Algemene Inlichtingen- en Veiligheidsdienst
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Hoe herkent u een aanval vanuit een Advanced Persistent Threat?

En hoe kan deze informatie gebruikt worden in een detectie- en monitoringsoplossing?

Voorwoord

Tegenwoordig is er nauwelijks een werksituatie voor te stellen zonder computers en internet. Veel bedrijfsprocessen zijn geautomatiseerd, er is veel uitwisseling van informatie waarbij er vele koppelingen met de buitenwereld zijn. Omdat dit risico's met zich meebrengt op het gebied van beveiliging zijn bij veel organisaties al preventieve maatregelen geïmplementeerd. Firewalls, antivirusoplossingen en versleutelde harde schijven en USB-sticks zijn hier voorbeelden van.

Lange tijd leek deze preventieve aanpak afdoende om hackers of andere kwaadwillenden buiten te houden. Maar tegenwoordig volstaat het niet meer om bijvoorbeeld enkel een Demilitarized Zone (DMZ) te implementeren. Hiervoor zijn twee redenen aan te wijzen.

De eerste reden is de verandering van het dreigingsbeeld door bedrijfsspionage en aanvallen door onder andere georganiseerde misdaad, terreurgroepen en diverse buitenlandse inlichtingendiensten. Deze groepen vormen een dreiging die ook wel bekend staat als Advanced Persistent Threat (APT). Ze beschikken over voldoende geld, middelen en tijd om een aanval met geavanceerde middelen uit te voeren en kunnen deze gedurende een langere periode vol houden.

Ten tweede maken de keuzes van de wijze waarop technologische wijzigingen worden geadopteerd, aanpassingen nodig aan de huidige architectuur. Daarmee worden ook nieuwe risico's geïntroduceerd. Voorbeelden van technologische wijzigingen zijn: samenwerkingsplatformen die toegankelijk moeten zijn voor derden, plaats- en tijdonafhankelijk werken, cloud-oplossingen en 'Bring Your Own Device' (BYOD). Deze aanpassingen introduceren nieuwe risico's die niet afgedekt kunnen worden met slechts preventieve maatregelen. Hierdoor kunnen dreigingsactoren in verschillende gevallen onopgemerkt hun gang gaan. Dit zorgt voor een afbrokkeling van het huidige 'corporate netwerk' en het zogeheten 'system high model' (waarbij het merendeel van de beveiligingsmaatregelen aan de rand(en) van het netwerk of het informatie systeem worden toegepast). Dit vraagt om de vervolgstap om naast preventieve maatregelen en een incidentresponsproces ook **detectie en monitoring** toe te passen binnen de informatiebeveiliging. Deze vervolgstap is tevens zichtbaar in de visie van de Nederlandse overheid zoals deze te vinden is in de Nationale Cybersecurity Strategie 2.

De doelgroep van dit whitepaper laat zich omschrijven als functionarissen die zich op tactisch niveau bezighouden met informatiebeveiliging. Dat zijn onder meer Chief Information Security Officers, Information Security Officers, managers van Security Operation Centers (SOC), Architecten en Technical leads van een SOC binnen de Rijksoverheid.

Het doel van dit whitepaper is enerzijds een **algemeen beeld** te schetsen rondom de specifieke **kenmerken** (de Indicators Of Compromise, IOC) van een aanval vanuit een Advanced Persistent Threat. Anderzijds is het doel **bewustwording** over APT's te creëren bij de doelgroep van dit whitepaper.

Deze informatie kan gebruikt worden om detectie- en monitoringoplossingen zoals een Security Information & Event Management Systeem (SIEM) in te richten en te optimaliseren. Dit document kan gebruikt worden ter aanvulling op §3.3 uit het rapport 'Verhogen weerbaarheid tegen digitale spionage door statelijke actoren' [1] van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) waarin enkele adviezen voor detectie en monitoring worden gegeven.

Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD geeft advies over veilige verwerking van overheidsgegevens, preventieve en onderzoeksmaatregelen en ondersteunt met behulp van input voor risicoanalyses voor de gehele organisatie-infrastructuur. Op basis van de inventarisatie en de risicoanalyse die de organisatie zelf uitvoert, kan de organisatie vervolgens beveiligingsmaatregelen nemen. Wanneer een overheidsorganisatie zijn weerbaarheid tegen APT's wil vergroten, dan is de AIVD graag bereid hierin te adviseren.

