Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

De aanhouder wint

De wereld van Advanced Persistent Threats

Factsheet FS-2013-02c

versie 1.3 | 03 oktober 2013

Een Advanced Persistent Threat (APT) is de dreiging die uitgaat van een doelgerichte 'langdurige' cyberaanval op vooral kennisrijke landen en organisaties door statelijke actoren en criminele organisaties[1]. De aanvaller is daarbij volhardend in zowel de pogingen om een organisatie binnen te dringen als ook om binnen de ICT-infrastructuur heimelijk aanwezig te blijven.

Tijdens de APT-aanval zal de aanvaller vooral 'vertrouwelijke' informatie verzamelen en/of voorbereidingen treffen om werking van vitale componenten te kunnen verstoren. Het merendeel van deze aanvallen is eenvoudig van aard en vooral succesvol door het ontbreken, binnen organisaties, van adequate detectie en beveiligingsmaatregelen.

In het Engels wordt deze dreiging 'Advanced Persistent Threat' (APT) genoemd. De indruk bestaat dat tegen doelgerichte aanvallen weinig maatregelen te nemen zijn. Dit is zeker niet het geval. Deze factsheet biedt, naast een analyse over APT-aanvallen, praktische handvatten om de bescherming tegen en detectie van deze aanvallen te verbeteren.

Wat is een APT-aanval?

Een APT-aanval is een gemotiveerde doelgerichte aanval op een staat, organisatie, persoon of groep van personen. Het motief bij een dergelijke aanval is veelal spionage, surveillance, financieel en/of politiek gewin, sabotage[2] of ideologische.

Oorspronkelijk waren APT-aanvallen[3] (in)directe, door overheden gefinancierde internetaanvallen in het verlengde van reguliere spionageactiviteiten. De laatste jaren maken ook andere groeperingen steeds meer gebruik van doelgerichte en complexe aanvalscampagnes om informatie te stelen en door te verkopen aan de hoogste bieder, onder andere op speciale cybermarktplaatsen. Informatie is geld waard en kwaadwillenden zijn 'actief' op 'zoek' naar 'handel'. Door deze handel lopen steeds meer organisaties die eerder geen spionagedoelwit waren nu een reëel risico[4]. Dit alles maakt een doelgerichte aanval een wezenlijk andere cyberdreiging, vooral omdat de aanvaller duidelijk inzet op heimelijk optreden, extractie van informatie en een langdurige en blijvende compromittatie van de doelwitorganisatie.

Advanced: Achter doelgerichte aanvallen zit een aanvaller die (ICT) expertise en financiële middelen inzet om, zonder gedetecteerd te worden, toegang tot, goed[5], beschermde netwerken en gevoelige informatie probeert te krijgen en te behouden. Vaak zit er achter dit type aanvaller een staat, een 'legitieme' bedrijfstak of een criminele organisatie als afnemer of facilitator. Het hierbij in fase inzetten van steeds meer kundige aanvallers in combinatie met verschillende, op maat toegepaste, aanvalstechnieken, waaronder social-engineering, maakt de aanval geavanceerd.

Echter veel APT-aanvallen zijn niet zo geavanceerd, maar slagen juist door een gebrek aan beveiliging(sbewustzijn) en detectiemiddelen bij de doelwitten. Daar komt bij dat in veel aanvallen ogenschijnlijk lukraak exploits worden ingezet in de hoop op een infectie, dit getuigt niet altijd van een gedegen inzicht in de netwerkomgeving van een doelwit en een geavanceerde aanpak. In deze gevallen is het aannemelijk dat de aanvaller enkel een globaal beeld heeft van de informatie die hij wil verkrijgen en empirisch acteert.

---

[1] Cybersecuritybeeld 2012, Nationaal Cyber Security Centrum, juni 2012, https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten

[2] Een sabotage bij een APT is anders dan een DoS-aanval. Bij een DoS-aanval worden er geen systemen gecompromitteerd (besmet) met malware. Meer informatie vindt u in de factsheet ' continuïteit van onlinediensten van het NCSC. https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-continuiteit-van-online-diensten.html

[3] De US Air Force is de term Advance Persistent Threat rond 2006 gaan gebruiken voor gerichte aanvallen.

