Digitale spionage en cybercriminaliteit groeiende dreiging voor de energiesector

Ir. Matthieu Paques CISSP CISA en Dennis Waalewijn

De energiesector is in de laatste jaren een belangrijk doelwit geworden voor cyberaanvallen. De energiesector wordt beschouwd als één van de twaalf vitale infrastructuren. Vitale infrastructuren worden omschreven als: 'Producten, diensten en de onderliggende processen die, als zij uitvallen, maatschappelijke ontwrichting kunnen veroorzaken. Dat kan zijn omdat er sprake is van veel slachtoffers en grote economische schade, dan wel wanneer herstel zeer lang gaat duren en er geen reële alternatieven voorhanden zijn, terwijl deze producten en diensten niet gemist kunnen worden.' ([NCTB04]). Hoe gevaarlijk zijn de toenemende cyberaanvallen op de organisaties in deze sector? Wie zijn de aanvallers en wat zijn hun motieven? Welke maatregelen kan en moet je als organisatie nemen? In dit artikel proberen de auteurs daar hun antwoord op te geven.

Ir. M.B. Paques CISSP CISA
is manager bij
KPMG Advisory N.V..
paques.matthieu@kpmg.nl

Dennis Waalewijn
is stagiair universitair bij
KPMG Advisory N.V.
waalewijn.dennis@kpmg.nl

Inleiding

Energie is van cruciaal belang voor ons dagelijks leven. Met de energiesector doelen we in dit artikel op alle industrieën die betrokken zijn bij productie, transport en levering van energie, denk hierbij aan energie uit fossiele brandstoffen (olie-industrie), nucleaire energie, aardgas, elektriciteit en kolen, maar ook energie uit waterkracht en windkracht, en zonne-energie. De dreigingen in dit artikel betreffen in algemene zin alle hiervoor genoemde industrieën in de energiesector. Tevens worden ook voorbeelden van aanvallen en risico's gegeven die specifiek zijn voor één van deze industrieën.

In elk van deze genoemde industrieën zijn de verschillende actoren in de keten verantwoordelijk voor de opwekking, distributie, levering en meting van energie en is er tussen deze actoren een sterke mate van (keten)afhankelijkheid. De Nederlandse elektriciteitsmarkt bestaat bijvoorbeeld uit verschillende actoren:

- De producenten van elektriciteit (bijvoorbeeld NUON, Essent, Electrabel, Intergen, Delta, Eneco en E.ON.).
- TenneT, ofwel de Nederlandse Transmission System Operator (TSO). De beheerder van het landelijk hoogspanningsnet voor spanningen van 110 kV en hoger.
- De regionale netbeheerders. Zij beheren hoogspanningsdistributienetten (10 tot en met 110 kV) en het laagspanningsnet.
- De programmaverantwoordelijke (PV-Partij). Zij kopen de stroom in voor de leverancier. De PV-partij is verantwoordelijk voor het in balans houden van de in- en verkoopvolumes van de elektriciteit.
- De meetbedrijven. Zij meten het daadwerkelijke verbruik van de afnemers.
- De leveranciers. Zij leveren stroom aan de afnemers.

Kwetsbare elementen in de energieketen

Bij een geslaagde cyberaanval op één van de actoren in de keten kan dit door de sterke afhankelijkheid direct gevolgen hebben voor de andere partijen in de keten en voor de keten in zijn geheel.

Industrial Control Systems

De energieproductie en -distributie van de eerdergenoemde industrieën in de energiesector worden aangestuurd en gecontroleerd door zogenaamde *Industrial*

Control Systems (ICS). Dat is een verzamelnaam voor verschillende typen controlesystemen die in industriële productieomgevingen gebruikt worden. Daartoe behoren zogenaamde 'supervisory control and data acquisition' (SCADA)-systemen, 'distributed control systems' (DCS), en kleinere controlesystemen zoals 'programmable logic controllers' (PLC).

Smart grids en smart meters

Met de term smart grid word gedoeld op een modern geavanceerd elektriciteitsnetwerk waaraan een meet- en regelsysteem is toegevoegd om sterke fluctuaties in de vraag naar en het aanbod van elektriciteit te reguleren. Fluctuaties in vraag en aanbod kunnen bijvoorbeeld veroorzaakt worden door het gebruik van elektrische auto's die op hetzelfde moment (na werktijd) in een wijk moeten worden opgeladen of door lokale teruglevering aan het elektriciteitsnetwerk door particulieren bij eigen opwekking van zonne- of windenergie bij gunstige weersomstandigheden. Door middel van smart grids kan de aanvoer van energie naar het netwerk worden beperkt, of kunnen bijvoorbeeld gebruikers worden afgesloten als de vraag te hoog is. Hoewel de meet- en regelsystemen van een smart grid deze efficiënter maken, worden hiermee ook aanvullende risico's voor cyberaanvallen geïntroduceerd. De beveiliging van een smart grid is van cruciaal belang om de stabiliteit en betrouwbaarheid ervan te kunnen garanderen. Bij gebrek aan adequate securitymaatregelen kan mogelijk in grote delen van het grid stroomuitval optreden.

Smart meters zijn moderne meters voor elektriciteit-, gas- of waterverbruik die van traditionele meters verschillen in die zin dat deze kunnen communiceren met de netbeheerder voor monitoring- en facturatiedoeleinden. Wanneer aanvallers via deze nieuwe functionaliteit toegang weten te krijgen tot meetgegevens van klanten kan een privacy- en/of imago-issue ontstaan. Een aanvaller kan deze verbruiksinformatie weer gebruiken in verdere aanvallen, bijvoorbeeld door inbraken te plegen in huishoudens waar voor langere periode een lager verbruik wordt doorgegeven (vakantie). Wanneer ook home automation functionaliteit gekoppeld gaat worden aan de smart meter (denk aan de thermostaat instellen via mobiele telefoon en bijvoorbeeld koppelingen van alarmsystemen met de smart meter zodat de hele home automation vanuit één mobiele app kan worden uitgevoerd) ontstaan hier nieuwe risico's wanneer cybercriminelen in staat zijn deze 'besturing van je huis' op afstand over te nemen.

