikkeld wordt. Hieruit wordt duidelijk dat de firmware niet ontwikkeld of onderhouden wordt door een leverancier uit een land met een offensief cyberprogramma.	**NEE**
Wordt de hardware ontwikkeld of onderhouden door een leverancier uit land X?	De CISO treedt in contact met de potentiële leverancier via de inkoopafdeling van TechnologyS. Hieruit blijkt dat de hardware in de laptops en bijbehorende drivers ontwikkeld worden door een leverancier uit een land met een offensief cyberprogramma.	**JA**

Uit de bovenstaande inventarisatie volgt dat de geplande aanschaf van nieuwe laptops mogelijk tot een verhoogd beveiligingsrisico voor het intellectueel eigendom leidt. De CISO besluit om met behulp van een aanvullende risicoanalyse verder onderzoek te doen.

2 Handelingsperspectief voor een aanvullende risicoanalyse

Als uit de Cybercheck volgt dat de inzet van een product of dienst mogelijk tot een verhoogd beveiligingsrisico leidt, dan biedt een aanvullende risicoanalyse de mogelijkheid om deze risico's gerichter te onderzoeken. Het handelingsperspectief in dit hoofdstuk biedt handvatten om jouw organisatie te ondersteunen bij het uitvoeren van een aanvullende risicoanalyse.

We adviseren om deze aanvullende risicoanalyse uit te voeren op basis van de onderdelen 'dreiging', 'te beschermen belangen' en 'weerbaarheid'.[15] De informatie in de inleiding van deze handreiking vormt een basis voor het onderdeel 'dreiging'.[16] Met behulp van een risicomanagementproces heeft jouw organisatie doorgaans al inzichtelijk gemaakt wat de belangrijkste TBB's-NV zijn. De onderdelen 'dreiging' en 'te beschermen belangen' vormen vervolgens de basis om het onderdeel 'weerbaarheid' te onderzoeken.

Door een aantal aannemelijke supply chain aanvalsscenario's op te stellen ontstaat er houvast om te onderzoeken of, en in welke mate, jouw organisatie weerbaar is tegen specifieke supply chain risico's als gevolg van de inzet van bepaalde producten en diensten.[17] Hierbij kan gebruik worden gemaakt van voorbeelden van supply chain aanvallen die in het verleden hebben plaatsgevonden. Denk bijvoorbeeld aan de incidenten die zich hebben voorgedaan bij SolarWinds, RSA en MeDoc. Het is belangrijk om de voorbeelden en handvatten in deze handreiking naar de specifieke context van jouw eigen organisatie te vertalen om de scenario's aannemelijk en passend te maken.[18]

Met behulp van de uitkomsten van het onderdeel 'weerbaarheid' kan er beoordeeld worden of er sprake van een verhoogd beveiligingsrisico is en zo ja, wat in dat geval de potentiële impact van dit risico op de TBB's van de organisatie is. Het inzichtelijk maken en beoordelen van deze risico's is een noodzakelijke stap voorafgaand aan het kiezen van passende beveiligingsmaatregelen.[19]

Het opstellen van supply chain aanvalsscenario's

Een belangrijke overweging: Aanvallers kiezen de weg van de minste weerstand

Bij het opstellen van aanvalsscenario's adviseren we om er rekening mee te houden dat misbruik van de supply chain door een land met een offensief cyberprogramma in de meeste gevallen een zwaarder aanvalsmiddel met een hoger afbreukrisico zal vormen. Zo bestaan er ook meer laagdrempelige digitale middelen om hetzelfde doel te bereiken. Denk hierbij aan het versturen van een spearphishing e-mail of het misbruiken van een (bekende) kwetsbaarheid of configuratiefout.[20] Deze aanvalstechnieken hebben doorgaans een lager afbreukrisico, omdat deze technieken op afstand of via het internet uitgevoerd kunnen worden en het hierdoor moeilijker maken om te achterhalen wie de aanval heeft uitgevoerd.[21]

Denk aan een situatie waarbij een aanvaller heeft ontdekt dat bepaalde software binnen jouw organisatie een kritieke kwetsbaarheid bevat die relatief eenvoudig op afstand misbruikt kan worden. Dit vormt een laagdrempelige manier om de organisatie binnen te dringen. Een aanval op de supply chain via een leverancier om hetzelfde doel te bereiken zou in dit voorbeeld een hogere inspanning vergen.