[4] Let wel deze organisaties kregen wellicht in het verleden ook al de nodige aandacht in de vorm van (bedrijfs)spionage, diefstal en sabotage. De handel in informatie zorgt ervoor dat er actiever 'gezocht' wordt naar 'handel' door kwaadwillenden.

[5] De term goed is relatief. Er zijn goed beveiligde ICT omgevingen. Echter het merendeel van de infrastructuren zijn slechter beveiligd.

Persistent: de aanvaller wendt, mogelijk over een lange periode (jaren) en in meerdere aanvalsstappen, verschillende technieken aan. De aanvaller is daarbij zeer volhoudend en creatief in het gebruik van technieken om zo toegang te verkrijgen, aanwezigheid te vergroten, te behouden en kans op detectie te minimaliseren. De gebruikte aanvalsmiddelen, zoals malware, zijn daarbij moeilijk uit het netwerk te verwijderen doordat deze in reactie op de verdediging wordt aangepast en geactualiseerd. De volhardendheid van de aanvaller, de langdurige aanwezigheid en het heimelijke karakter maken een APT-aanval bijzonder.

Threat: sabotage, manipulatie van vitale bedrijfsprocessen, imagoschade en spionage zijn de meest relevante dreigingen bij doelgerichte aanvallen. De dreiging[6] wordt versterkt indien de ontrokken informatie actief misbruikt wordt door de aanvaller voor het verstevigen van de concurrentiepositie, politiek / landelijk gewin en/of maatschappelijke ontwrichtingen. Hoe groter de belangen en het gewin: hoe meer middelen, motivatie en kennis er zal worden ingezet door de kwaadwillenden, hoe groter de dreiging.

Wie zijn de aanvallers?

Een APT-aanvaller wordt ook wel APA (Advanced Persistent Adversary) genoemd. Achter de aanvallen kunnen statelijke actoren (inlichtingen- en veiligheidsdiensten en militaire entiteiten) zitten die vanuit een economisch, politiek of militair-strategisch gewin acteren. Daarnaast is er een toenemende activiteit van hackers, ad-hoc allianties en cybercriminelen die doelgerichte aanvallen gebruiken voor financieel gewin, onvrede en/of ideologische gronden. Binnen het domein van de aanvallers vindt een verregaande professionalisering plaats waar diensten aangeboden worden als “crime / malware-as-service[7]” en de inhuur van hackers bij het voorbereiden en ondersteunen van een APT.

Over het algemeen heeft de aanvaller een beter besef van de waarde van de informatie en de houdbaarheid van de verdedigingsmaatregelen en kwetsbaarheden dan de meeste aangevallen organisaties. Via openbare bronnen en netwerkscans wordt er een beeld verkregen in de kwetsbaarheden van een organisatie en/of personen. De aanvaller kiest een exploit, kwetsbaarheid en/of persoon als startpunt of vervolgstap in de aanval. Bij elke stap wordt bepaald welke informatie belangrijk is en waar de informatie in de volgende fase van de aanval te vinden kan zijn.

Buiten het feit dat veel APT-aanvallen ‘eenvoudig’ van aard zijn en met simpele middelen worden uitgevoerd zijn er ook ‘zwaardere’ doelgerichte aanvallen. Bij deze aanvallen wordt continu gereageerd op tegenmaatregelen van de organisatie en indien nodig worden steeds geavanceerdere aanvalstechnieken en/of resources ingezet. De aanvaller is daarbij vasthoudend, flexibeler en reageert sneller dan de verdediging met de (tegen)maatregelen, vaak ook omdat dit type aanvaller al heeft geanticipeerd op een eventuele detectie en eventuele repressiemaatregelen van de doelwitorganisatie.

Voor wie is een doelgerichte aanval een reële dreiging?

Als een kwaadwillende denkt dat informatie of sabotage iets kan opleveren (een waarde heeft) dan kan een organisatie geconfronteerd worden met een doelgerichte aanval. Vaak zijn dit omgevingen met grote economische, kennisrijke, financiële, politieke belangen en / of activiteiten. Daarnaast wordt ter ondersteuning en in de voorbereiding van de aanvallen ook de ICT infrastructuur, cyberonderzoekers, opsporingsorganisaties, leveranciers en klanten aangevallen om (extra) informatie[8] te verkrijgen[9] en/of deze partijen heimelijk in te zetten als onderdeel van de aanval.

De motieven van de aanvaller bepalen daarbij de ernst van de dreiging in plaats van de reguliere risico-inschattingen van een organisatie.

