Waarom DDoS-aanvallen door de procesindustrie serieus genomen moeten worden

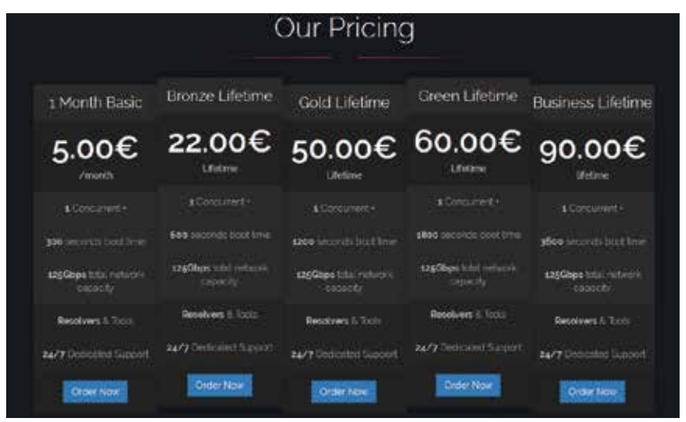
DDoS-aanvallen: kwajongens of echte boeven?

Onlangs werden enkele Nederlandse banken en de Belastingdienst het slachtoffer van DDoS-aanvallen. Men vermoedde dat de Koreanen, of de Russen erachter zaten, maar de dader bleek een 18-jarige puber te zijn die het 'gewoon wel grappig' vond om een aantal instellingen plat te leggen. Dit geval werpt direct de vraag op in hoeverre de procesindustrie bestand is tegen dit soort aanvallen. En wat is dat nou eigenlijk precies, zo'n DDoS-aanval?

Trojans kenden we al, USB-sticks die op parkeerplaatsen liggen gebruiken wij niet, maar DDoS-aanvallen, dat is toch iets nieuws. Of eigenlijk ook niet, want vrijwel iedereen heeft er weleens van gehoord, maar dat het zo simpel zou zijn om zoveel schade te berokkenen, dat is enigszins beangstigend. DDoS-aanvallen beperken zich niet langer tot pesterijtjes, maar worden ook ingezet om grote bedrijven plat te leggen.

Kinderspel

Het opzetten van een eigen DDoS-aanval is kinderlijk eenvoudig. Volgens Marcel Jutte, Managing Director bij Hudson Cybertec, gebruiken cybercriminelen DDoS-aanvallen om meerdere redenen: "Het kan zijn dat een concurrent je tijdelijk buitenspel wilt zetten. Dan ben je door zo'n aanval vaak niet bereikbaar en dat kan bijzonder nadelig zijn bijvoorbeeld tijdens het lanceren van een nieuw product. Aan de andere kant, op het moment dat in het nieuws komt dat bedrijf X het slachtoffer is geworden van een DDoS-aanval, kan dit ook weer een PR-effect hebben."
Een andere, tevens vaak gehoorde reden, is het 'voor de grap' uitvoeren van een DDoS-aanval. "Je kunt voor tien dollar een DDoS-aanval kopen", weet Jutte. "Dat is voor iedere kwaadwillende te doen. Cybercrime at your service dus".



DDoS-aanvallen koop je online net zo makkelijk als een paar nieuwe sokken.

Stepping stone

In principe worden bij DDoS-aanvallen geen gegevens gestolen of gemanipuleerd. Maar dat betekent niet dat een DDoS onschuldig is. Jutte: "Op het moment dat een bedrijf afhankelijk is van het functioneren van een website, bijvoorbeeld omdat klanten daarop moeten kunnen inloggen, kost zo'n DDoS-aanval je gewoonweg een smak geld."
Het kan echter nog een stuk erger. DDoS-aanvallen worden namelijk ook gebruikt als zogenaamde 'stepping stone'. Jutte: "Een DDoS is een ideale tactiek om een andere aanval te verhullen. Op het moment dat je aan de voorkant een website aanvalt met een DDoS, is de complete IT-afdeling in rep en roer om zo snel mogelijk die aanval af te slaan. In de tussentijd maakt de aanvaller gebruik van de verminderde aandacht door aan de achterkant het systeem binnen te dringen. Dat zien we steeds vaker."