We adviseren daarom om aanvalspaden te kiezen die in het geval van jouw organisatie het meest aannemelijk zijn.[22] Het is bijvoorbeeld mogelijk dat je met behulp van de bovenstaande overweging al tijdens de aanvullende risicoanalyse tot de conclusie komt dat een gerichte supply chain aanval in het geval van jouw organisatie niet het grootste risico vormt.

Een hulpmiddel: De Cyber Kill Chain

Voor het opstellen van aanvalsscenario's vormt de Cyber Kill Chain (CKC) een praktisch hulpmiddel.[23] Dit model beschrijft de fasen die aanvallers kunnen doorlopen om hun doel te bereiken. Deze fasen beschrijven: hoe een aanvaller de organisatie binnen probeert te dringen *(in)*, op welke manier deze zich permanente toegang verschaft en digitaal door de organisatie heen beweegt *(through)* en op welke manier de aanvaller zijn doelen bereikt *(out)*.[24] De Cyber Kill Chain biedt houvast bij het opstellen van aanvalsscenario's waarmee ook specifieke supply chain aanvalsscenario's uitgewerkt kunnen worden.

Een overzicht: voorbeelden van supply chain aanvalsscenario's

Het onderstaande overzicht geeft voorbeelden van supply chain aanvalsscenario's die jouw organisatie kan gebruiken bij het opstellen van aanvalsscenario's. Dit overzicht is geen volledige weergave van alle mogelijke scenario's, maar geeft een zo breed mogelijk beeld van de verschillende supply chain aanvals-technieken die landen met een offensief cyberprogramma kunnen inzetten.[25]

Voor elk van de aanvalsscenario's wordt aangegeven of dit in mogelijke beveiligingsrisico's voor de beschikbaarheid, integriteit en vertrouwelijkheid resulteert. Ook is er een onderverdeling gemaakt in de verschillende aanvalsfasen van *'in'*, *'through'* en *'out'* zoals hierboven omschreven.

Voorbeeld aanvalsscenario	Fase	Beschik-baarheid	Integriteit	Vertrouwe-lijkheid
1. Bewust geplaatste backdoor of kwetsbaarheid	In	√	√	√
2. Kwaadaardige update van software	In	√	√	√
3. Insider threat via onderhoudsmonteur	In	√	√	√
4. Misbruik van een product of dienst voor toegang tot een ander product of dienst	Through	√	√	√
5. Spionage op data die standaard naar de leverancier verzonden wordt	Out	-	-	√
6. Heimelijke beïnvloeding van het functioneren van een product of dienst	Out	-	√	-
7. Sabotage van een product of dienst	Out	√	-	-

De *'in'* aanvalsfase

In de onderstaande scenario's proberen landen met een offensief cyberprogramma via producten of diensten oneigenlijke initiële toegang te verkrijgen tot (delen van) de technische infrastructuur van een organisatie.

1. Een bewust geplaatste backdoor of kwetsbaarheid

Landen met een offensief cyberprogramma kunnen een digitale achterdeur, ook wel backdoor genoemd, (laten) inbouwen in de hardware of software van een product of dienst.[26] Het is ook mogelijk om bewust een kwetsbaarheid in te (laten) bouwen die als een backdoor werkt. Met behulp van deze backdoor kunnen landen met een offensief cyberprogramma oneigenlijke toegang tot delen van de technische infrastructuur verkrijgen en hebben zij ook directe controle over het product of dienst. Dit biedt bijvoorbeeld de mogelijk-heid om de data die door het product of dienst verwerkt wordt in te zien. Daarnaast kan deze toegang ook misbruikt worden om de werking van het product of dienst te saboteren (zie ook scenario 6 en 7) of vormt het product of dienst een zogeheten 'stepping stone' voor netwerken of apparaten die hieraan gekoppeld zijn (zie ook scenario 4).

