Bent u zich bewust van de risico's van **cyberspionage?**

Een publicatie van de AIVD en MIVD

Bent u zich bewust van de risico's van cyberspionage?

De informatie- en communicatiesystemen van Nederlandse instellingen en bedrijven worden op grote schaal aangevallen door cyberspionnen, concluderen de Nederlandse inlichtingendiensten. Het gaat hier dan om digitale aanvallen die worden uitgevoerd door, of in opdracht van andere landen.

Twee derde van de getroffen organisaties weet niet dat ze slachtoffer zijn. In sommige gevallen zijn aanvallers daardoor jaren onontdekt aanwezig in de systemen. Slechts weinig organisaties beseffen dat ook zij een potentieel slachtoffer zijn, waardoor hun systemen en netwerken onvoldoende weerstand bieden tegen aanvallen.

Deze brochure gaat over cyberaanvallen op de Nederlandse overheid en het bedrijfsleven door buitenlandse cyberspionnen. Doel van deze aanvallen is het verkrijgen van vertrouwelijke informatie. Deze aanvallen zijn schadelijk voor de reputatie en het verdienvermogen van bedrijven en kunnen (op termijn) de militaire en geopolitieke positie van Nederland en bondgenoten aantasten.

Dit eerste deel van de brochure biedt inzicht in de wijze waarop cyberspionnen te werk gaan en basismaatregelen die u daartegen kunt nemen. Het tweede deel is bedoeld voor uw ICT-afdeling en biedt een aantal aanbevelingen om de weerbaarheid van uw organisatie tegen cyberaanvallen te vergroten.

"Twee derde van de getroffen organisaties weet niet dat ze slachtoffer zijn."

Het risico op cyberaanvallen is groot

Door de digitalisering van onze samenleving neemt het risico op cyberaanvallen toe. Aanvallen in opdracht van overheden zijn technisch geavanceerd en moeilijk te traceren. Veel organisaties zijn daardoor vaak niet op de hoogte dat zij slachtoffer zijn, totdat derde partijen, waaronder vaak inlichtingendiensten, ze waarschuwen. Hierdoor, maar ook door het grote geografische bereik en lage afbreukrisico, is cyberspionage een aantrekkelijk

middel dat afgelopen jaren enorm is gegroeid in omvang en diversiteit. Jaarlijks worden wereldwijd duizenden publieke en private organisaties aangevallen.

"Jaarlijks worden wereldwijd duizenden publieke en private organisaties aangevallen."

Het Nederlandse bedrijfsleven en de overheid zijn structureel slachtoffer

Het Nederlandse bedrijfsleven en de overheid worden structureel aangevallen. Verschillende ministeries en topsectoren zijn al getroffen, zoals defensie-toeleveranciers, hightech, chemie, energie, life sciences and health en de watersector.

De vertrouwelijke overheidsinformatie die cyberspionnen hierbij buitmaken, wordt door buitenlandse staten misbruikt om invloed uit te oefenen op andere landen. Dit kan door middel van het gebruik van gevoelige informatie over politieke besluitvorming en stellingname, de inhoud van politiek-economische plannen, militaire planning en Nederlandse agendapunten bij onderhandelingen.

Met waardevolle informatie op technisch en wetenschappelijk gebied kunnen buitenlandse staten ook hun afhankelijkheid van kennis en producten uit het buitenland verminderen. Zo verbeteren zij hun economische concurrentiepositie of geopolitieke machtspositie, bijvoorbeeld door een versnelde modernisering van hun krijgsmacht.

Schade en onrust in het Duitse parlement door cyberaanval

In 2015 werd spionagesoftware op het computernetwerk van het Duitse parlement gevonden. Parlementsleden verkeerden weken in onzekerheid. Welke gegevens werden er gestolen? Welke communicatie werd afgeluisterd en door wie? Naast politieke onrust, discussies over het internet als vitale infrastructuur en de mogelijke betrokkenheid van buitenlandse inlichtingendiensten was de materiële schade groot. Omdat de aanvallers toegang hadden verkregen tot het hele netwerk en mogelijk verschillende moeilijk vindbare achterdeurtjes hadden geïnstalleerd in hard- en software, zijn circa 20.000 computers, inclusief randapparatuur (printers, telefoons, routers en dergelijke) vervangen[1]. Dit om er zeker van te zijn dat de aanvallers zich in de toekomst niet opnieuw toegang konden verschaffen tot de vertrouwelijke informatie en communicatie van het Duitse parlement.

1 *Verfassungsschutzbericht 2015*

De gevolgen van cyberaanvallen worden vaak onderschat

Het Nederlandse bedrijfsleven en de overheid zijn zich vaak niet bewust van de omvang, duur, impact en gevolgen van cyberaanvallen. Organisaties zien de kosten voor het herstellen van de gevolgen als een acceptabel bedrijfsrisico. Men gaat ervan uit dat dit goedkoper is dan investeren in structurele preventieve maatregelen tegen cyberaanvallen.

Hierbij gaan deze organisaties voorbij aan de mogelijke (financiële) gevolgen op langere termijn: imagoschade, verlies van marktaandeel en aantasting van de concurrentiepositie. Het aantal cyberaanvallen dat de Nederlandse inlichtingendiensten zien, en de omvang van de (economische) schade, bewijzen dat spionageaanvallen een reëel risico vormen voor het Nederlandse bedrijfsleven en de overheid.

Verlies van intellectueel eigendom en investeringsgelden

Uit onderzoek is gebleken dat de kosten van het ongedaan maken van een cyberaanval kunnen oplopen van 200.000 dollar[2] tot vier miljoen dollar[3]. Dit bedrag is hoger dan het gemiddelde budget van veel bedrijven voor ICT-beveiliging. De daadwerkelijke kosten verschillen per cyberaanval en per organisatie. Voor veel bedrijven zijn het verlies van intellectueel eigendom en het tenietdoen van investeringen in Research and Development belangrijker dan de kosten voor herstel na een aanval. Feit is dat de (gemiddelde) kosten al jaren oplopen.