Blended Attack

Op het moment dat een DDoS-aanval vergezeld wordt van een ander type aanval, spreekt men van een zogenaamde 'blended attack'. Volgens Jutte komt zo'n combinatie van aanvallen in de praktijk steeds vaker voor. "De DDoS-aanval wordt dan vaak niet alleen gebruikt om de aandacht af te leiden, maar ook om de communicatie zoveel mogelijk plat te leggen. Je kunt met een DDoS het telefoon- en emailverkeer verstoren, waardoor het voor het slachtoffer bijna onmogelijk wordt om de noodzakelijke acties te ondernemen. Vergelijk het maar met scenario's die je wel eens in films ziet: als je een bedrijf wilt binnendringen, is het slim om eerst het brandalarm te laten afgaan. In de paniek die er op volgt, heb je een grotere kans van slagen. Er zijn helaas ook al voldoende echte casussen waarbij een DDoS-aanval wordt gevolgd door een fysieke breach, bij de toegangscontrole dus. Als je er voor zorgt dat de bewaking het te druk heeft met de DDoS-aanval, maak je simpelweg meer kans om langs de controle te kunnen glippen."
Dat wetende, kan je echter ook stellen dat op het moment dat er een DDoS-aanval plaatsvindt, het zaak is dat er niemand door de toegangscontrole wordt gelaten en dat de cyberbeveiliging wordt verscherpt. "Klopt," meent Jutte, "maar dat heeft alles te maken met de mate waarin een organisatie op dit soort gevallen is voorbereid."

Je kunt met een DDoS het telefoon- en emailverkeer verstoren, waardoor het voor het slachtoffer bijna onmogelijk wordt om de noodzakelijke acties te ondernemen...

IT vs OT

Er is een discrepantie tussen de IT- en OT-domeinen. Waar het IT-domein in de regel voorzien is van de meest up-to-date beveiliging, loopt het OT-domein vaak achter. Dat de OT-hardware vaak zomaar tien jaar ouder is dan de IT-hardware binnen hetzelfde bedrijf hoeft nog niet eens het grootste probleem te zijn. "Zulke legacy-systemen kun je op zich nog steeds prima beveiligen," meent Jutte, "mits je de juiste maatregelen treft.
De truc is dat je je netwerk opnieuw configureert en/of segmenteert. Als wij bij een bedrijf aan de slag gaan om de cybersecurity op orde te krijgen, verdelen we het netwerk vaak onder in zogenaamde 'zones' en 'conduits'. Je isoleert dan delen van het systeem die een risico vormen voor je cybersecurity. Veel netwerken zijn twintig, of soms wel dertig jaar geleden opgezet en in de loop van de tijd zijn daar allerlei apparaten aan toegevoegd. In het OT-domein weten ze vaak niet meer precies hoe hun netwerk nu eigenlijk in elkaar zit. Het documenteren van wijzigingen aan het netwerk gebeurt niet altijd en OT'ers hebben vaak te maken met productiechefs die vooral weer 'snel willen kunnen draaien'. Na dertig jaar heb je dus een onoverzichtelijk en potentieel gevaarlijk netwerk. Maar dat kan je prima verhelpen door een assessment uit te laten voeren en maatregelen te treffen. Bijvoorbeeld door te zorgen dat machines met een hoog risico, die onderdeel uitmaken van een productieproces, in een eigen zone geïsoleerd worden en niet direct op internet worden aangesloten."

Mens, Organisatie en Techniek

Volgens Jutte is het echter vooral belangrijk om verder te kijken dan de hardware en software alleen: "Het gaat om de cybersecurity pijlers mens, organisatie en techniek. Alleen als je al die factoren op orde hebt, heb je voldoende kans om je te weren tegen cyberaanvallen. Je kan eindeloos investeren in firewalls, maar als je overal je login en wachtwoord op verschillende devices in je plant hebt geschreven, ben je niet slim bezig. Zo was ik laatst nog bij een bedrijf waar een bepaald apparaat stond met daarop een briefje met inlognaam en password. Dat apparaat en dus ook de inloggegevens werden door zo'n honderdvijftig man gebruikt.
Je kan je voorstellen dat er ook weleens mensen ontevreden zijn, of bij dat bedrijf vertrekken. Met deze algemeen gebruikte inloggegevens wordt het moeilijk de verantwoordelijke op te sporen wanneer er iets gebeurt. Op het moment dat zo'n apparaat ook remote te bedienen is, heb je wel echt een probleem. Je kan nooit meer achterhalen wie er in je systeem is bezig geweest.
Als bedrijf heb je dus duidelijke en strenge voorschriften nodig. En houdt iedereen zich daar ook aan? Is daar controle op? Is je per-

Marcel Jutte

soneel voldoende bewust van de mogelijke gevaren? En hebben ze voldoende kennis in huis? En geldt dat voor iedereen? Zo zijn er nog veel organisaties waarbij slechts één man binnen het OT-domein echt goed op de hoogte is van de gevaren van cybercrime. Maar die ene man is een soort roepende in de woestijn: vaak neemt de IT-afdeling hem totaal niet serieus. Die kloof tussen het IT- en OT-domein zie ik helaas maar al te vaak."