2. Een kwaadaardige update van software
Landen met een offensief cyberprogramma kunnen via vereiste updates invloed uitoefenen op een product of dienst. Door een kwaadaardige update te installeren of het bewust verzwakken van de gebruikte cryptografie, kan er bijvoorbeeld een backdoor of kwetsbaarheid in een bepaald product of dienst aangebracht worden (zie ook scenario 1).

3. Insider threat via onderhoudsmonteur
Voor sommige producten en diensten is het nodig om gespecialiseerd onderhoudspersoneel in te huren. Zo wordt het onderhoudspersoneel doorgaans ingehuurd via de leverancier waarbij ook het product of dienst is aangeschaft. Dit onderhoudspersoneel beschikt in de meeste gevallen over ruime toegang tot het product en in sommige gevallen ook over toegang tot datacentra of gekoppelde producten. Landen met een offensief cyberprogramma kunnen bijvoorbeeld de leverancier uit het betreffende land verplichten om de onderhoudsmonteur in dienst een backdoor te laten plaatsen.[27]

De '*through*' aanvalsfase

In het onderstaande scenario nestelen landen met een offensief cyberprogramma zich dieper in de technische infrastructuur van de organisatie nadat ze in de 'in' aanvalsfase toegang hebben verkregen. Het doel van deze fase is om te bepalen welke onderdelen binnen de technische infrastructuur nog meer kunnen misbruikt kunnen worden om zo de achterliggende doelen te realiseren.

4. Misbruik van een product of dienst om toegang tot een ander product of dienst te verkrijgen
Een product of dienst moet in de meeste gevallen in staat zijn om verbinding te kunnen maken met andere producten of diensten van de organisatie. Denk hierbij bijvoorbeeld aan een mobiele telefoon die verbonden is met de mailservers van een organisatie. Wanneer landen met een offensief cyberprogramma initiële toegang kunnen verkrijgen via een product of dienst (zie ook scenario 1 t/m 3), kunnen deze verbindingen vervolgens misbruikt worden om toegang tot andere producten of diensten te verkrijgen.

De '*out*' aanvalsfase

De onderstaande scenario's zijn voorbeelden waarop landen met een offensief cyberprogramma via producten of diensten hun achterliggende doelen kunnen realiseren:

5. Spionage op data die standaard naar de leverancier verzonden wordt
Bijna alle moderne producten en diensten versturen data naar de leverancier. Deze data kan variëren van gegevens uit sensoren en locatiegegevens tot grote hoeveelheden gebruiksgegevens. Al deze gegevens worden op de servers van de leverancier opgeslagen. Landen met een offensief cyberprogramma kunnen heimelijk of middels wettelijke middelen toegang verkrijgen tot deze data.

6. Het heimelijk beïnvloeden van het functioneren van een product of dienst
Landen met een offensief cyberprogramma kunnen het functioneren van een product of dienst heimelijk beïnvloeden waardoor een product of dienst ongemerkt bepaalde functies niet meer (volledig) uitvoert of juist extra functies uitvoert. Zo kan bijvoorbeeld een sensor gemanipuleerd worden om foutieve data te genereren. Ook kan er bewust voorkomen worden dat berichten of e-mails bij de organisatie aankomen.

7. Het saboteren van een product of dienst
Landen met een offensief cyberprogramma kunnen na het verkrijgen van toegang bewust het functioneren van een product of dienst verstoren. Denk hierbij bijvoorbeeld aan het manipuleren van de toegang tot stroom voor een product of het op afstand uitschakelen van het product of dienst. Ook kunnen landen met een offensief cyberprogramma een leverancier verplichten om bepaalde onderdelen of ondersteunende producten en diensten niet meer te leveren. Het gevolg hiervan is dat bepaalde producten of diensten niet langer ondersteund kunnen worden of zelfs in zijn geheel niet meer functioneren.

