Welke opties zijn er om cyberaanvallen te weren?

Cyberaanvallen op onze kritieke infrastructuur voor terrorisme, sabotage of commercieel gewin zijn niet hypothetisch meer. Helaas brengt een betere bescherming van de netwerken ook een aanzienlijke toename van de beheerskosten. Sandro Etalle en Marcel Jutte leggen uit wat er kan worden gedaan.

Sandro Etalle | Marcel Jutte

Tot niet zo lang geleden werden cyberaanvallen vooral voor de lol uitgevoerd. Dit is in de laatste paar jaren compleet veranderd. Tegenwoordig wordt een groot deel van cyberaanvallen uitgevoerd voor economisch of politiek gewin door gemotiveerde en goed gefinancierde criminele organisaties, door concurrenten, door cyberterroristen, cyberactivisten en zelfs door de staat gesponsorde overheidsinstanties.

De door een staat gesponsorde Stuxnetworm werd in 2010 gebruikt om het Iraanse nucleaire programma te vertragen. Door velen bestempeld als eerste cyberwapen heeft het brede publieke aandacht gekregen. Maar het is slechts het topje van een snel groeiende ijsberg met grote impact op de gehele industriële branche. Hedendaagse malware wordt veel gebruikt voor het uitvoeren van industriële spionage en sabotage. Voorbeelden van geavanceerde malware zijn Duqu, Flame en niet te vergeten de tools die worden gebruikt door het Red October-netwerk, dat jarenlang onopgemerkt bleef. Frankrijk heeft zelfs de VS beschuldigd Flame in te zetten om het netwerk rondom de president te hacken en te bespioneren.

Steeds meer beleidsmakers maken zich zorgen over de vitale infrastructuur: energie, gas, olie, telecommunicatie, water en de voedselketen. Er is een duidelijke toename van cyberaanvallen binnen deze gebieden, zowel kwantitatief als kwalitatief. In 2009 rapporteerde het Amerikaanse ICS-Cert in zijn Incident Response Summary Report nog elf incidenten. In 2012, slechts drie jaar later, is dat aantal toegenomen tot bijna tweehonderd, een groei van ongeveer tweeduizend procent. Bij het Shamoon-incident van afgelopen augustus werden op dertigduizend pc's van het Saoedi-Arabische oliebedrijf Aramco alle documenten, spreadsheets, e-mails en andere bestanden vervangen door een afbeelding met daarin een brandende Amerikaanse vlag. Volgens de Amerikaanse defensieminister Leon Panetta is dit de meest destructieve aanval op het bedrijfsleven tot nog toe.

Je kunt je afvragen: wat is er zo bijzonder aan deze virussen? Waarom zijn ze zo moeilijk te detecteren? Hadden deze slachtoffers soms hun firewalls en antivirusprogramma's niet op orde? De realiteit is dat geen enkel antivirusprogramma deze aanval had kunnen ontdekken en geen firewall Shamoon had kunnen blokkeren. Dit virus is ontwikkeld om totaal onzichtbaar te zijn voor de huidige beveiligingstechnologieën. Om dit te begrijpen, moeten we kijken naar de manier van werken en de details van de huidige detectietechnologie.

Nooit en te nimmer

Er zijn drie hoofdmethodes om cyberaanvallen te detecteren: *blacklisting*, *whitelisting* en anomaliedetectie. Een vierde methode, het uitvoeren van vermeende malware in een virtuele omgeving, is weliswaar een belangrijke nieuwe ontwikkeling, maar vereist een gespecialiseerde aanpak en is beperkt toepasbaar.

De blacklisting- of signatuurgebaseerde methodiek komt veruit het meeste voor en wordt vooral gebruikt bij de gangbare antivirustools. Deze systemen herkennen een aanval aan de hand van een specifiek patroon. Wat niet wordt herkend als een bedreiging, wordt beschouwd als legitiem. Een blacklist kan daarom alleen bedreigingen detecteren die eerder zijn geanalyseerd of die daar veel overeenkomsten mee hebben.