Cyberaanvallen

Industrial Control Systems worden vaak voor tientallen jaren in gebruik genomen. Daardoor bevatten veel oudere systemen nog beperkte of nauwelijks securitymaatregelen. Op het moment dat zij ontwikkeld werden was er namelijk geen dreiging van cyberaanvallen op deze omgevingen. Gezien de vaak hoge eisen met betrekking tot stabiliteit en continuïteit van ICS is het bovendien vaak moeilijk, zo niet onmogelijk om bijvoorbeeld patches en updates uit te rollen op deze systemen. ICS worden echter in toenemende mate verbonden met het internet voor beheer op afstand en monitoringdoeleinden zonder dat daarvoor in alle gevallen adequate securitymaatregelen geïmplementeerd worden. Dit gegeven tezamen met de grote impact die een geslaagde aanval op de energieketen als onderdeel van de vitale infrastructuur kan veroorzaken, maakt deze keten tot een aantrekkelijk en relatief makkelijk doelwit voor cyberaanvallen.

Het doel van cyberaanvallen varieert van diefstal van intellectual property tot sabotage vanuit staatsbelangen. Verderop in dit artikel wordt nader ingegaan op door wie deze aanvallen worden uitgevoerd en de onderliggende motivatie.

Waarom cyber security op de agenda thuishoort

In hoofdlijnen zijn er drie ontwikkelingen waarom cyber security een belangrijk onderwerp op de agenda van organisaties in de energiesector zou moeten zijn.

Toename van dreigingen	Cyberaanvallen op de energiesector nemen elk jaar toe in aantal en worden in hoog tempo geavanceerder en toegespitst op specifieke doelwitten.
Veranderingen in de eigen sector	Innovaties als cloud, social media, smart meters en smart grid zorgen mogelijk voor nieuwe cyberrisico's en kwetsbaarheden.
Toenemende regulering	In toenemende mate wordt druk uitgeoefend waarbij organisaties worden geacht aantoonbaar in control te zijn.

Figuur 1. **De drie hoofdontwikkelingen omtrent cyber security in de energiesector.**

Toename van dreigingen

De energiesector is inmiddels een geliefd doelwit voor cyberaanvallen en de laatste jaren is het aantal gerichte aanvallen op deze sector sterk toegenomen. Een greep uit de nieuwsfeiten omtrent deze ontwikkeling:

De vitale infrastructuur maakt de energieketen tot een aantrekkelijk doelwit voor cyberaanvallen

- Uit een rapportage van KPMG uit 2011 blijkt dat de olie- en gassector in de top 10 van sectoren wereldwijd staat die te maken heeft met het lekken van vertrouwelijke informatie (information leakage). Deze sector staat tevens in de top 10 met betrekking tot het posten van systeeminformatie op forums en nieuwsgroepen. Hoewel dit op het eerste gezicht wellicht niet ernstig lijkt is deze informatie zeer waardevol voor het voorbereiden van verdere aanvallen op een organisatie.
- Een rapport van McAfee uit 2011 geeft aan dat vier van de vijf organisaties in de olie-, gas- en elektriciteitssector minimaal getroffen zijn door één Denial of Service (DoS)-aanval in 2011.
- In april 2012 werd in het United States (US) Department of Homeland Security News Wire gepubliceerd dat Amerikaanse bedrijven in de water- en energiesector elke dag te maken hebben met cyberaanvallen (over het algemeen vormen van cyberspionage of DoS-aanvallen tegen ICS) ([USDH12]).
- Volgens een cybercrime survey uitgevoerd door KPMG in 2012 ([KPMG12]) heeft 49 procent van de onderzochte organisaties een vorm van cybercrimeactiviteit waargenomen. De overige 51 procent heeft dit niet waargenomen, maar heeft veelal ook geen of zeer beperkte detectiemiddelen daartoe ingericht. Merk op dat de respondenten aangaven dat het merendeel van de incidenten niet is opgepakt door de media en daarmee niet publiek bekend is.
- In maart 2014 waarschuwt het US Department of Homeland Security voor toenemende aanvallen gericht op het veroorzaken van sabotage in de energiesector ([USDH14]).
- In januari 2014 meldt Symantec dat de energiesector wereldwijd op de vijfde plaats staat met betrekking tot cyberaanvallen en goed is voor 7,6 procent van alle cyberaanvallen wereldwijd ([Syma14]).

'Beroemde' aanvallen zoals Stuxnet, Night Dragon, Shamoon, Red October

De afgelopen paar jaar heeft de energiesector verschillende keren kennisgemaakt met zeer geavanceerde en complexe aanvallen waaronder Stuxnet, Night Dragon en Shamoon. Deze malware is specifiek voor ICS ontwikkeld en is soms zelfs specifiek gericht op bepaalde landen of organisaties. Met name Stuxnet heeft aangetoond tot welke schade cyberaanvallen op ICS kunnen leiden. Sinds de ontdekking van Stuxnet in 2010 zijn er onder andere door het Kaspersky lab verschillende varianten gevonden waarvan vermoed wordt dat ze veel ICS hebben geïnfecteerd. De oorspronkelijke versie van Stuxnet is specifiek ontwikkeld voor het infecteren van Iranese kernreactoren en maakte gebruik van verschillende zero-day exploits (publiek nog onbekende kwetsbaarheden) op de systemen die in die reactoren draaiden. Eén van deze exploits die Stuxnet gebruikt, betreft de kwetsbaarheid in de Microsoft Windows Shortcut (CVE-2010-2568) die het mogelijk maakt dat de malware zich tevens via USB-sticks kan verspreiden naar geïsoleerde systemen die niet verbonden zijn aan het interne netwerk of internet. De malware had als doel om de ultracentrifuges die gebruikt worden voor het maken van nucleaire brandstof te saboteren, en zou het kernprogramma met vier jaar vertraagd hebben. Andere malware, zoals Duqu, Flame en Red October, die ingezet is tegen organisaties in de energiesector, had in plaats van sabotage als doel informatie te vergaren en door te sturen, ofwel spionage.