Wat is de slagingskans van een APT?

Het succes van een APT is afhankelijk van de middelen van een aanvaller en de weerbaarheid van een organisatie. Veel organisaties zijn onwetend dat dit soort aanvallen kunnen plaatsvinden en zijn daarom niet voorbereid. Het management ontbreekt vaak de nodige ICT-kennis, waardoor het besef van de cyberrisico’s en het belang van beveiligingsmaatregelen onderbelicht blijven en niet een integraal onderdeel uitmaken van het primair (besluitvorming)proces. Vooral in complexe omgevingen met veel (netwerk) componenten en eindgebruikers is daarom de kans op menselijke fouten[10] groot. Ook worden in de dagelijkse operatie de beveiligingsmaatregelen onvoldoende continu bewaakt en onderhouden. Ze zijn vooral gericht op preventie en ontberen de noodzakelijke ‘situational-awareness’ welke noodzakelijk is om APT-aanvallen te onderkennen en er adequaat op te kunnen reageren. Het reageren op de snelle technologische ontwikkelingen en dreigingen wordt daarbij vertraagd door lange doorlooptijden van procedures, te beperkt budget, lange beslistrajecten en een structureel onvermogen van organisaties om te reageren (mandaten en bevoegdheden).

---

[6] Het verlies van financiële, economische, technisch-wetenschappelijke of politiekgevoelige informatie kan leiden tot schade aan de organisatie, economie en/of nationale veiligheid.

[7] Er is een zwarte markt (economie) waar op bestelling malware ontwikkeld kan worden. Een onderhoudscontract, exclusief gebruik van de exploit en zelfs een helpdesk zijn daarbij onderdelen van de “dienstverlening”.

[8] Informatie over zwakheden, tools, organisatiekennis, etc.

[9] Kwetsbaarheidsanalyse spionage, Spionagerisico’s en de nationale veiligheid, AIVD, september 2010.

[10] Een e-maillink is snel geopend, een website met malware wordt niet herkend, informatie wordt welwillend gedeeld, een deur wordt beleefd opengehouden, een nieuwe muis als relatiegeschenk wordt gewoon aangesloten, et cetera.

Organisaties met een securityincident-responseproces[11] hebben een duidelijk betere startpositie.

Tegenover de organisatie staat de aanvaller. Een kwetsbaarheid vinden is voldoende. De aanvaller reageert adaptief en sneller dan de meeste organisaties. De opbrengsten zijn interessant[12], een aanval en de heimelijke activiteiten worden door de meeste organisaties nauwelijks gedetecteerd.

Dit maakt de slagingskans van een APT-aanval zeer groot.

Enkele bekende doelgerichte aanvallen

- Saudisch oliebedrijf Aramco, 2012
- LuckyCat, 2012
- Flame 2007-2012
- NASA, 2011
- Lockheed Martin, 2011
- Diginotar, 2011
- EU-Commission, 2011
- Taidoor, 2011
- Nitro & RSA, 2011
- US Nuclear Lab Attack, 2011
- GhostRat 2009-2011
- Operation Payback, 2010
- Google Aurora, 2010
- Stuxnet, 2009-2010
- GhostNet, 2007-2009
- Belgacom 2010-2013

Hoe verloopt een APT-aanval?

Een doelgerichte aanval doorloopt meestal een aantal herkenbare stappen. Deze stappen kunnen in volgorde en gelijktijdig door de aanvaller(s) uitgevoerd worden.

Bij elke stap worden een aantal mogelijke tegenmaatregelen benoemd.

Stap 0: verkenning

Kenmerken: de aanvaller kiest en identificeert het doel. Via openbare bronnen, 'social media mining', netwerkscanning en social engineering wordt gezocht naar interessante personen en kwetsbaarheden van het aan te vallen doel. Met deze informatie wordt een aanvalscampagne opgesteld.

Tegenmaatregelen: beperk het publiceren van bedrijfs- en persoonlijke informatie, onder andere adresgegevens, actuele werkzaamheden en reisdoelen, op openbare bronnen. Registreer en reageer op social engineering aanvalspogingen. Geef werknemers, vooral met veel externe contacten[13] en die werken met gevoelige informatie, tijdig instructie in het herkennen van onder andere social engineering aanvallen. Stel een protocol op over zichtbaarheid op social media en internet en het gebruik en publicatie van (gevoelige) bedrijfsinformatie. Bewaak de naleving van deze regels door actief op internet en social media op zoek te gaan naar bedrijfsinformatie. Detecteer portscans en beperk de informatie die via de portscans gevonden kan worden (onder andere door het harden van de infrastructuur).