Die IT/OT-kloof is het gevolg van de historie die veel bedrijven zullen herkennen. "De IT-afdeling staat fysiek en hiërarchisch vaak dichterbij de directie dan de OT-afdeling", licht Jutte toe. "IT'ers zijn vaak academici, terwijl de OT'ers techneuten zijn. Dat zijn dus twee totaal verschillende culturen. Die OT'ers komen eigenlijk te weinig bij de directie in de buurt om hun punt te kunnen maken."

Instrumentatie en IoT

Een vaak gehoorde misvatting is dat voor een succesvolle hack van het OT-domein altijd eerst het IT-domein gehackt dient te worden. "Absoluut niet", benadrukt Jutte. "Je kunt los van het IT-domein prima een OT-domein hacken. Dat wordt alleen maar makkelijker met de huidige hyperconnectivity die we overal zien. Noem het Internet of Things, of wat dan ook, op het moment dat je allerlei IoT en/of OT-apparaten aan elkaar knoopt, bijvoorbeeld met smart devices met een wifi-module of een webserver, creëer je een mogelijkheid om van buitenaf dat apparaat te benaderen." Het omgekeerde van wat velen nu denken, is daardoor mogelijk geworden: niet alleen kun je zonder het IT-domein te hacken bij het OT-domein komen, maar ook ziet Jutte steeds vaker dat hackers via het OT-domein in het IT-domein weten in te breken. "Dit soort smart devices zullen we in de toekomst alleen maar vaker

tegenkomen", denkt Jutte. "En ook daarvoor geldt: laat een assessment uitvoeren."

Risicoprofiel

Een assessment, zoals Jutte met regelmaat voor zijn klanten uitvoert, geeft de klant een goede kijk op de huidige staat van cybersecurity. Een nulmeting, kan je het noemen. En zo'n assessment gaat uiteraard verder dan alleen het kijken naar de techniek. "Het is belangrijk dat je eerst kijkt naar hoe interessant zo'n bedrijf is voor cybercriminelen", begint Jutte. "Voor een bedrijf dat onderdeel uitmaakt van de vitale infrastructuur, zoals bijvoorbeeld waterschappen, krijg je een heel ander risicoprofiel dan bij een producent van wasknijpers." Het is belangrijk dat organisaties weten waar ze staan op gebied van cybersecurity. Na het laten uitvoeren van een assessment zijn de risico's duidelijk in kaart en dan pas kunnen de juiste maatregelen genomen worden.

Kat en muis

Hoe bescherm je je nu tegen DDoS-aanvallen? Of misschien is een betere vraag: kun je jezelf überhaupt beschermen tegen DDoS-aanvallen? "Er zijn tegenwoordig algoritmes om DDoS-aanvallen af te wenden", begint Jutte. "Maar je ziet dan vaak een kat-en-muis-spel ontstaan. Na het afweren van de aanval, komt de aanvaller vaak weer met een andere aanval. Een algoritme dat is ontworpen om DDoS-aanvallen te weerstaan, maakt onderscheid tussen normaal internetverkeer en verkeer dat uitsluitend bedoeld is om de server plat te leggen. In dat laatste geval zal het algoritme die IP-adressen blokkeren. Maar bij een DDoS worden vaak tienduizenden verschillende devices gebruikt om die server plat te leggen. Elke nieuwe DDoS-aanval maakt weer gebruik van nieuwe methodes en dat resulteert dus in een kat-en-muis spel. Het is wel zo dat die verdedigingsalgoritmes ook weer leren van DDoS-aanvallen, dus zo'n algoritme herkent op een gegeven moment dat er opnieuw gebruik wordt gemaakt van een ander, of hetzelfde botnet. Er zijn nu al mogelijkheden om succesvol vele DDos aanvallen te weren. Een van de meest bekende is de Nationale Wasstraat (NaWas). Deze wasstraat bestaat uit anti-DDos-apparatuur waarlangs verkeer geleid kan worden als iemand wordt aangevallen. Op deze wijze wordt het aanvalsverkeer gefilterd van het normale verkeer en hierdoor wordt de impact van een DDoS-aanval beperkt."

Voor wie het zich afvraagt; net als andere vormen van cybercriminaliteit, is elk bedrijf in Nederland ook verplicht om melding te maken van geslaagde DDoS-aanvallen. De sancties zijn bekend, ook al is de handhaving op dit moment nog vrij summier.