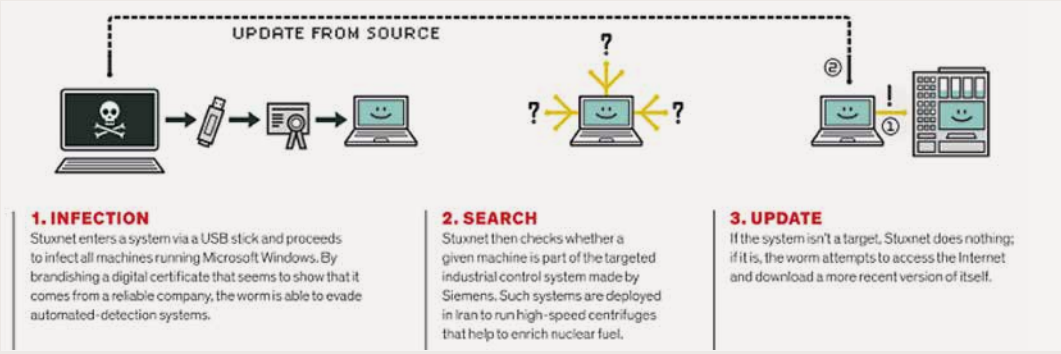
Deze ontdekkingen zijn het bewijs dat samenwerking van getalenteerde programmeurs met erg veel kennis (ook intern) noodzakelijk was. Tevens moeten er significante financiële middelen beschikbaar zijn geweest voor de ontwikkeling van zulke complexe aanvallen. Gesuggereerd wordt dat er een overheid achter de ontwikkeling van Stuxnet zit en dat de ontwikkeling hiervan 15 miljoen euro heeft gekost.

Een ander bekend voorbeeld betreft de cyberaanvallen op het energiebedrijf RasGas, één van 's werelds grootste producenten van vloeibaar petroleumgas, dat in 2012 door een aanval met een 'onbekend virus' een groot deel van het netwerk offline moest halen. In hetzelfde jaar werd ook oliemaatschappij Aramco ('s werelds grootste olieproducent) getroffen door een virusaanval waardoor meer dan 30.000 systemen wekenlang offline moesten worden gehaald. Beide organisaties bleken te zijn getroffen door het Shamoon-virus en hadden daarmee de primeur van een cyberaanval van significante omvang, specifiek gericht op doelwitten in de olie- en energiesector. Het Shamoon-virus werd later omschreven als één van de meest geavanceerde aanvallen op de sector tot dat moment.

Een derde berucht voorbeeld van aanvallen in de energiesector heeft de naam Night Dragon gekregen ([Mcaf]). Dit betreft aanvallen gericht op het verkrijgen van financiële informatie met betrekking tot olie- en gasprocessen. De aanvallen begonnen met het compromitteren van publiek beschikbare webservers via SQL-injection en het plaatsen van web shells (met een web shell kan een aanvaller via een normale webbrowser systeemcommando's op het systeem uitvoeren). Vervolgens werd door de aanvallers verdere informatie op het systeem verzameld, zoals

De werking van Stuxnet

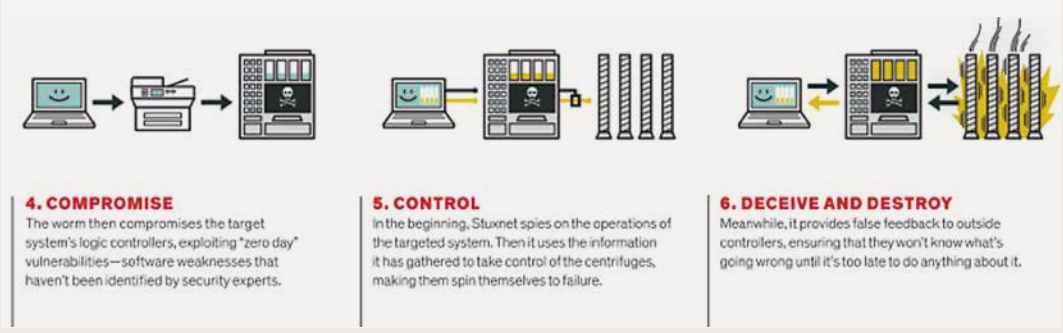
Een computerworm zoals Stuxnet werkt eigenlijk in drie fasen, namelijk de propagatie, de verspreiding en de sabotage. Allereerst moet de malware op een manier het systeem binnendringen. In de energiesector zijn de ICS vaak afgesloten van open netwerken zoals het internet, maar op de controlesystemen van waaruit het energieopwekkingsproces wordt gecontroleerd, draaien veelal verouderde applicaties en besturingssystemen. Dataoverdracht vindt plaats via cd-drives of USB-ingangen. Gebruik van deze poorten is hoogstwaarschijnlijk de meest voorkomende propagatietechniek van dit soort malware, bijvoorbeeld via een geïnfecteerde USB-stick die op een controlecomputer van een ICS wordt ingeplugd (zie figuur 2).



Figuur 2. **Propagatie van Stuxnet** (bron: [Kush13]).

De malware gaat vervolgens op zoek naar systemen die geïnfecteerd kunnen worden en verspreidt zich over het netwerk. De volgende stap is controleren of de target software, in dit geval de Siemens software, op het systeem draait. Als dit het geval is kan de 'payload' worden geleverd en daarmee wordt de interne logica veranderd. In geval van Stuxnet betekende dit concreet dat de turbines in kwestie opeens buiten hun limiet konden draaien. Om detectie door personeel te voorkomen werden door de malware meetwaarden opgenomen tijdens normale operatie en werden deze valse meetwaarden tijdens de daadwerkelijke aanval 'afgespeeld' naar de gebruikersinterface.