3 De uitkomsten: hoe nu verder?

Een belangrijke laatste stap na het uitvoeren van een aanvullende risicoanalyse, is om de bevindingen ook vast te leggen en terug te koppelen aan de personen binnen jouw organisatie die eindverantwoordelijk zijn voor het beheersen van digitale risico's als gevolg van de inzet van producten en diensten uit landen met een offensief cyberprogramma.

Wanneer de uitkomsten van de aanvullende risicoanalyse niet in het brede risicomanagementproces van de organisatie wordt opgenomen, kan er door de eindverantwoordelijke(n) ook niet gestuurd worden op het beheersen van deze risico's of kunnen deze risico's niet in samenhang beoordeeld worden om te komen tot een onderbouwd besluit over de inzet van een product of dienst.

Dit hoofdstuk sluit af met een vervolg op het voorbeeld van TechnologyS. Deze verdere uitwerking licht de handvatten uit het vorige hoofdstuk toe en laat zien op welke manier de resultaten van de aanvullende risicoanalyse gebruikt kunnen worden om verdere stappen ten aanzien van risicobeheersing te zetten.

Het voorbeeld van TechnologyS: aan de slag met een aanvullende risicoanalyse

De CISO van TechnologyS heeft met behulp van de Cybercheck besloten om een aanvullende risicoanalyse uit te voeren. Dit biedt houvast om mogelijke beveiligingsrisico's ten aanzien van de aan te schaffen laptops voor bestuurders gerichter te onderzoeken.

De TBB's zijn in kaart gebracht en het management heeft vastgesteld dat het belangrijkste TBB het intellectueel eigendom is. Hierbij is ook uitgewerkt wat de mogelijke impact voor TechnologyS is als de vertrouwelijkheid van het intellectueel eigendom aangetast wordt. Uit deze TBB-analyse blijkt dat dit niet alleen TechnologyS zelf zou raken, maar ook de nationale veiligheid van Nederland. De CISO heeft op basis van verschillende dreigingspublicaties geconcludeerd dat TechnologyS hoogwaardige kennis en innovatie in huis heeft. Daarmee zou de organisatie een interessant doelwit kunnen vormen voor landen met een offensief cyberprogramma die de motivatie en middelen hebben om deze hoogwaardige en innovatieve kennis middels spionage vergaren.

De CISO besluit om een brede bijeenkomst met de ICT-afdeling en interne securityspecialisten te organiseren om samen de weerbaarheid met behulp van aanvalsscenario's te onderzoeken.

De 'in' aanvalsfase
Voor de 'in' aanvalsfase stellen de CISO en zijn team een aannemelijk aanvalsscenario op. In dit geval nemen ze de aan te schaffen laptops als uitgangspunt. Het aanvalsscenario gaat er hierbij vanuit dat er een backdoor in de hardware van de laptops is gebouwd en deze initiële toegang verschaft tot de technische infrastructuur van TechnologyS.

Eén van de securityspecialisten merkt op dat het netwerk van TechnologyS meerdere externe koppelingen met het internet heeft en daarmee ook ingangen zou kunnen bieden voor aanvallers. Ook wordt het voorbeeld van een spearphishing e-mail of het op afstand misbruiken van configuratiefouten genoemd.

De CISO en zijn team wegen deze verschillende aanvalsmethoden tegen elkaar af en maken hierbij ook de huidige beveiligingsmaatregelen inzichtelijk. De conclusie die volgt is dat er verschillende basismaatregelen en aanvullende maatregelen getroffen zijn die rekening houden met aanvallen vanaf het internet en het aanvallers moeilijker maken om hier misbruik van te maken. Er is in eerdere scenario's nog geen rekening gehouden met de mogelijkheid van een backdoor in de hardware. De CISO en zijn team besluiten dat dit een aannemelijk, maar ook relevant supply chain aanvalsscenario voor TechnologyS zou kunnen zijn en besluiten om deze verder uit te werken.