2 *Journal of Cybersecurity, Examining the costs and causes of cyber incidents, 25 augustus 2016.*
3 *Ponemon institute, 2016 Cost of Data Breach Study; Global Analysis, juni 2016.*

Hoe wordt u aangevallen?

Uit het onderzoek van de Nederlandse inlichtingendiensten blijkt dat cyberaanvallen vaak succesvol zijn, omdat het bedrijfsleven en de overheid niet weten hoe zij hun ICT-netwerken kunnen beschermen tegen digitale aanvallen van statelijke actoren. Een goede beveiliging en veiligheidsbewust handelen zijn daarom cruciaal om een ICT-systeem weerbaar te maken tegen cyberaanvallen.

Voor een goede beveiliging is het belangrijk om te begrijpen hoe cyberspionnen te werk gaan en welke (technische) methoden zij gebruiken. Met deze kennis kunt u het de aanvallers moeilijker maken en met een aantal basismaatregelen uw weerbaarheid tegen deze aanvallen verhogen.

Cyberaanvallen bestaan globaal uit drie fasen.

1 Initiële toegang verkrijgen.
2 Permanente toegang verzekeren.
3 Stelen van informatie of plegen van sabotage.

Cyberspionnen doorlopen tijdens de gehele aanval deze fasen steeds opnieuw, om de toegang die zij hebben uit te breiden of te herstellen. De aanvaller en het getroffen ICT-netwerk wisselen data uit, waarbij informatie kan worden gestolen en schadelijke software (malware) kan worden geïnstalleerd op uw systemen. Dit proces vergt vaak langdurige toegang tot het netwerk. Daarom doen cyberspionnen extra moeite om niet ontdekt te worden.

Fase 1

Initiële toegang verkrijgen

Cyberaanvallen zijn niet willekeurig. Buitenlandse inlichtingendiensten maken een 'boodschappenlijst' van doelwitten, afhankelijk van het doel dat de betreffende staat heeft met de gestolen informatie. Met die lijst kijken cyberspionnen hoe zij toegang kunnen krijgen tot het gekozen doelwit. Dit kan bijvoorbeeld via medewerkers, toeleveranciers of slecht beveiligde systemen.

Internet en sociale media hebben het cyberspionnen makkelijk gemaakt om kwetsbaarheden te identificeren en te benaderen. Door middel van poortscans[4], maar ook met onderzoek op Google of sociale media, kunnen aanvallers veel informatie over hun doel verzamelen. De meeste organisaties worden binnengedrongen via een nietsvermoedende

4 Het op afstand controleren of de poort naar de computer openstaat voor kwaadwillenden.

medewerker, die via persoonlijke mails ('spearfishing') verleid wordt om een bijlage te openen of een besmette website te bezoeken. *Social engineering* en spearphishing zijn de meest voorkomende aanvalsmethoden omdat ze zo succesvol zijn, maar steeds vaker zien de inlichtingendiensten geavanceerdere aanvallen op bijvoorbeeld hardware.

Fase 2 **Permanente toegang verzekeren**

Eenmaal binnen installeren aanvallers een achterdeur, die hen blijvend toegang verschaft tot het netwerk. In hun zoektocht naar relevante informatie proberen cyberspionnen hun toegang tot een binnengedrongen netwerk te verbreden. Hiertoe brengen zij alle systemen binnen een netwerk in kaart. Vervolgens gaan ze op zoek naar aanvullende gebruikersnamen en wachtwoorden om toegang te krijgen tot andere systemen of netwerksegmenten. Daarnaast installeren aanvallers vaak extra achterdeurtjes om de continuïteit van hun aanval te bevorderen. Aanvallers gaan hierbij behoedzaam te werk en proberen zich aan te passen aan de reguliere activiteit op het netwerk, om onderkenning te voorkomen.

Nadat cyberspionnen toegang hebben tot uw netwerk, installeren zij malware op de systemen. Hiermee doorzoeken zij op afstand het netwerk automatisch of handmatig op de benodigde informatie, zoals gebruikersnamen en wachtwoorden. Hiermee vergroot de aanvaller zijn gebruikersrechten binnen het netwerk, waardoor hij eenvoudiger bij de benodigde informatie kan komen. Het maximaal haalbare resultaat is om uiteindelijk de hoogste rechten te verkrijgen, zoals die van de systeembeheerder. Dit verschaft toegang tot alle informatie en systemen in het netwerk.

De aanvaller brengt het totale netwerk in kaart, besmet andere aangesloten computers, servers en apparaten zoals printers en soms zelfs telefoons of camera's en deuren. Om niet afhankelijk te zijn van de initiële toegang installeert de aanvaller nieuwe of extra ingangen ('achterdeuren') op het netwerk, waarmee hij ook na beveiligingsupdates of het offline halen van systemen nog steeds toegang heeft. Door het gebruik van tussenstations (proxy's) en encryptie is de aard van de activiteiten en de herkomst van de aanvaller moeilijk te herleiden.

Fase 3 **Stelen van informatie of plegen van sabotage**

In deze fase gaan cyberspionnen op zoek naar relevante informatie. Eenmaal gevonden, wordt deze informatie gekopieerd naar tijdelijke bestanden. Deze bestanden worden vaak versleuteld en vermomd als regulier netwerkverkeer verstuurd naar de systemen van de aanvaller, om de activiteiten en intenties van de aanvaller verborgen te houden. De gestolen informatie wordt vaak via meerdere tussenstations in diverse landen gerouteerd om de identiteit van de aanvallers af te schermen. Aanvallers wissen vervolgens deze bestanden en andere sporen, waardoor slachtoffers vaak geen idee hebben van hun aanwezigheid. Het is niet ongebruikelijk dat aanvallers zich maanden tot jaren in een netwerk nestelen.