Figuur 3 geeft een weergave van hoe het vervolg van de aanval in zijn werk gaat. Gedurende deze fasen wordt door middel van root-kit functionaliteit, encryptie en het gebruik van verschillende zero-day exploits gepoogd de aanval onder de radar van moderne detectiemiddelen te houden.



Figuur 3. **Sabotage door Stuxnet** (bron: [Kush13]).

wachtwoorden en informatie over andere systemen op het netwerk. De aangetroffen wachtwoorden stelden de aanvallers in staat verder op het netwerk door te dringen. Ook werd informatie verzameld via spear phishing-aanvallen. (Bij spear phishing worden gerichte phishingaanvallen uitgevoerd op enkele personen die relevante informatie of toegang voor de aanvallers kunnen verschaffen.) Opmerkelijk is dat al deze aanvallen werden uitgevoerd met publiek beschikbare tools die dus voor iedereen toegankelijk zijn.

Figuur 4 bevat een chronologisch overzicht van de belangrijkste cyberaanvallen in de energiesector van de aflopen jaren. Merk op dat zoals eerder opgemerkt een groot deel van de aanvallen niet publiek bekend is.

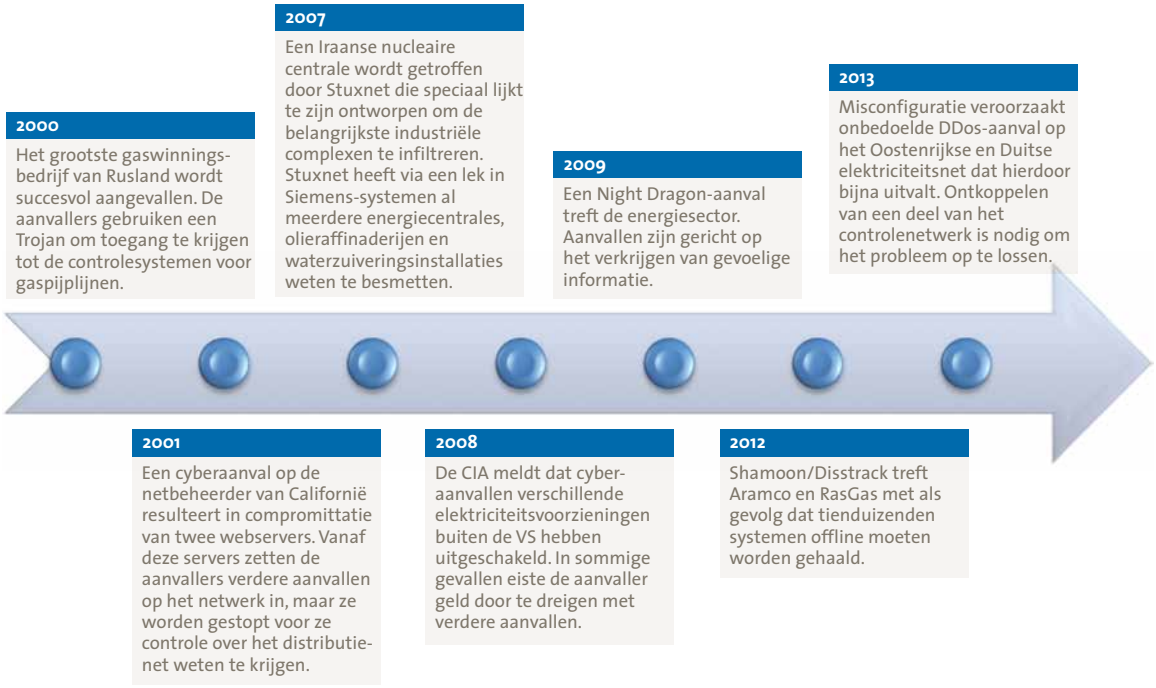
Veranderingen in de energiesector

Voorheen waren veel Industrial Control Systems (ICS) en Supervisory Control and Data Acquisition (SCADA)-systemen fysiek gescheiden van kantoornetwerken en internetkoppelingen. In de praktijk vindt veelal toch dataoverdracht plaats naar deze 'geïsoleerde' omgevingen via bijvoorbeeld USB-sticks. Zoals reeds beschreven geeft dit malware zoals Stuxnet de mogelijkheid toch door te dringen tot deze netwerken. Een bijkomend gevolg van deze isolatie is dat security updates op deze systemen niet (tijdig) bijgewerkt worden. Door de wens om (remote) systemen te kunnen monitoren en (beperkte) bediening mogelijk te maken worden meer en meer omgevingen gekoppeld aan bestaande netwerken en internet en daarmee blootgesteld aan daarbij behorende risico's.

Ontwikkelingen in de elektriciteitssector op het gebied van smart grids en smart meters hebben aanvullende mogelijkheden geïntroduceerd voor hackers ([Blac12]). Voor smart meters is bijvoorbeeld een opensource hacking framework beschikbaar ([SECB12]). Naar verwachting zullen de komende jaren miljoenen smart meters en sensors worden geïnstalleerd. In aanvulling daarop vindt de energieopwekking meer en meer decentraal plaats. Particulieren kunnen door middel van eigen opwekking (bijvoorbeeld zonne- of windenergie) een overschot aan energie terugvoeden aan het smart grid. Niet alleen betekent dit meer kwetsbare installaties, ook zorgen zij voor moeilijker balancering van het smart grid en fluctuaties in de energietoevoer.