Inhoud

1 APT en IOC's

Advanced Persistent Threat, hierna APT, is een verzamelnaam voor dreiging door een groep aanvallers die niet alleen over geavanceerde technische middelen en voldoende geld beschikt, maar ook een sterke motivatie heeft om bedrijfsgeheimen of gerubriceerde (staatsgeheime) informatie te bemachtigen. Door deze bijzondere positie en werkwijze is het gebruik van slechts preventieve maatregelen niet meer afdoende.

Een **Indicator of Compromise** is, simpel gezegd, een forensisch kenmerk of spoor van een inbraak dat ter identificatie gebruikt kan worden op een host of netwerk. Dergelijke IOC's kunnen worden verwerkt in *signatures* of patronen die gebruikt kunnen worden in Intrusion Detection Systemen of in een Security Information and Event Management (SIEM) ter correlatie.

1.1 Wat werkt onvoldoende?

Een aantal zaken biedt onvoldoende bescherming.

De traditionele manier van beveiligen waarbij de focus voornamelijk op preventie ligt.
Veel informatiesystemen hebben bekende, maar ook onbekende kwetsbaarheden, ook wel *zero day exploits* genoemd. Deze kwetsbaarheden worden door aanvallers misbruikt om ongemerkt door de preventieve beveiliging heen te komen.

Wat is een APT precies?

Bij dreiging door een APT wordt er vanuit gegaan dat de dreigingsactor beschikt over:
- een specifiek doel;
- bovengemiddelde hoeveelheid geld;
- uitgebreide en/of unieke kennis en technische middelen.

In verschillende gevallen is de groepering achter een APT ook in de positie om een aanval over een langere periode uit te spreiden zodat er minder kans is om gedetecteerd te worden.
Bij de bovenstaande punten kunt u denken aan de in de BIR uitgesloten groepen:
- inlichtingendiensten;
- georganiseerde criminaliteit;
- terreurgroepen.

Hoewel het in eerste instantie kan lijken dat uw organisatie niet direct doelwit zal zijn van een APT, is het raadzaam altijd alert te blijven op veranderingen in economische situaties en geopolitieke spanningen, en de technologische voortuitgang te monitoren. Veranderingen hierin kunnen mogelijk consequenties voor de organisatie hebben.

In onder andere het Cybersecuritybeeld Nederland (CSBN-4) is te lezen dat er potentie is vanuit geheime diensten en overheden om digitale spionage uit te voeren en dat diverse commerciële partijen 'backdoors' hebben ingebouwd in hun soft- en hardware. Dergelijke informatie bevestigt dat rekening gehouden moet worden met dreigingen vanuit deze partijen.

De belangen van uw organisatie kunnen wel degelijk interessant zijn voor partijen waar APT-dreiging van uitgaat. In dat geval is het des te meer van belang dat de informatiebeveiliging daar weerstand tegen biedt.

Daarnaast is er nog de menselijke factor, die (meestal onbedoeld) een succesvolle aanval mogelijk kan maken. Denk hierbij aan *social engineering*-tactieken zoals *pretexting* (door een leugen van de hacker het slachtoffer iets te laten uitvoeren), *spear phishing* (gerichte phishing-mails) en *baiting* (rondstrooien van USB-sticks met malware op parkeerplaatsen). Maar ook de natuurlijke neiging van de mens om omwegen te zoeken om de 'beperkingen' van security te omzeilen, zoals het plaatsen van documenten op *Dropbox* wanneer USB poorten geblokkeerd zijn, kan een risico zijn. Dit wil niet zeggen dat preventieve maatregelen overbodig zijn. Integendeel, preventie in combinatie met detectie en monitoring dekt een groter geheel aan risico's af en vult elkaar waar nodig aan.

Traditionele manier van detectie: signatures en network based detection.
Een aanvaller achter een APT zal, voorafgaand aan het uitvoeren van een aanval, zijn werkwijze testen tegen verschillende detectiemechanismen om zo vooraf de kansen op detectie in te schatten. De aanvaller kan een complete testomgeving opstellen, waarin verschillende scenario's kunnen worden getest. Bekende signatures zijn zodoende niet altijd of onvoldoende effectief.