In deze fase voeren cyberspionnen de daadwerkelijke aanval uit. Nadat permanente toegang is verkregen, kan de aanvaller gegevens verzamelen en op afstand de besmette systemen bedienen. Ook kan hij sluimerend op het systeem aanwezig blijven, om op een later moment zijn doel te realiseren.

Gestolen informatie wordt vaak versleuteld en als regulier netwerkverkeer verwerkt, om te voorkomen dat detectiesoftware deze opmerkt. Via meerdere tussenstations (servers, proxy's of satellieten) verplaatst de aanvaller de informatie naar zijn eigen systemen. Door het gebruik van dergelijke tussenstations is de dader van de cyberaanval en de gestolen informatie vaak moeilijk te achterhalen.

PlugX is een voorbeeld van malware die sinds 2012 in verschillende varianten is waargenomen bij aanvallen van cyberspionnen op onder andere (defensie)bedrijven en overheidsinstellingen. Deze malware combineert een aantal van de functionaliteiten uit fase 2 en 3[5]. PlugX fungeert als een 'Zwitsers zakmes' met verschillende componenten die op afstand worden aangestuurd en op ieder moment aan te passen zijn. Hierdoor zijn deze moeilijk te detecteren voor virusscanners.

Wat kunt u doen?

Beveiliging tegen cyberspionage is een ongelijke strijd. De kosten van goede beveiliging zijn hoog vergeleken de kosten van een aanval. Immers, een aanvaller hoeft maar één zwak punt in het netwerk te vinden, terwijl u alle zwakke punten moet vinden en afdekken. Toch is het goed mogelijk om het cyberspionnen moeilijker te maken. In vier stappen vergroot u de basisbeveiliging van uw gehele ICT-infrastructuur.

1. Identificeer uw 'kroonjuwelen'.
2. Bepaal uw dreigingsscenario's.
3. Neem maatregelen.
4. Laat uw ICT-systemen periodiek onderzoeken.

Stap 1 Identificeer uw 'kroonjuwelen'

Het is belangrijk dat u eerst in kaart brengt wat de digitale 'kroonjuwelen' in uw netwerk zijn en waar deze zich bevinden. Dit kan vertrouwelijke of gevoelige informatie zijn, maar

5 *PlugX – The Next Generation, Sophos, juni 2014.*

ook systemen met bijvoorbeeld persoonsgegevens. U weet wat de unieke meerwaarde van uw organisatie is en door welke gegevens en processen deze (mede) wordt bepaald[6]. Daarbij is het belangrijk om actuele dreigingsinformatie te verzamelen via de overheid, commerciële bronnen of branchegenoten (ISAC's). Dit is onontbeerlijk voor een adequaat zicht op relevante dreiging en daarmee ook beveiliging.

Stap 2 **Bepaal uw dreigingsscenario's**

Als u uw kroonjuwelen in kaart heeft gebracht, kunt u een aantal reële dreigingsscenario's bedenken: via welke wegen komen cyberspionnen het gemakkelijkst bij deze vertrouwelijke informatie? Dreigingsscenario's zijn voor elke organisatie uniek en zonder ICT-kennis moeilijk te bepalen. Betrek daarom uw ICT-afdeling bij het proces. Ook sectorgenoten, de overheid en commerciële partijen kunnen hierin ondersteunen.

Stap 3 **Neem maatregelen**

Aan de hand van de dreigingsscenario's kunt u tegenmaatregelen nemen.
Deze zijn op te delen in drie categorieën.

1 Preventieve maatregelen.
Deze zijn bedoeld om de kans op een succesvolle aanval op het systeem te verkleinen.
2 Detecterende maatregelen.
Deze verhogen de kans dat een aanval opgemerkt wordt, zodat u kunt reageren.
3 Impact reducerende maatregelen.
Deze beperken de effectiviteit van malware en van schade na een succesvolle aanval.

In het tweede deel van deze brochure is uitgewerkt hoe uw ICT-afdeling deze maatregelen kan implementeren.

Stap 4 **Laat uw ICT-systemen periodiek onderzoeken**

Cyberbeveiliging is een continu proces. Met de maatregelen uit de vorige stap is de weerstand van uw netwerk sterk verhoogd. Maar dat biedt geen 100% beveiliging tegen geduldige en goed uitgeruste cyberspionnen. Het is belangrijk om aanvallers een stap voor te zijn, door uw ICT-systemen periodiek te (laten) onderzoeken met een gesimuleerde aanval aan de hand van de dreigingsscenario's uit stap 2. Deze onderzoeken kunnen helpen bij het aanscherpen van processen en reacties op daadwerkelijke aanvallen. Ook is het mogelijk dat u hiermee een werkelijke aanval identificeert.

---

6 U kunt hierbij bijvoorbeeld gebruik maken van de 'Handleiding Kwetsbaarheidsonderzoek Spionage' (KWAS) op www.aivd.nl/onderwerpen/cyberdreiging/documenten/publicaties/2011/02/17/handleiding-kwetsbaarheidsonderzoek-spionage

ICT-maatregelen

Dit deel van deze brochure bestaat uit specifieke instructies voor uw ICT-afdeling of uw ICT-leverancier om deze wijzigingen door te voeren. In de onderstaande tabel zijn beveiligingsmaatregelen opgenomen. De volgorde geeft aan in welke mate de Nederlandse inlichtingendiensten de genoemde maatregelen belangrijk vinden.

De genoemde maatregelen zijn niet in het bijzonder gericht op het tegengaan van cyberspionage. Het zijn maatregelen die tot de 'standaardhygiëne' van ICT-systemen en -netwerken behoren. Ze verhogen de weerstand tegen cyberaanvallen afkomstig van statelijke actoren. Daarom is het belangrijk ze te implementeren.