Nationaal beleidsplan vitale infrastructuur

Minister Opstelten van Veiligheid en Justitie is verantwoordelijk voor het beleid met betrekking tot cyber security. Eén van de speerpunten van de afgelopen drie jaar is het stijgende beveiligingsniveau van ICS die wor-



Figuur 4. **Chronologisch overzicht van belangrijke publiek bekende cyberaanvallen in de energiesector.**

De georganiseerde misdaad voert steeds geavanceerdere cyberaanvallen uit

den gebruikt in vitale infrastructuren. Het meest recente beleidsplan (2014-2016) heeft als doel Nederland weerbaar te maken tegen cyberaanvallen. De beleidsacties die voor de energiesector van belang zijn:

1. Er gaan steeds meer minimumbeveiligingseisen gesteld worden tezamen met een stelsel van gedragen open (technische) standaarden en de sectorale toezichthouder, de Energiekamer, gaat de naleving hiervan controleren.
2. Het nationaal detectie- en responsnetwerk is sinds 2013 in werking gesteld vanuit een EU-richtlijn, en zal in toenemende mate moeten worden gebruikt. Bij dit gebruik hoort bijvoorbeeld het melden van incidenten.

Het National Institute of Standards and Technology (NIST) heeft een raamwerk opgesteld waaraan ICS getoetst kunnen worden op het gebied van security ([NIST13]). Dit bevat (alleen) managementgerelateerde punten (zoals het regelmatig medewerkers wachtwoorden laten veranderen) waaraan getoetst kan worden. Dit raamwerk is vertaald door de Europese standaardenorganisatie IEC voor gebruik in de EU. De EU-richtlijn beschrijft verder dat landen een eigen raamwerk mogen ontwikkelen. De Nederlandse Norm (NEN) is een Nederlandse stichting voor de creatie en het beheer van normen en standaarden die deze taak in samenwerking met grote organisaties in onder andere de energiesector uitvoert. De NEN heeft het IEC-raamwerk voor beveiliging van ICS naar het Nederlands vertaald. Daarnaast wordt door de ENISA, een Europese Organisatie voor Netwerk en Informatie Beveiliging, aan een raamwerk voor technische standaarden omtrent ICS gewerkt ([ENIS11]).

Wie zijn de aanvallers?

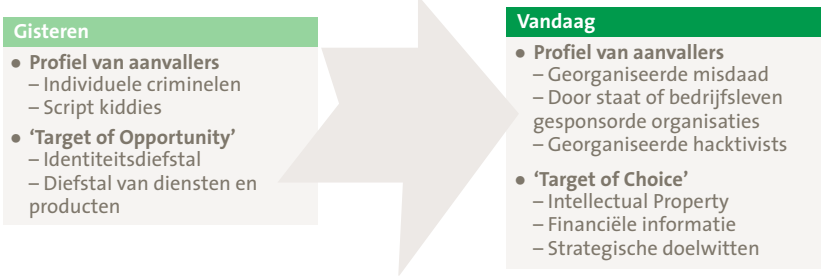
Waar voorheen cyberaanvallen het domein waren van hackers, script kiddies en hacktivisten, is dit in toenemende mate het domein aan het worden van de georganiseerde misdaad die met praktisch onbeperkte (financiële) middelen steeds geavanceerdere cyberaanvallen uitvoert. Dat gebeurt steeds meer 'onzichtbaar' en gericht op specifieke doelen. Over de afgelopen jaren zijn twee grote trends waar te nemen met betrekking tot cyberaanvallen. Allereerst verschuiven de doelwitten van individuele organisaties naar *ketens* van gerelateerde organisaties. En ten tweede verplaatst het profiel van de aanvallers zich van individuele criminelen en script kiddies naar professionele en goed georganiseerde criminele organisaties. Belangrijke spelers in het huidige veld zijn:

- Georganiseerde criminelen die uit zijn op het massaal stelen van persoonsgegevens en financiële data.
- Door de staat of het bedrijfsleven gesponsorde organisaties die uit zijn op spionagegevoelige data of bedrijfsgegevens. Denk hier ook aan cyber warfare. In 2009 kwamen al berichten naar buiten dat China en Rusland het Amerikaanse elektriciteitsnet hadden geïnfiltreerd en computerprogramma's hadden achtergelaten die kunnen worden gebruikt om het systeem te verstoren.
- Hacktivists zoals Wikileaks, Anonymous en dergelijke.
- Kwaadaardige insiders, die bijvoorbeeld interne informatie lekken.

Motivatie

De motivatie voor het plegen van aanvallen varieert van het verkrijgen van toegang tot informatie, financiële middelen en systemen voor het verkrijgen van een financieel of strategisch voordeel tot staatsgesponsorde activiteiten met als doel het saboteren van het productieproces van energieleveranciers en het ontregelen van de vitale infrastructuur. Er zijn 'freelance hackers' te huur zoals de 'Hidden Lynx Group' en hacktivisten die hun eigen politieke doelen nastreven.

In 2013 werden door hackers die zich uitgaven voor Anonymous, gestolen inloggegevens op internet geplaatst voor, volgens de beschrijving, Israëlische SCADA-systemen in onder andere elektriciteitscentrales. Een ander voorbeeld uit 2013 betreft de actiegroep 'Save the Arctic', die verschillende oliemaatschappijen wereldwijd aanviel als protest tegen boringen op de Noordpool. Werknemers kunnen aanvallen uitvoeren met afpersing of omkoping als doel, of uit wraakgevoelens jegens de werkgever. Afhankelijk van de motivatie van de aanvaller kan een jarenlange voorbereiding aan een aanval voorafgaan.