Steeds vaker wordt bij geavanceerde aanvallen 'end to end'-encryptie toegepast. Hierbij wordt malware als versleutelde data meegestuurd met het netwerkverkeer waardoor een signature niet wordt herkend. Hierdoor valt een (groot) gat in de beveiliging.

Het dichten van bekende kwetsbaarheden en zero days.
Aanvallers achter een APT beschikken, volgens de definitie die wij hanteren, over geld en uitgebreide kennis. Ook is zeker dat deze groep aanvallers beschikt over nieuwe aanvalstechnieken en kennis heeft van nog niet bekende kwetsbaarheden in systemen. Er is immers voldoende geld om *zero day exploits* te (laten) ontwikkelen.

1.2 Wat kan mogelijk wel werken?

Om weerstand te bieden tegen een APT moet een organisatie naast een gedegen bewustwording omtrent informatiebeveiliging bij de medewerkers, een aantal stadia doorlopen. Deze stadia staan hieronder opgesomd, en worden verdiept in *hoofdstuk 2 -Hoe kunnen IOC's gedetecteerd worden?*

1. *Een organisatie moet een gedegen risico- en dreigingsanalyse (laten) uitvoeren voordat gestart wordt met implementatie van oplossingen voor detectie en monitoring.*

Allereerst is het belangrijk om te weten wat de 'kroonjuwelen' van de organisatie zijn. Welke assets zijn belangrijk? Daarna kunnen de risico´s binnen de organisatie-infrastructuur in kaart gebracht worden aan de hand van een risicoanalyse. Hierbij kunnen om risicoanalysemethodieken te gebruiken zoals IRAM, of een Security Assurance Analysis Method, ook wel SAAM analyse, waarbij het NBV ondersteunt. Vervolgens moet de organisatie onderzoeken welke dreigingen zich kunnen voordoen, voor zover dit niet al in de risicoanalysemethodiek besproken is.

2. *Een organisatie moet in staat zijn om op een uitgebreide manier detectie uit te voeren.*

Wij raden aan om naast detectie op netwerkniveau (NB-IDS) ook detectie op host- (HB-IDS) of zelfs op applicatieniveau (bijvoorbeeld de OWASP app sensor [3]) uit te voeren.
Daarnaast adviseren wij om ook andere informatie als context te gebruiken bij het detecteren van een aanval. Hierbij kan gedacht worden aan logfiles en configuratiefiles, maar ook aan proces- en organisatie-informatie en de beschikbare informatie van derden (threat intelligence platformen).

3. *Een organisatie moet in staat zijn om detectieresultaten en events te onderzoeken en te correleren.*

Het analyseren en onderzoeken van de resultaten en het verder optimaliseren van detectiemechanismen vereist vergaande specialistische (technische) kennis. Deze kennis is op dit moment (volgens diverse commerciële bedrijven zoals Cisco) erg schaars op de arbeidsmarkt. Uit onderzoek van consultancybureau Noordbeek, uitgevoerd in opdracht van de Rijksoverheid, blijkt dat deze kennis ook binnen de Rijksoverheid schaars is.

Naast technische kennis moet de organisatie ook over voldoende kennis beschikken op het gebied van bedrijfsvoering, processen en de organisatie zelf. Alleen de gecombineerde kennis over deze gebieden maakt het mogelijk resultaten vergaand te correleren en te prioriteren. Combineert of correleert een organisatie deze informatie niet of onvoldoende, dan is er grote kans dat bepaalde indicatoren over het hoofd worden gezien of worden gemist door de grote hoeveelheid data en verkleint dit de kans op het detecteren van een gerichte aanval.

Verder moet rekening gehouden worden met het feit dat het implementeren van een gedegen correlatiemethode een langdurig en zelfs oneindig proces is, waarbij de technische- en bedrijfsprocessen, maar ook de correlaties continu verfijnd en gecorrigeerd moeten worden om hun werking te effectueren. Een aanvalswijze wordt immers ook steeds gewijzigd.

Daarnaast is het van belang dat al het 'bewijs' gelogd en bewaard wordt. Een voorbeeld. Een spamfilter dat phishing- en spearphishing-mails correct detecteert, filtert en deze vervolgens weggooit, zorgt door de ontbrekende mail dat nader forensisch onderzoek om de aanval uit te zoeken en vast te leggen niet mogelijk is.