Een 'Red-team'-oefening of een pentest kan aanvullende inzichten verschaffen over bestaande zwakheden, naleving en reactiepatronen binnen de organisatie.

Stap 1: initiële aanval (*breach*).

Voor de initiële aanval wordt vaak gebruik gemaakt van een doelgerichte e-mail ('spearphishing') die gestuurd wordt vanaf een 'bekend' e-mailadres over een actueel (werk gerelateerde) onderwerp. Een voorbeeld hiervan is een e-mail van een bezoek aan een beurs, van een leverancier, klant of bekende relatie. Deze e-mail bevat een bijlage of link naar een website met malafide code die bij het openen de computer infecteert. Naast e-mails worden ook demo cd's, usb-sticks, het lokken naar websites met malware (drive-by), aangepaste USB-devices zoals muizen, via wifi, bluetooth of onbeheerd achtergelaten of 'refurbished' telefoons, IPad's, laptops, pc's, routers, etc gebruikt om malware te introduceren.

Tegenmaatregelen: maak een communicatieplan voor de gehele organisatie met daarin instructies om onrechtmatigheden te herkennen en hoe deze te melden. Denk daarbij ook aan scenario's om eindgebruikers actief te informeren tijdens aanvallen en preventieve awareness (bijvoorbeeld hoe om te gaan met e-mailbijlagen en websitebezoek). 'Harden' de ICT-infrastructuur (waaronder whitelisting van applicaties) en zorg voor actief patchmanagement. Maak gebruik van verschillende malwarescanners op cliënts, fileservers, proxy's en de e-mailservers. Implementeer een intrusiondetectieoplossing met APT-detectie. (bijvoorbeeld een IDS, HDS, honeypot).

Stap 2: creëren van een achterdeur (backdoor)

De geïnfecteerde machine probeert in deze fase contact te maken met een in- of externe command en control server[14]. Hier heeft de aanvaller aanvullende hulpmiddelen, malware (zoals rootkits, passwoordkrakers of filetransfertools) klaarstaan voor de download. Deze hulpmiddelen worden lokaal geïnstalleerd en/of op systemen ter voorbereiding van stap 2a.

[11] Dit kan een ITIL proces, csirt, cert, soc en/of sic zijn.
[12] De winsten van cyberkartels evenaren tegenwoordig die van de drugskartels.
[13] Zoals personeelszaken, communicatie, persvoorlichting, accountmanagement.
[14] C&C's kunnen cloudservices, gecompromitteerde servers en internetdiensten als irc-kanalen, news- en webservers zijn.

Stap 2a: verdere infectie (*lateral movement*) en extra rechten verkrijgen (*obtain credentials*)
In deze fase worden[15] zoveel mogelijk (andere) machines geïnfecteerd en informatie over de infrastructuur en rechten (wachtwoorden en/of hashes) gestolen. Indien nodig wordt speciale software[16] ingezet om informatie en/of administratorrechten in het verdere netwerk te krijgen.
Tegenmaatregelen: ook in deze fase is actief en tijdige patch-management van belang. Monitor en log alle in- en uitgaande verkeer op verdacht en afwijkend patronen. Controleer realtime het juist functioneren (en de onregelmatigheden) van alle (vitale) ICT-infrastructuurcomponenten. Segmenteer het netwerk, gebruik verschillende credentials voor toegang tot de verschillende netwerken en informatiebronnen (vooral de beheerders en medewerkers met toegang tot gevoelige gegevens). Definieer en minimaliseer de gecontroleerde doorgangen tussen deze verschillende segmenten ('trusted-paths') en monitor het verkeer bij deze doorgangen (ook die voor beheerdoeleinden). Bepaal welke doorgangen toegang geven tot vitale informatie. Stel een detectie- en repressieplan op om bij onregelmatigheden direct te kunnen reageren.