	Ref.	Maatregel
Noodzakelijke maatregelen		
1	3.1	Compartimenteer en segmenteer netwerken en systemen.
2	1.1	Versterk de basisbeveiliging van servers en werkstations.
3	1.5	Gebruik 'whitelisting' van vertrouwde applicaties.
4	1.4	Pas op publieke infrastructuur end-to-end encryptie toe.
Belangrijke maatregelen		
5	3.2	Minimaliseer gebruik van verhoogde rechten.
6	2.1	Pas intrusion detection/prevention toe op bekende IoC's.
7	1.2	Scan inkomende e-mail op veiligheidsrisico's.
8	3.3	Dwing het gebruik van sterke authenticatie af.
9	1.3	Verhoog het veiligheidsbewustzijn van gebruikers.
10	2.2	Voer met regelmaat beveiligingstesten uit zoals penetratietesten, kwetsbaarheidsscans en red teaming.
11	2.3	Check door werknemers bezochte websites op malware.
12	2.4	Gebruik anomalie-detectie voor het kroonjuwelen-compartiment.
13	2.5	Gebruik 'honeypots' en 'honeytokens'.

Op de volgende pagina's is een uitwerking opgenomen waarmee uw ICT-afdeling preventieve en detecterende maatregelen kan nemen voor een effectievere verdediging tegen cyberaanvallen. De referenties in de tabel verwijzen naar de specifieke paragrafen in de uitwerking.

	Algemene doeltreffendheid van de maatregel	**Impact** op werkproces medewerker	**Initiële kosten**	**Vaste kosten**
	Essentieel	Laag	Hoog	Laag
	Essentieel	Laag	Gemiddeld	Gemiddeld
	Essentieel	Hoog	Hoog	Gemiddeld
	Essentieel	Laag	Gemiddeld	Gemiddeld
	Goed	Gemiddeld	Gemiddeld	Gemiddeld
	Goed	Laag	Hoog	Gemiddeld
	Goed	Gemiddeld	Gemiddeld	Laag
	Goed	Hoog	Hoog	Gemiddeld
	Goed	Gemiddeld	Laag	Laag
	Goed	Laag	Gemiddeld	Gemiddeld
	Goed	Laag	Gemiddeld	Laag
	Goed	Laag	Hoog	Laag
	Gemiddeld	Laag	Gemiddeld	Laag

1. Preventie

Om uw weerbaarheid tegen cyberspionnen te verhogen, kunt u de volgende preventieve maatregelen nemen.

1.1 Versterk basisbeveiliging van servers, werkstations en netwerkapparatuur

Veel cyberaanvallen maken misbruik van kwetsbaarheden in de basisbeveiliging van servers, werkstations en netwerkapparatuur. De aanval EXTRABACON vereist bijvoorbeeld leestoegang tot SNMP en netwerktoegang tot beheerdersservices als Telnet of SSH[7]. Dergelijke aanvallen kunnen vaak afgeweerd worden door netwerktoegang tot deze services alleen toe te staan aan vertrouwde systemen. Dit is een basis-beveiligingsmaatregel. De volgende maatregelen zijn ook basismaatregelen en zeer effectief.

a. *Patch software tijdig en op een geautomatiseerde manier.*
   Malware kan een kwetsbaarheid in software gebruiken om het systeem te infecteren. Hierbij zijn drie scenario's mogelijk.

   1. De kwetsbaarheid in de software is bekend en is er een patch beschikbaar (bij voorkeur van de producent van deze software) die deze fout herstelt.
   2. De kwetsbaarheid in de software is bekend maar er is nog geen corrigerende patch beschikbaar, het is mogelijk de software (tijdelijk) te verwijderen of inactief te houden, totdat er een patch beschikbaar is.
   3. De kwetsbaarheid in de software is niet bekend (een 0-day).

   Het merendeel van de aanvallen gebruikt bekende kwetsbaarheden en kan dus met relatief eenvoudige maatregelen voorkomen worden. Het patchen van software heeft daarom een hoge prioriteit en moet een integraal onderdeel zijn van de bedrijfsvoering. Om maximaal te kunnen patchen, is een goed overzicht van alle software op verschillende systemen erg belangrijk.

b. *Harden browsers en applicaties.*
   Maak browsers zo robuust mogelijk. Dit verkleint het risico dat medewerkers door het bezoeken van geïnfecteerde webpagina's besmet raken. Browsers moeten voorzien moet zijn van de laatste patches en plug-ins die als kwetsbaar bekend staan, zoals Flash, Java(script) en Silverlight, moeten uitgeschakeld zijn. Voor verschillende browsers zijn

7 *https://blogs.cisco.com/security/shadow-brokers*

additionele plug-ins beschikbaar die het aanvalsoppervlak van de browser verkleinen. Schakel ook de mogelijkheid om Office macro's te gebruiken uit: deze worden vaak ingezet als middel om malware over te brengen.

c. *Gebruik de beveiligingsmaatregelen die met het besturingssysteem zijn meegeleverd.*
De meeste besturingssystemen worden geleverd met firewall-functionaliteit en geheugenprotectietechnieken zoals EMET of ASLR. Maak gebruik van deze meegeleverde technieken.

d. *Schakel niet-gebruikte functionaliteiten uit.*
Als een server of een werkstation bepaalde services of applicaties niet nodig heeft (zoals remote access of een met het besturingssysteem meegeleverde database), schakel deze dan uit of configureer ze zo restrictief mogelijk.