4. Een organisatie moet in staat zijn de resultaten van het onderzoek te vertalen naar nieuwe IOC's.

Het kunnen analyseren van resultaten voortkomend uit de monitoringactiviteiten, zoals *false positives*, stelt een organisatie beter in staat bekend regulier verkeer of patronen te herkennen en deze te onderscheiden van onbekend, kwaadaardig verkeer of patronen. Met andere woorden, maak gebruik van het lerend vermogen van een organisatie.
Een andere effectieve manier om van nieuwe IOC's te identificeren is het uitvoeren van een *pen-test* of een *red teaming-test*. De uitkomsten van dergelijke tests kunnen niet alleen worden gebruikt om gaten te dichten en nieuwe maatregelen te treffen. Ze kunnen ook worden gebruikt om potentiële compromittaties voor de organisatie te herkennen en deze verder uit te werken in passende detectiemaatregelen en correlatieregels. Werkwijzen van zogeheten *ethical hackers* kunnen ook een IOC-patroon of signature opleveren.

5. Een organisatie moet in staat zijn om threat intelligence te verzamelen en te delen.

Het valt aan te bevelen op dit vlak samenwerking te zoeken. Er zijn diverse platformen, zoals Information Sharing and Analysis Centers (ISAC) en het Malware Information Sharing Platform (MISP), die informatie delen over *threats* of dreigingen die binnen een specifieke sector bekend zijn. Een optie is om aan te sluiten op het Nationale Detectie Netwerk (NDN) en op deze wijze gebruik te maken van unieke kennis op het gebied van gebruikte malware, aanvallen, aanvalsmethoden, spionage mogelijkheden enzovoort.

2 Hoe kunnen IOC's gedetecteerd worden?

Waar nu gericht met 'kleine visnetten met grote mazen' op digitale inbrekers wordt gevist, kunnen veelgebruikte technieken van vrij verkrijgbare malware en hacktools worden herkend.

Zoals gezegd is een APT gebaseerd op het gebruik van (nog) onbekende technieken en zwakheden van zowel gebruikers als gebruikerssystemen zodat een aanvaller door de figuurlijke mazen in de visnetten kan zwemmen.

Dit hoofdstuk beschrijft een methode om juist het hele visgebied in kaart te brengen en een groot visnet uit te zetten met fijne mazen. Deze maatregelen vergroten de kans dat er meer dan alleen *script kiddies* gevangen worden en verkleinen de kans dat een geavanceerde aanval tussen de geïmplementeerde informatiebeveiligingsmaatregelen door glipt.

De nadruk ligt, zoals in het vorige hoofdstuk al aan bod kwam, op het waarnemen van ongebruikelijke patronen die kunnen worden afgeleid uit verschillende informatiebronnen. Deze manier van detectie wordt ook wel *anomaly detection* genoemd. In dit hoofdstuk gaan we hier verder op in.

2.1 IOC's in de praktijk

Het waarnemen van ongebruikelijke patronen en het opbouwen van intelligentie rondom wat gebruikelijke en wat ongebruikelijke signalen zijn, is essentieel bij het detecteren van aanvallen vanuit een APT.
Het gaat hierbij niet om slechts technische signalen. Een IOC kan ook worden gevonden in de vertaling van de reguliere bedrijfsvoering naar techniek, zoals geautomatiseerde bedrijfsprocessen.

Aanvalsstadia

Met betrekking tot detectie is het belangrijk de verschillende stadia van een aanval te kennen, dan wel te herkennen

De aanvalsstadia kunnen worden onderverdeeld in de vaak gebruikte 5 P's. Deze 5 P's worden bijvoorbeeld door NOREA (de beroepsorganisatie voor IT-Auditors) [2] gebruikt. Er zijn nog tal van andere modellen en variaties, maar in dit whitepaper is gekozen voor de 5 P's.