De 'through' aanvalsfase
Wanneer er via een backdoor toegang verkregen wordt, dan zullen de aanvallers binnen het interne netwerk van TechnologyS op zoek gaan naar het intellectueel eigendom. TechnologyS maakt gebruik van segmentering waardoor het intellectueel eigendom binnen een afgeschermde omgeving staat die niet gekoppeld is met het internet. De CISO en zijn team denken na over mogelijke aanvalspaden vanaf de laptop naar de omgeving waar het intellectueel eigendom staat en brengen deze in kaart. Hierbij maken zij bijvoorbeeld inzichtelijk of een aanvaller voldoende rechten zou hebben om toegang tot de omgeving waar het intellectueel eigendom staat te verkrijgen, maar ook of het op zou vallen als er hogere rechten worden aangevraagd of dat lateraal bewegen door het netwerk opgemerkt zou kunnen worden. De CISO en zijn team merken op dat er beveiligingsmaatregelen zijn getroffen om aanvallers buiten het netwerk van TechnologyS te houden, maar dat er nog onvoldoende beveiligingsmaatregelen zijn getroffen om verdacht gedrag op het interne netwerk snel en effectief op te kunnen merken.

De 'out' aanvalsfase
De acties in de 'in' en 'through'-fase stellen de aanvallers in staat om toegang te verkrijgen tot de afgeschermde omgeving waar het intellectueel eigendom staat. Dit geeft hen de mogelijkheid om gevoelige data in te zien en voor eigen gewin te gebruiken. Eén van de securityspecialisten merkt op dat het inzien van de data een risico voor spionage vormt, maar dat het ook mogelijk zou zijn om de data van de afgeschermde omgeving te kopiëren naar de laptop, waardoor de data via de laptop gestolen kan worden. De CISO en zijn team maken daarom ook inzichtelijk welke beveiligingsmaatregelen ten aanzien van data-exfiltratie er momenteel zijn getroffen.

Uitkomsten en hoe nu verder?

Op basis van het voorstelbare aanvalsscenario concluderen de CISO en zijn team dat er een beveiligingsrisico voor het intellectueel eigendom van TechnologyS bestaat als gevolg van de aan te schaffen laptops. De CISO en zijn team stellen een rapport met bevindingen en aanbevelingen op. Deze bevindingen en aanbevelingen moeten ook in het bredere risicomanagementproces worden opgenomen om tot een zo volledig mogelijk beeld van de belangrijkste bedrijfsrisico's voor TechnologyS te komen.

In het rapport worden de volgende aanbevelingen gedaan:
- Een beveiligingsmaatregel die TechnologyS meer zekerheid zou kunnen bieden is om een preferred supplier te selecteren die extra garanties ten opzichte van de integriteit van de hardware kan bieden. Ook is het mogelijk om de integriteit van de hardware door securitytesters te laten onderzoeken voordat de laptops in gebruik genomen worden;
- TechnologyS zou ook detectie en – response oplossingen kunnen overwegen om verdacht gedrag op het interne netwerk en de laptops te kunnen detecteren en te kunnen stoppen;
- De rechten tot de afgeschermde omgeving zouden nog verder beperkt kunnen worden;
- TechnologyS zou aanvullende oplossingen kunnen implementeren om data-exfiltratie te voorkomen.

Het rapport met aanbevelingen wordt vervolgens aan de eindverantwoordelijke(n) gepresenteerd. Het management van TechnologyS kan op basis van dit rapport een onderbouwd besluit over de aanschaf van de laptops nemen. Hierbij wordt ook de mate van risicoacceptatie bepaald en worden er op basis van het rapport aanvullende beveiligingsmaatregelen gekozen die passen bij de bredere organisatiedoelen van TechnologyS.

Eindnoten

[1] Met een product wordt in deze handreiking het geheel aan digitale componenten aangeduid. Zo bestaat een smartphone bijvoorbeeld uit fysieke hardware, maar ook firmware, een bepaald type Operating System (OS) en software in de vorm van applicaties. Een dienst voorziet in een specifieke behoeftestelling van de organisatie, waarbij de betreffende dienstverlening van meerdere producten gebruik kan maken.