Figuur 5. **Ontwikkeling van cyberdreigingen.**

De Cybercrime Underground

Met de professionalisering van criminele dienstverlening is een groot scala aan platformen ontstaan waarop cybercriminelen diensten aanbieden en afnemen. Denk hierbij aan het kopen en verkopen van botnets, (laten) ontwikkelen van customized malware voor een specifiek doelwit, verhandelen van gesloten informatie als bedrijfsdata, gebruikersaccounts, DDoS-services, etc. Enkele 'beroemde' voorbeelden van deze underground markets zijn de volgende:

- De Hidden Wiki

http://kpvz7ki2v5agwt35.onion/
Links naar verscheidene verborgen diensten

- Silk Road (inmiddels offline gehaald)

http://ianxz6zefk72ulzz.onion/
Drugs, botnets

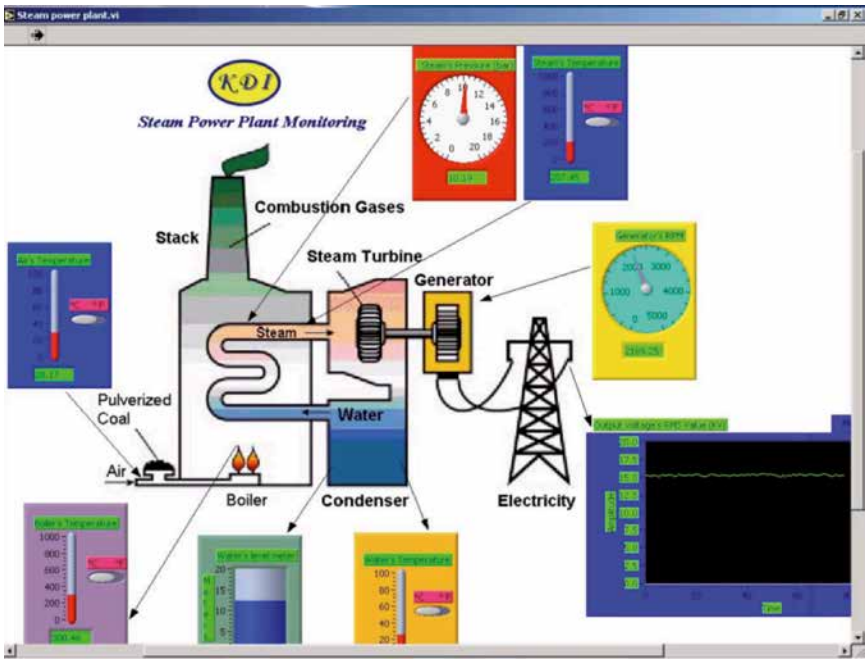
- Black Market reloaded

http://5onwnspjvuk7cwvk.onion/
Drugs, wapens, valse paspoorten

Bovenstaande links zijn niet via een normale browser bereikbaar om de anonimiteit hiervan te vergroten. Voor het bekijken van deze sites is de Tor browser nodig.

*Het is voor organisaties niet de vraag **of** ze gehackt worden, maar **wanneer** ze gehackt worden*

Figuur 6. **De Shodan zoekmachine.**



Figuur 7. **De gebruikersinterface voor het beheren van een energiecentrale.**

Aanvalsmethoden en tegenmaatregelen

Aanvalsmethoden

De energiesector is in grote mate afhankelijk van ICS en SCADA of vergelijkbare systemen. Een deel van deze systemen is (al dan niet bedoeld) via het internet te vinden en te benaderen. Een mogelijke manier om dergelijke systemen in kaart te brengen is via de publiekelijk beschikbare Shodan zoekmachine (shodanhq.com).

Via deze zoekmachine, die te zien is in figuur 6, kan eenvoudig gezocht worden naar online toegankelijke gebruikersinterfaces voor allerlei (onder meer industriële) systemen, zoals de bedieningsinterface voor de energiecentrale in figuur 7. Veelal kunnen via deze interfaces niet alleen meetwaarden van de systemen worden uitgelezen, maar ook daadwerkelijk aanpassingen worden uitgevoerd zoals het afsluiten van kleppen, het instellen van temperaturen of het uitschakelen van beveiligingsmechanismen. Vermoedelijk zijn beheerders van de betreffende systemen zich er niet van bewust dat deze systemen publiek toegankelijk zijn.

Ter illustratie een tweede voorbeeld: windturbines. Door middel van de volgende zoekopdracht kan de locatie van de gebruikersinterface van deze turbines worden opgezocht: http://www.shodanhq.com/?q=Jetty%2F3.1.8+%28Windows+2000+5.0+x86%29+. Figuur 8 geeft een voorbeeld van de gebruikersinterface van een dergelijke windturbine.

Er zijn zelfs tal van sites met 'handige zoekopdrachten' om interessante systemen te vinden zoals deze: http://www.scadaexposure.com/library/scada-googledorks-121227101926-phpapp01.pdf. Met tools als deze kan al met enkel een webbrowser of zelfs met een app vanaf de mobiele telefoon toegang worden verkregen tot een groot scala aan systemen en waardevolle informatie.

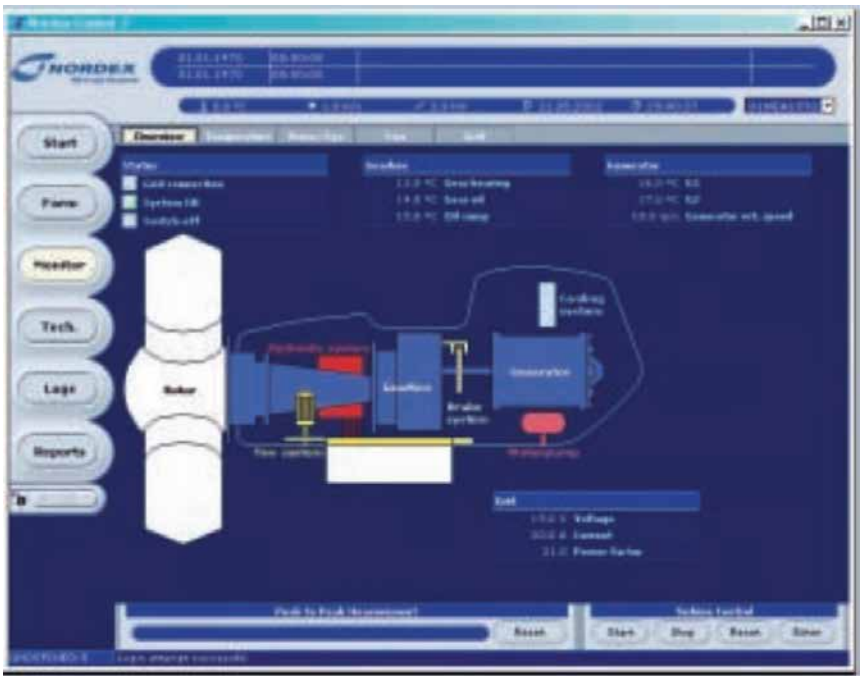
Naast deze zoektools zijn kwetsbaarheden in SCADA-infrastructuur en sourcecode van geavanceerde aanvals-tools zoals Stuxnet eenvoudig via zoekmachines als Google te vinden. Als gevolg hiervan kan ook een leek eenvoudig over geavanceerde tools beschikken om cyberaanvallen uit te voeren.