DDOS-terminologie

1. (D)D oS

Een Distributed Denial of Services (DDoS) aanval, is een malicieuze poging om een netwerk, webapplicatie of service te verstoren. Deze aanval wordt uitgevoerd door een grote hoeveelheid data vanaf meerdere bronnen te versturen. Hierbij kan gebruik gemaakt worden van een botnet. Een botnet is een netwerk van geïnfecteerde computers. Deze kunnen gebruikt worden door cybercriminelen om aanvallen mee uit te voeren.
Dit kan gebeuren zonder dat de eigenaar van een PC of IOT device dit doorheeft.

Hier tegenover staat een Denial of Sevices (DoS) aanval. Deze aanval richt zich vanuit één enkele bron.

DDoS-aanvallen kunnen op elk aspect van een organisatie en zijn assets gericht worden. Een DDOS-aanval kan:

- Een specifiek systeem, service of netwerk uitschakelen;
- Alarmen verstoren;
- Middelen zoals bandbreedte, schijfruimte of processortijd verstoren;

1.1. Soorten (D)DoS

Er zijn diverse soorten DDoS aanvallen, o.a.:

- HTTP Flood Attack

o Deze aanval richt zicht op webapplicaties en servers. Tijdens deze aanval maakt een aanvaller gebruik van de GET en POST requests op een doelsysteem, hierdoor is het voor legitieme gebruikers vaak niet mogelijk om het systeem te bereiken.

- SYN Flood Attack

o Deze aanval richt zich op de TCP-connectie door middel van de Three Way Handshake. De aanvaller vraagt telkens een verbinding aan met een server en beantwoordt deze vervolgens niet, waardoor bij de server de aanvragen overlopen.

- UDP Flood Attacks

o Deze aanval richt zich op een UDP-connectie. De aanvaller stuurt een grote hoeveelheid UDP packets naar de server met willekeurige informatie. Op deze manier kan de server niet meer reageren op legitieme gebruikers.

1.2. OT voorbeelden

- Schneider Electric , 2016

o Een zero-day exploit uit 2016, genaamd PanelShock, gevonden door CRITIFENCE, kon de gebruikerspanelen (HMI) van Schneider Electric onbruikbaar maken. Een hacker had de mogelijkheid om deze panelen te laten vastlopen en de connectie met de SCADA-netwerken te verbreken. Op deze manier kon er geen connectie gemaakt worden met de PLC's. Dit was mogelijk op elk product uit de Schneider Electric Magelis Advanced HMI Panel serie.

o Dit wordt gedaan door gebruik te maken van diverse http requests in de WEB Gate web service. Door een fysieke herstart kon de connectie hersteld worden.

- Finland, 2016

o In 2016 heeft een DDoS aanval heeft ervoor gezorgd dat de verwarming in twee Finse gebouwen werd uitgeschakeld. De aanval zorgde ervoor dat de computers die de centrale verwarming aansturen steeds werden herstart, met als gevolg dat de verwarming niet op gang kwam (gebouw gebonden systemen).

1.3. Mogelijke gevolgen

Een (D)DoS aanval kan verschillende gevolgen hebben voor een IACS-systeem.
In de volgende lijst zijn een aantal mogelijke gevolgen opgesomd:

- Een (D)DoS aanval kan bijvoorbeeld worden gebruikt worden om processen te verstoren, maar ook om andere activiteiten te verhullen. (Blended attack).
- Een (D)DoS aanval kan communicatie tussen verschillende externe sites verstoren, waardoor de netwerkbeheerders niet meer in staat zijn om de externe sites te controleren of aan te sturen.
- Contractuele verplichtingen

o Binnen diverse sectoren hebben zijn er contractuele afspraken over het leveren van diensten, te denken aan gas of elektriciteit. Indien deze systemen worden aangevallen kan de hoeveelheid gas of elektriciteit dat wordt geleverd niet meer worden vastgesteld. Als de voorgestelde leveringsvoorwaarden niet worden gehaald kan dit resulteren in hoge boetes.

- Onjuiste configuratie van netwerkcomponenten binnen een infrastructuur kunnen voor onregelmatigheden zorgen en leiden tot een interne DoS.

1.4. Wat te doen

Weet waar je staat aangaande de risico's die je loopt: Laat eerst een cybersecurity assessment uitvoeren. Dan weet je wat de huidige stand van zaken is. Deze nulmeting is de eerste noodzakelijke stap voor het invoeren van een verantwoord cybersecuritybeleid. Hudson Cybertec voert IEC 62443 assessments uit met focus op mens, organisatie en techniek. Zij helpen bedrijven met het implementeren/borgen van cybersecurity in hun organisatie. Hudson Cybertec werkt nauw samen met het Koninklijk Nederlands Normalisatie Instituut (NEN) en is betrokken bij de normontwikkeling voor cybersecurity voor Industriële Automatisering en Controle Systemen.