[2] Onder de 'supply chain' verstaan we alle leveranciers van componenten, (deel)producten en diensten die onderdeel uitmaken van de toeleveringsketen ten behoeve van het ontwikkelen of onderhouden van een product of dienst

[3] AIVD-publicatie 'Offensief cyberprogramma een ideaal businessmodel voor staten' | Publicatie | AIVD

[4] Het gaat hierbij om de mogelijke risico's die voortkomen uit het gebruik van producten en diensten waarbij leveranciers afkomstig uit landen met een offensief cyberprogramma een rol spelen in de supply chain van deze producten en diensten

[5] We adviseren om een risicoanalyse uit te voeren op basis van de onderdelen 'dreiging', 'te beschermen belangen' en 'weerbaarheid'. Zie pagina 12

[6] Door risico's organisatiebreed en in samenhang te beoordelen kunnen beveiligingskeuzes gemaakt worden die passen bij de organisatiedoelstellingen en die positief bijdragen aan de gewenste weerbaarheid. Zie voor meer informatie de factsheet "Risico's beheersen: de waarde van informatie als uitgangspunt" Factsheet Risico's beheersen: de waarde van informatie als uitgangspunt. | Factsheet | Nationaal Cyber Security Centrum (ncsc.nl) of NEN-ISO 31000:2018 – Richtlijn voor Risicomanagement

[7] We adviseren voor het opstarten van een inkoopproces ter aanvulling op de cybercheck ook "De Toolbox veilig inkopen 2024" te raadplegen. De Toolbox veilig inkopen is door de NCTV, EZK en BZK ontwikkeld om specifieke risico's voor de nationale veiligheid binnen inkoop-en aanbestedingstrajecten te signaleren: Toolbox veilig inkopen (2024) | Economische veiligheid | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl) .
Rijksoverheidsorganisaties kunnen de ICO wizard gebruiken om een set van informatiebeveiligingseisen samen te stellen voor inkoop/aanbestedingen en contracten. Organisaties buiten de Rijksoverheid kunnen deze tool ter inspiratie gebruiken: ICO Wizard - bio-overheid

[8] Overnames of nieuwe eigendomsconstructies vallen buiten de reikwijdte van deze handreiking, maar moeten wel in het bredere risicomanagementproces opgenomen en meegewogen worden om tot een zo volledig mogelijk en onderbouwd besluit te komen rondom de inzet van producten en diensten uit landen met een offensief cyberprogramma. Zie voor meer informatie Wet veiligheidstoets investeringen, fusies en overnames (35.880); Memorie van toelichting (TK, 3) - Eerste Kamer der Staten-Generaal. Zie voor verdere vragen over Economische veiligheid ook het EV-loket: Stel uw vraag | Ondernemersloket Economische Veiligheid

[9] De C2000-criteria zijn:

1. Is de partij die de dienst of product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of product levert afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

3a. Krijgt de partij die de dienst of product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen?

3b. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

[10] Zie voor meer informatie de paragraaf 'welke producten en diensten kies je voor de Cybercheck' om te komen tot een eerste selectie

[11] Zie voor meer informatie de paragraaf 'wat is een product of dienst'?

[12] Zie 'Wie voert de Cybercheck uit' voor meer informatie

[13] Voor meer informatie over het beveiligen van de software supply chain zie ook: Factsheet Open Source Security | Factsheet | Nationaal Cyber Security Centrum (ncsc.nl)

[14] Backdoor in SolarWinds Orion | Nieuwsbericht | Nationaal Cyber Security Centrum (ncsc.nl)

[15] De volgorde van de onderdelen 'dreiging' en 'te beschermen belangen' kan naar eigen inzicht toegepast en uitgevoerd worden. We adviseren echter om in alle gevallen het onderdeel 'weerbaarheid' als laatst te onderzoeken, omdat de onderdelen 'dreiging' en 'te beschermen belangen' hier een belangrijke basis voor vormen

[16] Zie voor meer informatie Cybersecuritybeeld Nederland 2022 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)

[17] Zie voor meer informatie Analysetechnieken en cybersecurity | Expertblogs | Nationaal Cyber Security Centrum (ncsc.nl)