Grootschalige aanvallen zijn veelal een complexe combinatie van de verschillende aanvalstechnieken, waarbij informatie verkregen in de ene aanval weer gebruikt wordt in de volgende aanval. Bij veel aanvallen speelt social engineering, waarbij gebruikers worden misleid om kritieke informatie als wachtwoorden te verkrijgen, een belangrijke rol. De meest gebruikte aanvalsmethoden volgens onderzoek van KPMG zijn weergegeven in figuur 9 ([KPMG12]).

Tegenmaatregelen

Organisaties kunnen zich op verschillende manieren wapenen tegen cyberaanvallen. Hieronder een zestal belangrijke maatregelen:

1. Allereerst is het van cruciaal belang om de motivatie achter de cyberaanvallen te begrijpen. Organisaties dienen zich bewust te zijn van de professionalisering in de cyberwereld en zich te realiseren dat ze mogelijk te maken hebben met spelers met onbeperkte tijd en middelen.
2. Ten tweede is het noodzakelijk om de risico's in kaart te brengen. Wat van ondergeschikt belang blijkt voor de organisatie kan van grote waarde zijn in de perceptie van een aanvaller.



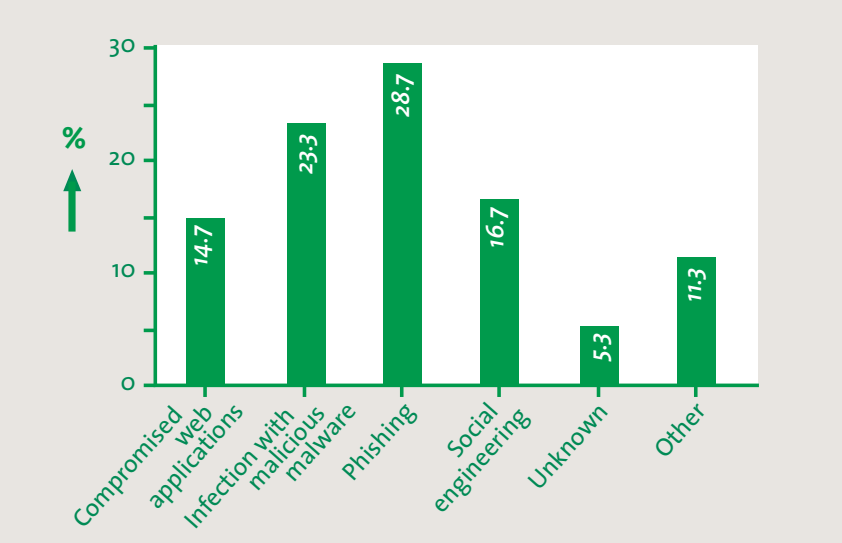
Figuur 8. **De gebruikersinterface van windturbines is via een normale browser eenvoudig te vinden.**

3. Ten derde, organisaties dienen zich niet af te vragen *of* ze gehackt worden, maar *wanneer* ze gehackt worden. Maatregelen dienen ingericht te worden op zowel het voorkomen als het detecteren en opvolgen van cyberaanvallen (figuur 10). Een incidentresponseplan is daarom ook van belang om een cyber security-incident op de juiste wijze te kunnen opvolgen en de schade zo goed mogelijk te beperken. Met name de eerste uren na detectie van een security-incident zijn hiervoor van cruciaal belang.
4. Een vierde belangrijk aspect is dat organisaties zich realiseren dat ze een rol spelen in de keten en mogelijk de keten het doelwit van de aanval is, en niet alleen de eigen organisatie.
5. Een vijfde belangrijk aspect is dat de menselijke factor veelal de zwakste schakel in de keten is. Organisaties dienen voldoende aandacht te geven aan deze vaak 'vergeten' schakel. Security awareness-tests en -trainingen kunnen effectief helpen tegen social engineering-aanvallen op medewerkers.
6. Organisaties dienen kennis te delen met andere partijen om zo zich effectiever te kunnen wapenen tegen aanvallen en beter voorbereid te zijn op cyberaanvallen.

Defense-in-depth componenten om deze bedreigingen tegen te gaan

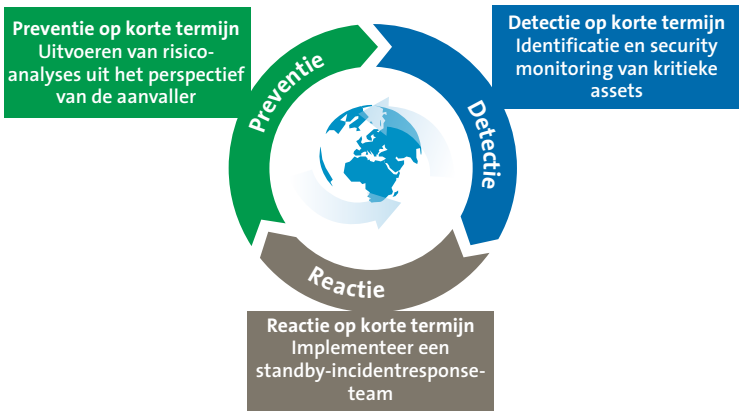
Een ICS bestaat uit meerdere lagen en verbindt als het ware de fysieke analoge wereld met de digitale wereld waar in netwerken gecommuniceerd wordt. Op zowel de fysieke, de netwerk- als de communicatielaag van zulke

Intrusion Detection Systemen voor ICS-omgevingen staan nog in de kinderschoenen



Figuur 9. **De meest gebruikte aanvalsmethoden bij cyberaanvallen** (bron: [KPMG12]).

systemen kunnen verschillende cyberaanvallen plaatsvinden. Daarom is een defense-in-depth plan met maatregelen in elke laag nodig om zo goed mogelijk deze dreigingen tegen te gaan.