Stap 3: het verkrijgen van informatie (*data extraction*)
De geïnfecteerde machine(s) sturen informatie (zoals e-mails, documenten, microfoongeluid, screendumps, webcambeelden, certificaten en hashes) automatisch en/of op commando naar een server van de aanvaller. Deze communicatie verloopt direct of via besmette proxymachines in het netwerk. In deze fase kunnen geïnfecteerde machines ook gebruikt worden om direct en/of via draagbare media, saboterende aanvallen op bijvoorbeeld ICS/SCADA-omgevingen te initiëren.
Tegenmaatregelen: stel profielen (baseline) op voor het gebruik van informatiebronnen, systeemgebruik en netwerkverkeer en detecteer daarbij de onrechtmatigheden en anomaliteiten. Beperk de toegang, ook in het aantal 'gelijktijdig' te benaderen netwerkcomponenten, bestanden, databaserecords en andere informatiebronnen. Isoleer de kantoor- van de procesomgeving en richt een gescheiden beheeromgeving in.

Stap 4: behouden van aanwezigheid (*maintain Presence*)
Actief zorgt de aanvaller ervoor dat de kans op detectie beperkt blijft en zal indien nodig additionele malware installeren om tegenacties van de verdediging voor te blijven. In deze fase wordt continu informatie uit de organisatie ontrokken.

Tegenmaatregelen: controleer regelmatig de fysieke en logische netwerk- en systeemconfiguraties. (bijvoorbeeld op de aanwezigheid van onbekende netwerkdevices, bestanden, toegangsrechten en policy's). Controleer de logs op ‚rare, foutmeldingen en afwijkingen, zoals ongebruikelijke pieken, tijdstip van verkeer en bestemmingen. Herinstalleer bij twijfel opnieuw de netwerkcomponenten en de systemen in de (vitale) infrastructuur.

Stap 5: exit
In de aanvalscampagne kan de aanvaller ervoor hebben gekozen om zo lang mogelijk (jaren) binnen de organisatie actief te blijven of na het verkrijgen van de informatie stil en heimelijk de malware te de-installeren en de sporen van aanwezigheid uit te wissen. Ook kan de aanvaller kiezen om zoveel mogelijk systemen en de responseorganisatie te saboteren. Dit om de analyse- en repressiecapaciteiten van de organisatie te verstoren en verdere forensisch onderzoek en daderattributie te frustreren.
Tegenmaatregelen: zorg voor een real-time logging omgeving, niet door kwaadwillenden te bereiken en/of te veranderen, van alle belangrijke ICT-infrastructuur-componenten. Bewaar deze voor een lange periode, bijvoorbeeld op een syslog-server, en controleer daarbij ook de compleetheid, ook bijvoorbeeld succesvolle authenticatie en juistheid van de meldingen. Maak regelmatig backups, bewaar deze over een lange periode en controleer deze op juistheid en terugzetbaarheid.

Tot slot

Tegen doelgerichte aanvallen kan een keur van maatregelen worden genomen. Een netwerkomgeving is nooit 100 procent waterdicht. Uiteindelijk kan de aanvaller een zwakheid, een beheerders-, eindgebruikerfout en/of een zero-day, uitnutten voor de aanval. Een goed georganiseerde aanval, bijvoorbeeld door een vreemde mogendheid, heeft uiteindelijk een grote slagingskans. Met deze kennis kan een juiste verdedigingsstrategie worden gekozen. Snelle detectie, netwerk- en informatiesegmentatie geeft de organisatie de mogelijkheden om schade te beperken en (tegen)maatregelen te nemen tijdens de aanval. Het houden van red-team-oefeningen en de inrichting van een incidentresponse-proces en/of een Security Operationele Center (SOC) zijn onmisbare aanvullende maatregelen om als organisatie, snel en kundig, te kunnen reageren.

Indien er duidelijk signalen zijn dat uw organisatie doelgericht wordt aangevallen kunt u contact opnemen met het NCSC, de AIVD en/of MIVD (bedrijven met ABDO-certificering) voor verdere ondersteuning.

"People only accept change when they are faced with necessity, and only recognize necessity when a crisis is upon them"
Jean Monnet (architect of European Unity).

[15] Is afhankelijk van de aanvalscampagne. Er zijn ook scenario's bekend waar doelgericht alleen één target-machine werd aangevallen.
[16] Veel gebruikte software waar detectie (IDS) op ingesteld kan worden zijn: cachedump, dbgview, getmail, gsecdump, htran, lsb-steno, lslsass, lz77, mapiget, netbox, pwdump, sdelete, upx shell, wce, zxproxy, zxportmap, zxhttpserver.