[18] Voor de verschillende onderdelen van een risicoanalyse zullen ook verschillende stakeholders binnen jouw organisatie betrokken moeten worden. Denk hierbij aan het management om te bepalen wat de belangrijkste TBB's zijn, maar ook securityspecialisten die vervolgens op basis van deze TBB's kunnen helpen bij het opstellen van aannemelijke supply chain aanvalsscenario's specifiek voor jouw organisatie

[19] De risico's en keuzes voor maatregelen moeten altijd aan de risico-eigenaren voorgelegd worden (doorgaans het management). De risico-eigenaren zijn eindverantwoordelijk voor het maken van een keuze met betrekking tot het beheersen van risico's.

[20] Zie Basismaatregelen cybersecurity | Nationaal Cyber Security Centrum (ncsc.nl) voor aanvullend advies ten aanzien van basismaatregelen die jouw organisatie weerbaarder kunnen maken tegen laagdrempelige aanvalsmethoden

[21] AIVD-publicatie 'Offensief cyberprogramma een ideaal businessmodel voor staten' | Publicatie | AIVD

[22] Welke aanvalspaden voor jouw organisatie aannemelijk en relevant zijn, is afhankelijk van de huidige gekozen beveiligingsmaatregelen en de intentie, capaciteit en activiteiten van landen met een offensief cyberprogramma die in het onderdeel 'dreiging' inzichtelijk zijn gemaakt. De onderdelen 'dreiging' en 'te beschermen belangen' vormen daarom een belangrijke basis voor het onderzoeken van de weerbaarheid.

[23] Zie voor meer informatie Publicatie AIVD/MIVD: Cyberaanvallen door statelijke actoren - zeven momenten om een aanval te stoppen | Publicatie | AIVD

[24] Unified Kill Chain: Raising Resilience Against Cyber Attacks

[25] We adviseren om aanvullend het MITRE ATT&CK framework te gebruiken. Dit framework geeft een uitgebreid overzicht van mogelijke aanvalstechnieken die in de praktijk zijn waargenomen en die kunnen helpen bij het opstellen van voorstelbare aanvalsscenario's voor jouw organisatie. Ook biedt het framework bijbehorende mitigerende maatregelen. Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®.

[26] Het Cybersecurity Woordenboek definieert 'backdoor' als een manier om via een ongewone omweg in een digitaal systeem te komen. Iemand heeft die omweg vaak met opzet gemaakt, en op zo'n manier dat anderen die niet kunnen zien.

[27] Zie voor meer informatie over insider threats ook Omgaan met insider threats | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

[28] Te Beschermen Belangen (TBB) worden ook aangeduid als 'Digitale Kroonjuwelen'. Zie voor meer informatie de 'Rijksbrede Risicoanalyse Nationale Veiligheid 2022', 'Leidraad Risicobeoordeling' of 'Digitale Kroonjuwelen: gegevens, documenten en registraties van Nationaal Belang' om te beoordelen of jouw organisatie over TBB's ten aanzien van de Nationale Veiligheid beschikt. Rijksbrede Risicoanalyse Nationale Veiligheid 2022 | Rapport | Rijksoverheid.nl, https://www.rivm.nl/nationale-veiligheid of Digitale Kroonjuwelen: Gegevens, documenten en registraties van Nationaal Belang | Rapport | Rijksoverheid.nl.

[29] De AIVD en MIVD scharen onder andere China, Rusland en Iran onder landen met een dergelijk offensief cyberprogramma. AIVD-jaarverslag 2022 | Jaarverslag | AIVD, pagina 29.

Deze brochure is een uitgave van:

Algemene Inlichtingen- en Veiligheidsdienst
aivd.nl
Postbus 20010 | 2500 EA Den Haag

CIO Rijk
Postbus 20011 | 2500 EA Den Haag

Nationaal Coördinator Terrorismebestrijding en Veiligheid
nctv.nl
Postbus 20301 | 2500 EH Den Haag

Nationaal Cyber Security Centrum
ncsc.nl
Postbus 117 | 2501 CC Den Haag