- Probing, *het onderzoeken en vergaren van informatie rondom een target.*
- Penetrate, *het aanvallen van een target.*
- Persist, *na een succesvolle aanval zorgt de aanvaller voor een manier om eventueel later terug te kunnen komen.*
- Propagate, *het verder onderzoeken van het systeem en netwerksegment waarin de aanvaller zich bevindt met als einddoel: het vinden van het werkelijke doelwit.*
- Paralyze, *het daadwerkelijk stelen van informatie en het onklaar maken van systemen.*

In de praktijk zullen veelal de eerste vier stappen elkaar een paar keer afwisselen ('permutation'). Bijvoorbeeld een aanvaller die verschillende netwerk-segmenten (denk aan een DMZ) door moet om bij zijn doel te komen. Ook ontbreekt er nog een laatste fase waarin een aanvaller probeert zijn sporen te wissen ('purge'). Deze acties zouden ook aangewezen kunnen worden als IOC.

Onderstaand wordt een eenvoudig voorbeeld geschetst van een werkproces om een gestructureerd beeld van stappen in systemen weer te geven.

Voorbeeld: facturatieproces
In een facturatieproces zijn verschillende systemen betrokken die in een bepaalde volgorde bepaalde acties verrichten op weg naar de afhandeling.

1. Per order wordt standaard een ticket aangemaakt in een werkvoorraadsysteem.
2. Het nummer op de order komt overeen met het nummer op de factuur.
3. Het doorzetten van de order kan alleen worden goedgekeurd door iemand anders dan de maker van de order (vier ogen principe).
4. Facturen worden altijd op vrijdagmiddag verzonden vanuit het SAP systeem.

Wanneer een factuur per e-mail wordt verzonden op een donderdag, is dit als los feit niet vreemd. Pas in vergelijking met het werkproces kan dit gezien worden als afwijking van normaal gedrag. Dit kan mogelijk duiden op een onschuldige gebruikersfout of systeemfout, maar ook op een opzettelijke fout zoals fraude of zelfs een IOC van een (APT-)aanval zijn.

Het voorbeeld laat twee dingen zien:
- Bedrijfsprocessen en informatie-bewegingen moeten in kaart worden gebracht om normaal gedrag te definiëren,
- Bij een afwijking is nader onderzoek nodig om achtergrondinformatie, context en beweegredenen te verzamelen.

Bij het detecteren van aanvallen vanuit een APT is het in dit voorbeeld van belang om de signalen van systemen die bij de facturatie betrokken zijn, te verzamelen en te correleren zodat hier controle op uitgevoerd kan worden. Wanneer u dit doet, bent u in staat om ongebruikelijke patronen te herkennen (een uitgebreide manier van anomaly detection). De praktijk wijst echter uit dat veel organisaties slechts beperkt inzicht hebben in wat bekende reguliere patronen zijn en wat afwijkend is.

Het is al bijzonder moeilijk om te weten welke applicaties en onderliggende processen draaien op een smartphone, laat staan in een complete bedrijfs- en IT infrastructuur. Een organisatie moet proberen in kaart te brengen wat normaal en abnormaal gedrag is. Voer een risicoanalyse uit of laat het NBV een SAAM-analyse uitvoeren, om de infrastructuur, risico's en zwakheden in kaart te brengen. Hierdoor wordt inzage gecreëerd zodat het gemakkelijker is te anticiperen op dreigingen.

Als we kijken naar de publiekelijk bekende APT-aanvallen, dan wordt het tot nu toe geschetste beeld bevestigd.

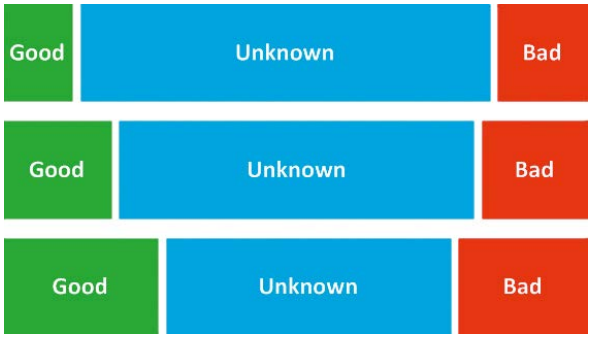
Bij de Belgacom-hack [4] in september 2013 was het CPU-[7]verbruik 's nachts extreem hoog. Nu valt CPU-verbruik op zichzelf niet onder de belangrijkste assets, maar het was in dit geval overduidelijk één van de Indicators of Compromise.