Mogelijke maatregelen tegen een APT-aanval / aanwezigheid:

1. Start een onderzoek binnen de (vitale) ICT infrastructuur op de aanwezigheid van malware, onduidelijke systeemrechten en/of back-doors in hard- en/of software.
   - Monitor het interne netwerkverkeer (IDS, HIDS) en update deze met actuele zero-day informatie.
   - Monitor al het in en vooral ook al het uitgaande netwerkverkeer op het lekken van informatie.
     - Controleer al het uitgaande verkeer. Vooral (versleuteld) uitgaand verkeer en verkeer dat afwijkt van de protocolstandaarden en/of plaatsvindt via bijzondere routes, poorten en bestemmingen. Log en monitor alle dns-verkeer (vooral op out-of-band requests).
     - Log de authenticaties (applicaties, services, directory services, single sign on diensten) en bewaar de log's op een extra afgeschermde locatie.
   - Monitor de eigen inter- en intranet services (waaronder (web)mail). Deze worden vaak gebruikt als APT-aanvalsvector.
   - Monitor en log de activiteiten binnen de vitale omgeving en detecteer afwijkingen. Controleer (bijvoorbeeld door contentscanning, extra autorisatiemechanismes) elke handeling (logisch, fysiek, transactie, update via USB, et cetera) voordat deze toegestaan wordt in het vitale netwerk.
   - Monitor internet en social media op de publicatie van gevoelige en/of ongewenste bedrijfsinformatie.

2. Incident Response:
   - Richt een toegewijd SIC / SoC (security intelligence (operational) centre) en/of een CSIRT (APT) team op dat autonoom en met de juiste bevoegdheden en middelen kan optreden in geval van een APT-incident. Zorg dat dit team zo klein mogelijk is en goede directe contacten heeft met het hoger management. Zorg dat dit team ook de juiste managementtaal kan spreken en dat het management dit team vertrouwd en erkent.
   - Stel een responseplan op voor incidenten en calamiteiten en test deze regelmatig. Ondanks preventieve en detective maatregelen zijn systemen binnen de organisatie al besmet of wordt de organisatie een keer succesvol aangevallen.
   - Implementeer een '*defense-in-depth-*' en repressie strategie. Hoe meer lagen in de verdediging, des te meer mogelijkheden en tijd men krijgt voor detectie en interventie. Door elke laag anders in te richten (met onder andere techniek) vereist het breken ervan specifieke kennis en tijd.
   - Ken je omgeving, weet waarvoor de verschillende IT-systemen normaal (normale gebruikspatroon) gebruikt worden en welke systemen er beschikbaar zijn om eventuele aanvallers in hun bewegingsvrijheid te beperken.

3. Infrastructuur en techniek.
   - Blokkeer toegang van vreemde devices (zoals usb, nic en wifi) tot de infrastructuur en sta alleen het uitvoeren van bekende programmatuur toe (whitelisting). Installeer geen onnodige of onveilige services en/of programma's.
   - Segmenteer de infrastructuur (ook het beheernetwerk).
     - Ontkoppel de infrastructuur met gevoelige informatie en/of vitale processen en de omgevingen met internettoegang. Indien er toch een internetverbinding gewenst is, gebruik dan een combinatie van technieken als proxy's, applicatie-middleware, datadiodes, firewalls, ids, monitoring, whitelisting en encryptie, et cetera.
     - Concentreer niet alle gevoelige informatie, maar versleutel en verspreid deze over verschillende segmenten en systemen. Installeer o.a. crypto-containers per afdeling voor de opslag (en versleuteling) van gevoelige informatie.
     - Ga niet naar internet met eindgebruiker middelen (pc, tablets, telefoon,..) waarmee ook toegang wordt verkregen met gevoelige informatie en/of vitale processen. Zet mobiele apparatuur uit binnen de vitale segmenten en bij vergaderingen.
     - Gebruik andere inloggegevens in de segmenten met toegang tot het internet, tot de beheersomgevingen en binnen de vitale omgeving. Beperk het aantal gebruikers met toegang tot administratorprivileges en /of vitale informatie en omgeving. Beperk daarbij alleen de toegang tot op dat moment noodzakelijke informatie en monitor de handelingen. Verander de standaard beheerdernamen en -wachtoorden. Gebruik geen privileged accounts op systemen welke niet 100% te vertrouwen zijn. (aanloggen met account op een werkplek van een besmet systeem is een garantie om (de admin) credentials te verliezen.
     - Beperk toegang van leveranciers tot de vitale omgeving. Verleen alleen toegang tijdens correctief en preventief onderhoud en controleer ook de uitgevoerde handelingen.
   - Denk na over het gebruik van standaardoplossingen en inrichtingsmodellen bij het inrichten van de vitale omgeving. (Standaardoplossingen zijn bekend en zijn daardoor een bekende aanvalsvector).