Per definitie loopt deze methode altijd achter de feiten aan. Malware die een nieuwe onbekende kwetsbaarheid gebruikt, is niet te detecteren, net zomin als goed gemaakte varianten van oude malware-*exploits*. Wanneer een nieuwe bedreiging wordt ontdekt, zal steeds een nieuwe handtekening ontwikkeld en verspreid moeten worden. Dat kan weken of zelfs maanden duren. Stuxnet, Duqu, Flame en Shamoon konden zo allemaal lange tijd hun gang gaan. Stuxnet bijvoorbeeld, dat onder meer vier tot dan toe onbekende kwetsbaarheden gebruikte (zogenaamde *zero day*-kwetsbaarheden), was al zeker een jaar actief voordat het werd opgemerkt.

In het internetdomein heeft blacklisting nut, maar voor de vitale infrastructuur zal deze aanpak nooit en te nimmer voldoende dekking bieden. In dit gebied willen indringers vooral niet in de spotlight staan en zijn de aanvallen vaak gericht op specifieke (besturings)systemen.

Omslachtig en niet ongevaarlijk

Computerwetenschappers werken al meer dan een decennium aan technieken en algoritmes om cyberdreigingen te detecteren die nog niet bekend zijn. Het legitieme dan wel normale netwerkverkeer wordt eerst in kaart gebracht, en bij afwijkend gedrag volgt een melding of wordt bepaald netwerkverkeer zelfs geheel geblokkeerd. Dit vormt de basis onder zowel whitelisting als anomaliedetectie, hoewel de benaderingen in de praktijk heel verschillend zijn.

Anomaliedetectie werkt met het opmerken van 'afwijkend gedrag'. De huidige anomaliedetectiesystemen kijken naar de kwantiteit van het netwerkverkeer. Het idee is dat sommige soorten aanvallen (*denial of service* om te beginnen, maar ook botnets) dusdanig veel netwerkverkeer genereren dat dit kan worden opgemerkt. Deze systemen zijn hooguit een aanvulling op andere detectiemechanismen.

In het verleden is er ook onderzoek gedaan naar *kwalitatieve* detectie van afwijkingen. In de praktijk is het echter nooit succesvol ingezet. Dit is voornamelijk te wijten aan het feit dat er geen manier is gevonden om het aantal loze foutmeldingen binnen te perken te houden.

Whitelisting is een andere aanpak. Dit is het tegenovergestelde van blacklisting: in plaats van een aanval te herkennen, detecteert een whitelisting-systeem juist het legitieme verkeer. De rest wordt geblokkeerd of gerapporteerd. Zo'n oplossing kan zeer effectief zijn, maar de efficiëntie is sterk afhankelijk van de nauwkeurigheid van de onderliggende analyse. Als vuistregel geldt: hoe nauwkeuriger de analyse, hoe groter de kans dat een gerichte aanval wordt gedetecteerd.

Er zijn firewall-achtige oplossingen die controleren of de eindpunten van het netwerkverkeer overeenkomstig de bedoelingen zijn, bijvoorbeeld specifieke combinaties van IP-adressen en TCP-poorten. Dit is een voorbeeld van whitelisting met betrekkelijk lage nauwkeurigheid. Deze oplossingen zijn zeer nuttig als een eerste (zeer belangrijke) beschermlaag, maar kunnen een geavanceerde aanval zeker niet detecteren en stoppen.

Op zijn minst is het echter theoretisch mogelijk om meer geavanceerde en accurate *deep packet whitelisting*-systemen te ontwikkelen. Deze interpreteren en begrijpen het berichtenverkeer; ze kijken dus naar de inhoud van de data. Dit soort whitelisting-oplossingen kan geavanceerde aanvallen wel blokkeren. Zonder de pretentie te hebben om volledig te zijn, zijn er reeds oplossingen op de markt die dit mogelijk maken. Voor industriële controle is er bijvoorbeeld het systeem van Tofino.

Een nadeel van deze whitelisting-oplossingen is dat een hogere nauwkeurigheid hand in hand gaat met hogere beheerskosten. In de eerste plaats moet iemand het systeem gaan 'vertellen' hoe het legitieme netwerkverkeer eruitziet. Dit is meestal een tijdrovende klus. Denk maar aan de tijd die nodig is om thuis een eenvoudige firewall te configureren. Voor een productienetwerk is – pak 'm beet – honderd keer die inspanning nodig.

Als echt accurate (deep packet) whitelisting gewenst of noodzakelijk is, zal naast de gebruikte IP-adressen en poorten ook moeten worden aangeven welke functiecodes zijn toegestaan. Dit betekent opnieuw weer makkelijk honderd keer zo veel werk. Het instellen, opzetten en, niet te vergeten, onderhouden van een dergelijk systeem is voor een complete site vaak onbetaalbaar.