Van de MASK of Careto-hack [5] zijn wereldwijd vele overheidsinstanties, energiecentrales, olieraffinaderijen, ambassades en dergelijke slachtoffer geworden. De hackers slaagden erin bestanden van onder meer het antivirusprogramma te wijzigen zodat zij 5 jaar lang onopgemerkt hun gang konden gaan. Als deze wijzigingen waren gelogd en vergeleken zouden zijn met tijden van de automatische updates van het antivirusprogramma, dan hadden de beheerders kunnen zien dat er ongeautoriseerde wijzigingen hadden plaatsgevonden. Zij hadden dan op basis hiervan onderzoek kunnen uitvoeren.

Net als in het voorbeeld van het facturatieproces geven deze indicatoren op zichzelf geen duidelijke aanval aan, maar kunnen ze wel als signaal dienen om nader onderzoek uit te voeren.

2.2 Verminder de ruis

Er zijn patronen waarvan een organisatie weet dat deze regulier zijn ('GOOD'). Ook zijn er patronen waarvan bekend is dat, als ze waargenomen worden, er iets aan de hand is ('BAD'). Denk bij dit laatste aan bijvoorbeeld de patronen zoals ze zijn opgenomen in de signatures van een IDS en zoals in de hier boven beschreven *anomalies*/patronen. Maar vooral zijn er heel veel signalen en patronen waarvan een organisatie niet precies weet waarvoor deze gebruikt worden ('UNKNOWN').
Door de kennis van GOOD en BAD te vergroten en dus de groep UNKNOWN te verkleinen, wordt de ruis verminderd met als gevolg: effectievere detectie van niet-reguliere patronen (potentiële IOC's dus!).



Figuur 1. Verminder de ruis

2.3 Zelflerend vermogen

Er is een methode om meer inzicht te krijgen in waar u als organisatie nu staat en waardoor meer inzicht verkregen kan worden in BAD–patronen. U kunt daarvoor een aantal penetratietesten (pen-testen) en red teaming-opdrachten uitvoeren of uit laten voeren waarbij per test de verschillende fases van de 5 P's (zie *aanvalsstadia* op pagina 6) doorlopen worden.

Dit geeft u inzicht in:
- hoe effectief de monitoring in de huidige situatie is;
- welke acties van de pen-testers niet werden gezien en waarom niet;
- welke acties van pen-testers u wel had kunnen zien, maar nog niet werden gemonitord of nog niet waren geïdentificeerd als IOC;
- welke signalen er nu gecorreleerd moeten worden om een bepaalde aanval wel te kunnen waarnemen.

Uw Security Operations Center (SOC) kan ook een *Honey-net* inrichten om aanvals-technieken te observeren. Een Honey-net is een omgeving die bewust kwetsbaar is ingeregeld om aanvallers en hun malware te lokken. Analyse van het gedrag van de hackers kan inzage geven in de aanpak en tactieken, wat weer verwerkt kan worden in IOC's.

2.4 Waar te beginnen als het gaat om IOC's?

Het is zinvol om een aantal aanvalsmethodes en bijbehorende kenmerken (IOC's) te formuleren voor uw organisatie. Deze scenario's kunnen vervolgens in relatie worden gebracht met de systemen die binnen de organisatie gebruikt worden.

Denk aan bijvoorbeeld *Probing*, het verzamelen van informatie voorafgaand aan een aanval.
- Worden er social engineering-aanvallen waargenomen (denk aan bijvoorbeeld verdachte e-mails)?
- Is de bedrijfswebsite buiten de 'normale' patronen bezocht?
- Zijn op het netwerk of op de poorten scans uitgevoerd (gericht op specifieke componenten)? Zijn deze scans anders van aard dan wanneer ze in een reguliere situatie plaatsvinden?

Als het specifiek gaat om probing, dan zijn dit voorbeelden van informatiebronnen.