e. *Houd virusscanners up-to-date.*
Virusscanners houden niet alle cyberaanvallen tegen – studies laten een slagingspercentage zien van rond de 70%. Om dit percentage te blijven behalen moet de virusscanner regelmatig van up-to-date virusdefinities worden voorzien. Dit geldt voor alle apparaten die aan een netwerk worden gekoppeld. Hierdoor wordt bij het detectie- en monitoractiviteiten geen aandacht opgeslokt door veel voorkomende (ongerichte) malware, waardoor aandacht aan overige (gerichte) dreigingen kan worden besteed. Om een analyse van malware mogelijk te maken, is het belangrijk dat de virusscanner de aangetroffen malware niet weggooit maar in quarantaine bewaart.

f. *Gebruik vercijferde dataopslag en dataverkeer.*
Cyberspionage is gericht op het verkrijgen van informatie. Vercijfer waar mogelijk de belangrijke data-at-rest en/of data-in-transit, hierdoor wordt de hoeveelheid informatie waartoe de aanvaller toegang heeft beperkt en wordt het risico dat deze informatie wordt gestolen, verkleind.

g. *Gebruik verwijderbare media onder strikte voorwaarden.*
Voer een restrictief beleid voor verwijderbare media en datadragers om infectie en/of verspreiding tegen te gaan. U verkleint het aanvalsoppervlak door bijvoorbeeld het schrijven naar en lezen van USB-media onmogelijk te maken. Als het voor de bedrijfsprocessen noodzakelijk is, zorg er dan voor dat dit alleen met een geregistreerde USB-media mogelijk is (uitgegeven en onder controle van de eigen organisatie). Schakel ook de autorun functionaliteit op de verschillende media uit. Scan (verwijderbare) media regelmatig en geautomatiseerd op de aanwezigheid van indicatoren van bekende malware.

1.2 Scan e-mails op een mailproxy

Omdat veel cyberaanvallen beginnen met phishing, is het essentieel om inkomende e-mail en eventuele bijlagen te scannen op malware en verdachte URL's voordat deze e-mails in de inbox van de gebruiker komen. Cyberspionnen laten e-mails vertrouwd overkomen: zij gebruiken namen van collega's, leidinggevenden of zakelijke contacten om u te verleiden op een link te klikken of een bijlage te openen. Een spamfilter werkt niet tegen een phishing-aanval.

Zorg ervoor dat uitvoerbare bestandstypen als .exe of .msi nooit als bijlage bij een e-mail in de inbox van een gebruiker terecht kunnen komen. Ook de herkomst van e-mails kan gecontroleerd worden aan de hand van technieken als DomainKeys Identified Mail (DKIM) en Sender Policy Framework (SPF). Indien verdachte kenmerken in een e-mail(bijlage) worden aangetroffen, is het voor nader onderzoek belangrijk dat de volledige e-mail in quarantaine wordt bewaard.

1.3 Verhoog het veiligheidsbewustzijn van medewerkers

Een geslaagde cyberaanval begint vaak met een gebruikersactie, zoals het openen van een e-mailbijlage of een URL. Behalve technische maatregelen om een infectie te voorkomen, moet een gebruiker zoveel als mogelijk in staat gesteld worden om verschillende aanvalsvormen te herkennen. Cyberspionnen kunnen iedere medewerker aanvallen om een netwerk binnen te komen. Zij zullen zich niet alleen richten op key accounts. U kunt hierbij gebruik maken van uw eigen specifieke dreigingsscenario's.

a. *Verifieer onverwachte e-mail van schijnbaar bekende afzenders.*
   Het is bijvoorbeeld verstandig dat uw medewerkers naar aanleiding van een onverwachte e-mail van een schijnbaar vertrouwde afzender eerst deze afzender bellen of mailen, voordat zij de bijlage of URL openen.

b. *Stel een centraal meldpunt in voor verdachte activiteiten.*
   Belangrijk is dat uw medewerkers een centraal punt hebben, waar zij in vertrouwen met hun vragen of met meldingen over verdachte e-mails of berichten naar toe kunnen. Ook loos alarm, mits serieus genomen en serieus afgehandeld, draagt bij aan het veiligheidsbewustzijn binnen uw organisatie.

c. *Wees terughoudend met contactgegevens op sociale media.*
   Het is zeer eenvoudig om de naam, functie en (digitale) contactgegevens van functionarissen binnen een organisatie te identificeren. Deze gegevens worden gebruikt in gerichte spearphishing-aanvallen. Medewerkers kunnen meer terughoudend zijn over

de exacte invulling van hun werkzaamheden (zoals specifieke projecten waaraan wordt gewerkt) en alert zijn bij het aangaan van nieuwe contacten via sociale media als Facebook of LinkedIn.

d. *Bescherm details van gebruikte ICT-componenten en configuraties.*
Alle informatie die een aanvaller van tevoren heeft (bijvoorbeeld over de scheiding van DMZ's, gebruikte proxy's, locatie en soort van dataopslag, locatie van mailservers, gebruikte interne DNS-servers) helpen hem het netwerk makkelijker te verkennen en sneller binnen te dringen.

1.4 Pas encryptie toe op publieke infrastructuur

Vertrouwelijke communicatie over publieke infrastructuur is zonder maatregelen per definitie onveilig. Als eigenaar van de informatie valt niet te controleren via welke weg de informatie wordt verzonden en wie er toegang toe heeft. Het is daarom van belang om vertrouwelijke communicatie te beveiligen. Dit kan door middel van end-to-end-encryptie. De netwerkverbinding tussen twee vertrouwde netwerken kan bijvoorbeeld worden versleuteld met een Virtual Private Network-oplossing zoals OpenVPN-NL. Verkeer naar uw web- en e-mailservers kan worden versleuteld met SSL. Een andere mogelijkheid is om encryptie toe te passen op de informatie zelf, bijvoorbeeld met communicatieproducten als PGP, LUNA of VeraCrypt.