4. Governance

- Maak gebruik van een risicomanagementmethode als iso27005 en normen als iso27001/2 (ISA99 voor de procesindustrie (ICS)). Herhaal periodiek (minimaal één keer per jaar) de analyse van de risico's en test regelmatig de effectiviteit van de genomen maatregelen (vooral de patch, back-up & restore), incidentrespons en de continuïteitsmaatregelen).
- Onderzoek welke informatie voor aanvallers van waarde kunnen zijn. Ook die van de organisatie bij klanten, leveranciers en ketenpartners. Focus (voor APT) op reële dreigingen die van toepassing zijn op de echt relevante waardevolle 'assets' (waaronder informatie). Maak van elk vitaal component (apparaat, informatie, object, persoon) een risicoprofiel en introduceer de benodigde (risicocompenserende) maatregelen.
- Zorg voor een vergaande awarenesstrainingen met daarin een uitleg over de vitale infrastructuur, beveiligen van informatie, risico's, kwetsbaarheden, het herkennen van onregelmatigheden en de daarbij gewenste reactie.
- Update (patch) zo snel mogelijk de componenten binnen de (vitale) omgevingen.

Additionele maatregelen:

- Implementeer een SIEM (Security Incident and Event Management) omgeving. Hiermee kunnen trendanalyses, doelmatigheidstudies van de maatregelen en voortijdige detectie van aanvallen worden gedaan.
- Wantrouw elk (mobiele) apparaat (pc, USB-stick, telefoon, IPad) dat onbeheerd is gelaten, is afgegeven aan derden en/of aangesloten is geweest op een niet vertrouwd netwerk. Vervang en/of formatteer deze bij twijfel. Wis onnodige informatie op deze devices bij buitenlandse reizen en/of gebruik hiervoor aparte apparaten.
- Controleer periodiek de aanwezigheid van ongewenste (fysieke en logische) componenten en autorisaties binnen de infrastructuur. Controleer regulier de normale werking en configuratie van de aanwezige assets (fysieke, logische en beveiligingscomponenten) binnen de infrastructuur. Herinstalleer deze bij twijfel.
- Doe onderzoek naar de businessmodellen en werkwijzen (aanvalmethodes) van de aanvaller. Begrijp welke informatie uit de eigen organisatie waardevol kan zijn voor de aanvaller. Kijk hierbij niet alleen naar of de informatie waardevol is voor de eigen organisatie, maar ook of het bijvoorbeeld waardevol voor een derde partij kan zijn als deze informatie niet meer toegankelijk is. Als men weet wat de motieven zijn van een aanvaller, kan men ook bepalen of de eigen informatie / infrastructuur een relevant doelwit kan zijn. Pas hier de detectie strategie op aan.
- Pas data-masquerade-technieken toe (op databases, bestanden en honeypots) om aanvallen op vitale componenten en informatie op te vangen (pareren) en te detecteren.

Bronnen:

- Australian Government Defence Signals Directorate's 35 mitigating strategies, http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm
- 20 Critical Security Controls, SANS, http://www.sans.org/critical-security-controls/
- Beveiligingsrisico's van online SCADA-systemen , https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/beveiligingsrisicos.html
- Checklist beveiliging van ICS/SCADA-systemen, https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/checklist-beveiliging-van-ics-scada-systemen.html
- In dept detecting APT network traffic: http://www.trendmicro.com/cloud-co ntent/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf
- Spionage en Kwetsbaarheidsanalyse Spionage: https://www.aivd.nl/onderwerpen-0/spionage-0/

Gezamenlijke uitgave van
Nationaal Cyber Security Centrum en de AIVD met medewerking van de MSP- en de multinational ISAC.
Postbus 117 | 2501 CC Den Haag
Publicatienr: FS2013-02c
www.ncsc.nl