- Webserver logfiles.
- Firewall logfiles.
- Logfiles van authenticatiesystemen.
- Spam en (spear-)phishingmeldingen (*Verizon rapport van 2014 laat zien dat spearphishing voor 81% van de succesvolle cyberspionageaanvallen zorgt [6]*).
- Incidentmeldingen bij een Security Officer. (*Zijn er USB-sticks op het terrein gevonden? Wellicht is iemand bezig met aanvalsfase 'Penetrating'?)*
- Gebruik van bepaalde systemen of resources op ongebruikelijke tijden of op een ongebruikelijke manier.
- IRC-en p2p-verbindingen die in het netwerk worden opgezet. (Propagate of Paralyze, *afhankelijk van het doel van de p2p-verbinding; verspreiding malware of opzetten verbinding om informatie naar buiten te krijgen.*)
- DNS Responses met een (extreem) lage Time To Live (TTL) (fast flux services).
- Meldingen uit HB-IDS, NB-IDS, firewall logs, Applicatie Based-IDS, enzovoort.
- Syslog- en SNMP-informatie.
- Wijzigingen in configuraties, wijzigingen in signature files.

En correleer het gedrag. Een voorbeeld:

- Hebben er recent phishingaanvallen plaatsgevonden?
- Zijn er logfiles gewist, zijn zonder aankondiging aanpassingen aan configuraties waargenomen? (Paralyze)
- Worden grote hoeveelheden data naar het internet verzonden?
- Is het CPU-gebruik hoog op een tijdstip dat ruim buiten de werktijden ligt?

Wanneer deze zaken zich binnen een bepaalde periode of in een bekend patroon voordoen, dan is dit mogelijk al voldoende aanleiding om nader onderzoek in te stellen.

2.5 GOOD-patronen voor context

Een aanpak zou kunnen zijn om gebruikers, systemen en processen te 'profilen' en zo een dossier met 'normaal' gedrag op te stellen en context te documenteren.

Bijvoorbeeld:

- Gebruiker A heeft toegang tot diverse systemen, maar gebruikt hoofdzakelijk systeem 1.
- Gebruiker A gaat op vakantie van 1 augustus tot 1 september.
- Gebruiker A werkt van 9 tot 5 en gaat altijd lunchen om 12 uur.
- Gebruiker A gaat elke dag met een *thin client* met een bepaald nummer, smartphone en tablet het netwerk op.

Wanneer dan tijdens zijn vakantie of na werktijd activiteit plaatsvindt op een van de systemen onder het account van gebruiker A, kan direct een melding worden gemaakt.

Hetzelfde geldt wanneer tijdens lunchtijd een tweede sessie wordt opgestart vanaf de thin client.

Wanneer het voorval een incident blijkt, is onderzoek een stuk makkelijker omdat zichtbaar is dat er een afwijking is geweest van het gebruikelijke, 'normale', gedrag. Op dat moment kunnen de security-analisten besluiten om het incident response-proces in te gaan of dat het gaat om een false positive.

Wanneer verder in deze lijn wordt gedacht wordt zichtbaar dat hiermee, in combinatie met preventieve maatregelen en traditionele signature based detectie, de detectiekans van aanvallen vanuit een APT steeds groter en realistischer wordt.

Samenvatting en conclusie

In dit document heeft u op hoofdlijnen inzicht gekregen in de IOC's waar het gaat om APT's. U heeft inzicht gekregen in waarom de traditionele manier van beveiliging in het algemeen en detectie specifiek onvoldoende werkt tegen deze groep aanvallers. Vervolgens is er aandacht gegeven aan de 5 P's en heeft u inzicht gekregen in wat zou kunnen helpen bij het detecteren van aanvallen vanuit een APT.
Geconstateerd is dat een APT-aanval meestal niet zichtbaar is, enkel een aantal effecten hiervan. Om deze effecten te vertalen naar een IOC is, naast technische kennis, een gedegen kennis nodig van de informatiehuishouding van de organisatie. Om detectie en monitoring op een verantwoorde wijze in te voeren naast bestaande preventieve maatregelen, moet u de huidige detectie- en monitoring-oplossing aan blijven vullen met nieuwe kennis. Doordat daarbij rekening gehouden wordt met dreiging vanuit een APT, vergt dit een goede en zorgvuldige voorbereiding. We adviseren u dan ook te beginnen met de volgende generieke stappen.

1. Bepaal door middel van een risicoanalyse wat de 'kroonjuwelen' van de organisatie zijn en waar deze zich bevinden.

2. Inventariseer de infrastructuur, informatieprocessen en bedrijfsprocessen.

Deze kennis is vaak niet vanzelfsprekend aanwezig binnen een SOC, dat veelal als aanbieder van een service is ingericht.