1.5 Gebruik application whitelisting voor vertrouwde applicaties.

Met application whitelisting kan alleen expliciet vertrouwde programmatuur op een systeem worden uitgevoerd. Deze maatregel verbiedt alle software op systemen met uitzondering van de software die op een door de organisatie samengestelde vertrouwde lijst (de whitelist) staat. Door gebruik te maken van whitelisting wordt het risico verkleind dat malware kan worden geïnstalleerd of uitgevoerd. Daarnaast kan door application isolation de toegang van een applicatie tot gegevens tot het noodzakelijke minimum worden beperkt.

Hoewel deze maatregelen zeer effectief zijn, is een keerzijde dat implementatie een goede planning en verfijning van instellingen vraagt. In combinatie met segmentatie is dit bij aanvang een administratieve last, dat echter voor het netwerksegment waar de kroonjuwelen zich bevinden zeer de moeite waard is.

2 Detectie

De volgende maatregelen vergroten de kans op detectie van een aanval, zodat (eerder) tegenacties genomen kunnen worden[8]. De effectiviteit van deze maatregelen is afhankelijk van de effectiviteit van uw incident response. Als u iets detecteert en er niets mee doet, is de effectiviteit nul.

2.1 Pas intrusion detection/prevention toe op bekende indicatoren

Intrusion detection/prevention is een scala aan maatregelen om een (geslaagde) cyber=aanval op uw infrastructuur te herkennen. De maatregelen zijn gebaseerd op bekende indicatoren (Indicators of Compromise; IoC's). IoC's kunnen voorkomen in netwerkverkeer of op een computersysteem. Een goed ingericht intrusion detection-proces levert veel data op die geanalyseerd moet worden. Intrusion detection/prevention kan worden opgedeeld in de volgende deelprocessen.

a. *Scan computersystemen actief op verdachte activiteiten.*
   Scan computersystemen (zowel servers als werkstations) actief en regelmatig op verdachte activiteiten. Dit wordt Host Based Intrusion Detection (HIDS) genoemd. Scan bijvoorbeeld op het opstarten van verdachte processen, het actief zijn van niet-toegestane bestandstypen en het initiëren van verdacht netwerkverkeer (bijvoorbeeld het opzetten van een VPN-verbinding naar een extern adres). Controleer periodiek of ieder aanwezig account nog operationeel moet zijn. Dit om de aanwezigheid van spook-accounts (accounts van al vertrokken werknemers of illegaal aangemaakte accounts) te voorkomen.

b. *Scan ingaand en uitgaand netwerkverkeer op verdachte activiteit.*
   Scan ingaand en uitgaand netwerkverkeer actief en regelmatig op verdachte activiteiten. Dit wordt network based intrusion detection (NIDS) genoemd. Verschillende hulp-programma's voor het real-time monitoren en filteren van netwerkverkeer zijn publiek beschikbaar. Gebruik van een Next Generation Firewall (NGFW) met stateful inspection of deep packet inspection (DPI) is noodzakelijk. Voor internetverkeer van gebruikers kan een proxy worden gebruikt. Idealiter kan de NGFW of proxy ook versleutelde verbindingen aan, bijvoorbeeld door middel van SSL Offloading.

8 *Zie ook de publicaties: 'Handreiking voor implementatie van detectie-oplossingen' en 'Hoe herkent u een aanval van een Advanced Persistent Threat'.*

c. *Leg centraal relevante netwerkconnectiviteit vast (en check deze logbestanden).*
Een goede logging van alle netwerkconnectiviteit, bijvoorbeeld met behulp van netflow of bro, is van belang om goed inzicht te krijgen in wat er in uw netwerk gebeurt en om te kunnen onderzoeken wat er in het verleden is gebeurd. Door gebruik te maken van proxy's tussen het interne netwerk en externe netwerken is het mogelijk om relevante netwerkactiviteiten en connectiviteit te loggen. Beoordeel deze logbestanden regelmatig (geautomatiseerd). Abnormaliteiten, bijvoorbeeld in de hoeveelheid netwerkverkeer, tijdstippen van connectiviteit en specifieke DNS-queries, kunnen dan direct (automatisch) gerapporteerd worden.

d. *Blokkeer netwerkverkeer met bekende C2-domeinen.*
Na een infectie met malware zal het geïnfecteerde systeem vaak proberen contact maken met een command and control (C2)-server van de aanvaller. Filter het netwerkverkeer actief op dit verkeer door gebruik te maken van de indicatoren uit rapporten over cyberaanvallen. Pogingen om contact te zoeken met malafide domeinen worden zichtbaar in de logging van het netwerkverkeer. Start dan direct een vervolgonderzoek. Blokkeren van dit netwerkverkeer kan via een NGFW of een proxy.

e. *Analyseer de informatie uit het intrusion detection/prevention-proces.*
Combineer informatie binnen het intrusion detection/prevention-proces om verdachte activiteiten op de interne infrastructuur te kunnen detecteren. Een intrusion detection-proces levert meestal te veel informatie op om handmatig te onderzoeken en het analyseren van dergelijke informatie is een vak apart. HIDS- en NIDS-systemen kunnen rapporteren aan een Security Incident and Event Management-systeem (SIEM). Een SIEM maakt de bulk aan informatie beter doorzoekbaar en maakt correlaties en statistieken mogelijk. Zorg voor gekwalificeerd personeel, dat de opgeleverde informatie kan duiden.

2.2 Voer regelmatig beveiligingstesten uit

Een ICT-infrastructuur is continu aan verandering onderhevig. Nieuwe systemen worden aangesloten, oude systemen worden geüpdatet en configuraties van netwerkapparatuur worden regelmatig aangepast. Met elke verandering in de ICT-infrastructuur verandert de beveiligingssituatie mee.