Bovendien moeten de instellingen van het whitelisting-systeem elke keer worden veranderd als de toepassingen in het netwerk wijzigen. Een omslachtige en niet ongevaarlijke klus, zeker als de modificaties worden uitgevoerd door andere medewerkers dan de beheerders van de netwerkapplicaties.

Daarnaast kan er na verloop van tijd een toenemende mismatch ontstaan tussen de whitelisting-regels en het werkelijke netwerkverkeer. Uit de praktijk blijkt namelijk dat veel '*allow*'-regels niet worden verwijderd, uit angst dat er iets misgaat waardoor het (productie)proces wordt verstoord of zelfs stil komt te liggen.

Ei van Columbus

Toch heeft whitelisting wat ons betreft de toekomst. De nieuwe generatie firewalls die bijvoorbeeld Palo Alto aanbiedt, gebruikt geen volledige deep packet-inspectie, maar maakt een analyse die voldoende is om het verkeer van de verschillende applicaties op het netwerk te onderscheiden. Hoewel de meeste gerichte aanvallen hiermee niet kunnen worden geweerd, is dit een belangrijke sprong vooruit in nauwkeurigheid en dus effectiviteit ten opzichte van standaard firewalls. In de toekomst zullen er vergelijkbare oplossingen op de markt verschijnen.

Bij UT-spin-off Securitymatters gebruiken we een alternatieve whitelisting-technologie met een lerend systeem. In de initiële fase analyseert het systeem het netwerkverkeer en genereert het hiermee automatisch de juiste configuratie. Dat beperkt de tijd die nodig is voor het inrichten van de whitelist tot een minimum. Deze oplossing biedt een uiterst nauwkeurige analyse die rekening houdt met de gebruikte protocollen en maakt een whitelist van alle functiecodes in gebruik en van alle legitieme functieparameters. Technisch gezien, is dit de meest nauwkeurige mogelijke analyse zonder naar informatie op hoger niveau te hoeven kijken, zoals timingaspecten en eventcorrelaties. Deze lerende whitelisting is toepasbaar voor de meest uitgebreide configuraties en voor de meest uiteenlopende systemen, zowel in industriële, Scada-, technische en procesomgevingen als ter bescherming van webapplicaties.

Hebben we het ei van Columbus gevonden om ons en onze installaties te beschermen tegen aanvallers? Niet helemaal. Whitelisting, al dan niet zelflerend, heeft ons zonder twijfel een grote sprong voorwaarts gebracht in het opsporen van geavanceerde aanvallen. Het verricht uitstekend werk voor sommige sectoren, maar kan niet alles oplossen. Er zijn omgevingen waar het netwerkverkeer nog te chaotisch is om te worden gecontroleerd met behulp van een scherp mes zoals whitelisting. Met name bij het uitgaande verkeer van backoffices of (– help! – eigen) apparatuur op het internet.

Gebrek aan regelgeving, ongedisciplineerde of onkundige ontwikkelaars en de wens en noodzaak om de dingen simpel te maken, hebben ertoe geleid dat er een communicatiejungle is ontstaan die steeds moeilijker te controleren is. Een omgeving waar kwaadwillenden hun netwerkverkeer maskeren en zich voordoen als iets anders. De ontwikkeling gaat door en we blijven werken aan de '*next-next-generation*' monitoringsystemen.

*Sandro Etalle (*sandro.etalle@secmatters.com*) is hoogleraar aan de Universiteit Twente, hoogleraar en hoofd van de beveiligingsgroep aan de TU Eindhoven en CEO van UT-spin-off Securitymatters (*www.secmatters.com*), dat werkt aan een nieuwe generatie netwerkbeveiligingssystemen. Verder is hij wetenschappelijk directeur van het Eindhovense Instituut voor Bescherming van Systemen en Informatie. Marcel Jutte (*marcel.jutte@hudsoncybertec.com*) heeft ruim vijfentwintig jaar ervaring in industriële controle. Hij bekleedde uiteenlopende functies, van* lead engineer *tot* managing director *voor een groot aantal projecten binnen onder meer de olie- en gasindustrie, defensie en vitale infrastructuur.*

Redactie Pieter Edelman