3. Zorg dat een SOC kennis heeft van de bedrijfsarchitectuur, de informatiearchitectuur en de technische architectuur van het informatiesysteem. Realiseer dit door de systeemeigenaren en informatie-eigenaren te betrekken bij het inrichten van detectie- en monitoring- oplossingen.

Een oplossing kan gevonden worden in een uitgebreide vorm van anomaly detection. Dat is een vorm van detectie waarbij kennis wordt opgebouwd over regulier 'GOOD' en bekende aanvallende 'BAD' patronen en gedrag, zodat afwijkingen kunnen worden waargenomen.

4. Om dit goed te doen moeten informatie en context uit verschillende informatiebronnen worden gecorreleerd. Hoe beter u hier in bent, des te effectiever detectie is als maatregel.

5. Begin klein en bouw rustig uit. Kies een dreiging, een dreigingsactor en een kroonjuweel en loop het mogelijke aanvalspad uit. Welke systemen zijn betrokken? Waar zou een IOC geformuleerd kunnen worden?

Ten slotte is een aantal praktische voorbeelden gegeven hoe u in de praktijk aan de slag kunt gaan met red teaming, threat intelligence-platformen en het inventariseren van normaal gedrag. Detectie en monitoring zal niet HET antwoord op alle problemen zijn en zal ook nooit 100% veiligheid garanderen, maar het verhoogt wel de weerbaarheid van de organisatie.

Met dit whitepaper ondersteunt het NBV, als onderdeel van de AIVD, Rijksoverheidsinstanties om aan de slag te gaan met detectie en monitoring of hun huidige oplossing te verbeteren.

Bronnen

[1] NBV, AIVD - *Verhogen Weerbaarheid tegen digitale spionage door statelijke actoren*. 2e druk, september 2013.

[2] NOREA - *5 P's*. Beschikbaar via http://www.norea.nl/readfile.aspx?ContentID=73197&ObjectID=1018127&Type=1&File=0000038619_Hacking_fact-sheet.pdf (Opgehaald op 2014-08-15)

[3] OWASP - *OWASP app sensor*. Beschikbaar via https://www.owasp.org/index.php/OWASP_AppSensor_Project (Opgehaald op 2014-08-15)

[4] Computing - *Belgacom hack*. Beschikbaar via http://www.computing.co.uk/ctg/news/2306175/gchq-used-fake-linkedin-pages-bearing-malware-to-attack-belgacom (Opgehaald op 2014-08-15)

[5] Kaspersky - *Mask / Careto hack*. Beschikbaar via http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-Uncovers-The-Mask-One-of-the-Most-Advanced-Global-Cyber-espionage-Operations-to-Date-Due-to-the-Complexity-of-the-Toolset-Used-by-the-Attackers (Opgehaald op 2014-08-15)

[6] Verizon -*2014 Data Breach Investigations Report*. Beschikbaar via http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf
(Opgehaald op 2014-10-02)

[7] ZDNet – *Researcher describes ease to detect, derail and exploit NSA's Lawful Interception*. Beschikbaar via http://www.zdnet.com/researcher-discribes-ease-to-detect-derail-and-exploit-nsas-lawful-interception-7000025073/ (Opgehaald op 2014-10-24)

Lijst met afkortingen

AIVD	Algemene Inlichtingen- en Veiligheidsdienst
APT	Advanced Persistent Threat
BIR	Baseline Informatiebeveiliging Rijksdienst
BYOD	Bring Your Own Device
DMZ	Demilitarized Zone
DNS	Domain Name System
HB-IDS	Host Based Intrusion Detection System
IOC	Indicator of Compromise
IRAM	Information Risk Analysis Methodology
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Center
NB-IDS	Network Based Intrusion Detection System
NBV	Nationaal Bureau voor Verbindingsbeveiliging
NCSC	Nationaal Cyber Security Centrum
NOREA	*Beroepsorganisatie van IT-Auditors*
P2P	Peer -to-Peer
SAAM	Security Assurance Analysis Method
SAP	*Leverancier van onder andere commerciële Enterprise Resource Planning (ERP) en Customer Resource Management (CRM) software*
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
TTL	Time to live

Colofon:

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

Postbus 20010, 2500 EA Den Haag

Mei 2015