Daarom is het belangrijk om regelmatig beveiligingstesten uit te voeren, uiteraard met de focus op de eerdergenoemde kroonjuwelen. De dreigingsscenario's voor uw organisatie helpen u hierbij. Bij het uitvoeren van gesimuleerde cyberaanvallen gaat het niet zozeer om detectie van de aanval, maar om het testen van de beveiliging als geheel: preventie, beperken van de impact, detectie en respons.

Globaal zijn drie soorten beveiligingstesten belangrijk.

a. *Kwetsbaarheidsscans*
   Een kwetsbaarheidsscan (of audit) is een toets van (een gedeelte van) het netwerk op kwetsbaarheden, zoals verouderde versies van netwerkservices en zwakheden in de configuratie van netwerkcomponenten of computersystemen. Een kwetsbaarheidsscan brengt de gevonden zwakheden in kaart.

b. *Penetratietesten*
   Een penetratietest is een audit, waarbij de gevonden kwetsbaarheden ook daadwerkelijk worden gebruikt om toegang te krijgen tot computersystemen. Zo wordt een aanvalsscenario reëler 'nagespeeld'.

c. *Red teaming*
   De beveiligingstest die de werkelijkheid het meest benadert is de red teaming-aanval. Waar een kwetsbaarheidsscan en een penetratietest worden uitgevoerd binnen een bepaalt bereik en met medeweten van de beheerder(s) van de systemen, wordt bij red teaming niemand op de hoogte gesteld van de aard en timing van de aanval. De aanval wordt zo onzichtbaar mogelijk uitgevoerd.

2.3 Scan door werknemers bezochte websites

Websites die door werknemers zijn bezocht, kunnen gelogd worden en onderzocht op eventuele aanwezigheid van malware. Een goed hulpmiddel hierbij is Honeyspider. Honeyspider biedt de mogelijkheid om geautomatiseerd en periodiek (een selectie van de) door werknemers bezochte websites te controleren. Er zijn ook commerciële producten beschikbaar, die eveneens gebruik maken van dergelijke 'sandboxing'-technologieën.

2.4 Gebruik anomalie-detectie voor het kroonjuwelen-compartiment

De beschreven intrusion detection-methoden zijn gebaseerd op al bekende indicatoren van cyberaanvallen. Anomalie-detectie heeft als doel om nog onbekende indicatoren te vinden door middel van het analyseren van afwijkingen in een 'normale' situatie. Anomalie-detectie kan alleen effectief plaatsvinden op kleine gecompartimenteerde netwerksegmenten, waar de 'normale' situatie relatief eenvoudig in kaart te brengen is en waar deze situatie constant blijft. Bij een juiste compartimentering voldoet het kroonjuwelen-compartiment waarschijnlijk aan deze voorwaarden. Analyse op afwijkingen van de normale situatie kan een aanval die gebruik maakt van onbekende indicatoren dan mogelijk alsnog detecteren.

2.5 Gebruik honeypots en honeytokens

Een honeytoken of een low interaction honeypot (l.i.h) slaat op een passief kenmerk, in een systeem of in gegevens, dat bewust is gecreëerd om aanvallen te kunnen detecteren.

In tegenstelling tot actieve honeypots, die vaak het doel hebben om een aanval te kunnen analyseren, is een honeytoken of low interaction honeypot te vergelijken met het plaatsen van een struikeldraad. Indien iemand erover struikelt, wordt u hier direct van in kennis gesteld. Bij meerdere goed gekozen honeytokens is het voor een aanvaller bijzonder lastig om er geen te raken.

Er zijn veel verschillende vormen van honeytokens en l.i.h.'s en verschillende manieren om deze te monitoren. Keuzes hierin zijn afhankelijk van de situatie en het doel waarvoor het token wordt ingezet. Zo kan een honeytoken een kenmerk zijn in productiedata of bewust gecreëerde 'fake data'. Er kan ook gedacht worden aan fake invulvelden, fake websites, netwerkshares, netwerkservices, en ga zo maar door.

Om te controleren of honeytokens daadwerkelijk worden gebruikt, kunnen relatief simpele IoC's worden gemaakt. Deze kunnen worden opgenomen in bijvoorbeeld een IDS of SIEM.

3.1 Compartimenteer en segmenteer netwerken en systemen

Veel ICT-netwerken zijn ingericht als een weiland; een stevig hek om de buitenranden en een groot open speelveld daarbinnen. Een dergelijk netwerkontwerp is nauwelijks te verdedigen. Zodra een cyberspion toegang heeft tot een systeem, zal hij proberen andere delen van uw netwerk of gekoppelde netwerken binnen te dringen. Om dit moeilijk te maken, moeten netwerken gesegmenteerd zijn en systemen gecompartimenteerd zijn. Segmenteren is het (her)indelen van uw netwerk in verschillende stukken. Zo beperkt u de toegang tot uw kroonjuwelen tot die mensen, applicaties en computers die deze toegang daadwerkelijk nodig hebben. Dit geldt voornamelijk voor belangrijke centrale systemen, zoals domain controllers in een Active Directory-omgeving.

Investeringen in beveiliging kunnen gericht worden op die segmenten waar ze het meest nodig zijn, terwijl eveneens ruimte blijft voor een minder vertrouwde omgeving voor de minder vertrouwelijke werkprocessen en gegevens. Segmentatie kan redelijk eenvoudig worden gerealiseerd met behulp van Virtual Local Area Networks (VLAN's) en firewalls. In de vertrouwelijke segmenten is toegang tot het internet zeer onwenselijk.

Vaak is er in een netwerk geen noodzaak dat werkstations direct met elkaar kunnen communiceren; meestal is communicatie met een of meerdere servers voldoende. Mogelijkheden voor werkstations om onderling te kunnen communiceren moeten dan uitgeschakeld zijn. Dit is compartimenteren. Als er geen noodzaak is voor verbinding met een extern netwerk dient deze mogelijkheid in de configuratie uit te staan.

3.2 Minimaliseer gebruik van verhoogde rechten

Netwerkbeheerders (admins) behoren tot de kroonjuwelen van de organisatie. Verdedig deze: beperk het aantal accounts en scherm hun identiteit af. Geef minimale rechten aan (accounts van) reguliere gebruikers. Gecompromitteerde gebruikersaccounts kunnen hierdoor beperkt gebruikt worden voor verkenningen van het systeem of netwerk door een cyberaanvaller. Ga zeer zorgvuldig om met (de uitgifte van) accounts met beheerdersrechten. Gebruikers met systeem(beheer)rechten op een werkstation hoeven niet dezelfde rechten op het netwerk te hebben en andersom. Schakel een account uit als dit niet meer gebruikt wordt. Gebruik verschillende accounts en wachtwoorden voor beheerstaken binnen verschillende compartimenten, zeker voor het kroonjuwelen-compartiment.

3.3 Dwing het gebruik van sterke authenticatie af

Een cyberaanvaller gaat op zoek naar credentials (zoals wachtwoorden of sleutelmateriaal) waarmee hij zijn rechten of toegang kan vergroten. Als hij bijvoorbeeld toegang heeft tot 'hashes' van wachtwoorden, dan zal hij proberen de bijbehorende wachtwoorden te achterhalen.

a. *Gebruik sterke wachtwoorden en sterke versleuteling.*
   Wachtwoorden moeten ingewikkeld zijn om de dreiging van het (geautomatiseerd) kraken van wachtwoorden te verkleinen. Controleer daarom regelmatig en actief of wachtwoorden sterk genoeg zijn (bijvoorbeeld door de hashes tegen een wachtwoord-recovery tool te houden). Bijvoorbeeld wanneer een gebruiker een (nieuw) wachtwoord instelt. Gebruik uitsluitend sterke cryptografische algoritmen voor versleuteling, zoals AES256.

b. *Sla cryptografisch sleutelmateriaal niet op het systeem van de gebruiker op.*
   Als dit wel noodzakelijk is, beschermt dit materiaal dan met een sterk wachtwoord (bij voorkeur in combinatie met een tweede vorm van authenticatie).

c. *Sta alleen sterke vormen van externe toegang tot het bedrijfsnetwerk toe.*
   Zodra een aanvaller een systeem heeft gecompromitteerd, zal hij op zoek gaan naar de credentials van de gebruiker. Dit biedt de aanvaller mogelijk ook externe toegang tot het bedrijfsnetwerk. Om dit risico tegen te gaan, is het raadzaam om externe toegang tot het bedrijfsnetwerk alleen mogelijk te maken via VPN-tunnels waarvoor twee-factor-authenticatie vereist is.

d. *Bescherm uw wifi-netwerk.*
   Voorzie ook de draadloze verbindingen binnen uw bedrijfsnetwerk van een sterke vorm van authenticatie, het liefst gebaseerd op digitale certificaten.

Ga het gesprek aan met uw ICT-leverancier

Steeds vaker wordt ICT uitbesteed aan leveranciers die zowel hardware als software als een dienst aanleveren. Indien u uw ICT heeft uitbesteed, ga dan het gesprek aan met uw leverancier. Zijn bovenstaande maatregelen voor u geïmplementeerd? Kan de leverancier bijvoorbeeld de juiste logging leveren, indien u onderzoek wilt doen naar een mogelijke aanval op uw organisatie? Uit onze ervaring blijkt dat dit niet altijd het geval is, bijvoorbeeld omdat logging voor uw organisatie door uw leverancier niet te scheiden is van andere klanten. Dit maakt het voor u moeilijk om aard en omvang van een digitale aanval te onderzoeken.

Hebt u een incident waarbij mogelijk een statelijke actor betrokken is?

Waar mogelijk delen inlichtingendiensten de opbrengsten van onderzoeken naar cyberaanvallen door statelijke actoren. Bijvoorbeeld door technische kenmerken van deze aanvallen te delen met ketenpartners of bilateraal met slachtoffers van een cyberaanval. Inlichtingendiensten doen dit bilateraal om de vertrouwelijkheid van uw informatie en van onze bronnen en werkwijze te waarborgen. Daarnaast adviseren de inlichtingendiensten over de bescherming van vertrouwelijke informatie binnen de rijksoverheid. Dit alles om anderen in staat te stellen de weerbaarheid te vergroten.

Incidenten waarbij mogelijk een statelijke actor betrokken is, kunt u melden bij de inlichtingendiensten. U kunt dan contact opnemen met de **Algemene Inlichtingen- en Veiligheidsdienst**, telefoonnummer 079-320 50 50. Als het incident betrekking heeft op defensie en defensiebelangen raakt, verzoeken wij u contact op te nemen met **Bureau Industrie Veiligheid**: indussec@mindef.nl

Voor de rijksoverheid en de vitale infrastructuur fungeert het **Nationaal Cyber Security Centrum** (ncsc.nl) als het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Medio 2017 zal de Wet gegevensverwerking en meldplicht cybersecurity in werking treden. Deze verplicht aanbieders binnen de vitale infrastructuur en de rijksoverheid maatschappij-ontwrichtende incidenten bij het NCSC te melden. Het NCSC adviseert om bij incidenten altijd aangifte te doen bij de politie.

Sinds 1 januari 2016 geldt de meldplicht datalekken. Deze meldplicht houdt in dat publieke en private organisaties een incident waarbij persoonsgegevens betrokken zijn direct moeten melden bij de **Autoriteit Persoonsgegevens**. Hiervoor bestaat een meldloket op de website autoriteitpersoonsgevens.nl.

Colofon

Deze brochure is een uitgave van:

Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties
Algemene Inlichtingen- en Veiligheidsdienst
aivd.nl

Ministerie van Defensie
Militaire Inlichtingen- en Veiligheidsdienst
defensie.nl/mivd

april 2017