Figuur 10. **Maatregelen dienen ingericht te worden op zowel het voorkomen als het detecteren en opvolgen van cyberaanvallen.**

Op fysiek niveau dient aandacht te worden besteed aan afbakening van fysieke locaties en beveiliging ervan (ook wel perimeter security). Denk hierbij aan hekken, prikkeldraad, toegangspoortjes, camera's en dergelijke. Verder moet het gebruik van fysieke ingangen van systemen, zoals USB-poorten, cd-rom drives en netwerkpoorten, zoveel mogelijk worden vermeden, bijvoorbeeld door onnodige poorten dicht te lassen, en door drivers te verwijderen of onbereikbaar te maken. In de communicatielaag is het aan te bevelen om zoveel mogelijk niet-open protocollen te gebruiken en de standaarden die worden opgesteld door de overheid na te leven. Daarnaast maakt het een behoorlijk verschil of een ICS bestaat uit componenten van een of van meer leveranciers. Zijn deze van meer leveranciers afkomstig, dan moeten er meer open protocollen worden ondersteund, hetgeen aanvullende risico's met zich mee kan brengen.

Op netwerkniveau kunnen maatregelen worden geïmplementeerd als netwerksegmentatie en demilitarized-zones in combinatie met Intrusion Detection Systemen (IDS) om indringers te detecteren. Merk op dat IDS voor ICS-omgevingen nog in de kinderschoenen staat. In de praktijk wordt ook een zogenaamd 'honeynet' ingezet om mogelijke aanvallers te misleiden naar een locatie die doet alsof zij de kritieke asset is, terwijl daar verder geen consequenties aan hangen. Juist hieruit kan een organisatie informatie vergaren over het type en de herkomst van aanvallen op dit niveau. Engineers en andere medewerkers die betrokken zijn bij het uitvoeren van het industriële proces dienen persoonlijke accounts te hebben; wachtwoorden om in het systeem te komen moeten regelmatig worden veranderd.

Samenvatting

De energiesector heeft tegenwoordig vrijwel dagelijks te maken met cyberaanvallen, spionage en sabotage. Deze aanvallen worden meer en meer complex en bovendien zijn aanvallen op deze sector in de afgelopen jaren sterk toegenomen. Aanvallers richten zich meer op gerichte doelen (target of choice); dit in tegenstelling tot voor kort toen aanvallen breed werden uitgevoerd en (target of opportunity) gericht waren op 'het laaghangend fruit'. Door toegenomen connectiviteit van ICS en ontwikkelingen als smart meters en smart grid ontstaan nieuwe

aanvalsmogelijkheden en wordt de dreiging verder vergroot. Naast de directe schade als gevolg van diefstal van vertrouwelijke gegevens of sabotage kunnen cyberaanvallen leiden tot indirecte schade op de langere termijn. Voor de energiesector is de ketenafhankelijkheid een belangrijk aspect. Energieleveranciers, netbeheerders, programmaverantwoordelijken, meetbedrijven en leveranciers zijn sterk van elkaar afhankelijk en een geslaagde aanval op één van deze partijen heeft mogelijk ingrijpende gevolgen voor andere spelers in de keten. Imagoschade kan tot gevolg hebben dat belangrijke klanten verloren gaan en verlies van gegevens kan leiden tot verlies van de strategische marktpositie en tot boetes of rechtszaken. Organisaties in de energiesector dienen zich bewust te zijn van deze toename van dreigingen en adequate maatregelen te treffen om cyberaanvallen te kunnen pareren, detecteren, en daar vervolgens op de juiste wijze op te kunnen reageren.

Literatuur

• *Bronnen waarnaar wordt verwezen*

[Blac12] Dissecting Smart Meters
https://media.blackhat.com/bh-eu-12/Searle/bh-eu-12-Searle-Smart_Meters-Slides.pdf

[ENIS11] www.enisa.europa.eu/?came_from=https%253A//www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Netherlands.pdf

[FBI] FBI – Combating Threats in the Cyber World Outsmarting Terrorists, Hackers, and Spies
www.fbi.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

[KPMG12] A nuanced perspective on cybercrime – Shifting viewpoints – call for action
www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf

[Kush13] Kushner, D. (2013). The real story of Stuxnet. *Spectrum, IEEE*, 50(3), 48-53.

[Mcaf] Global Energy Cyberattacks: 'Night Dragon'
www.mcafee.com/sg/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

[NCTB04] De Nationaal Coördinator Terrorismebestrijding 2004
www.infopuntveiligheid.nl/Publicatie/Dossier/10/vitale-infrastructuur.html

[NIST13] Guide to Industrial Control Systems (ICS) Security
http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[SECB12] Security B-Sides Vegas
https://media.blackhat.com/bh-eu-12/Searle/bh-eu-12-Searle-Smart_Meters-Slides.pdf

[Syma14] attacks-against-energy-sector
www.symantec.com/connect/blogs/attacks-against-energy-sector

[USDH12] U.S. power and water utilities face daily cyberattacks
www.homelandsecuritynewswire.com/dr20120406-u-s-power-and-water-utilities-face-daily-cyberattacks

[USDH14] National Electric Grid Remains at Significant Risk for Cyber-attack
www.infosecurity-magazine.com/view/37321/national-electric-grid-remains-at-significant-risk-for-cyberattack/

• *Andere bronnen*

[BBCN] Spies 'infiltrate US power grid'
http://news.bbc.co.uk/2/hi/technology/7990997.stm

[RSA12] RSA 2012: Aging industrial control systems increasingly vulnerable to cyberattack
www.infosecurity-magazine.com/view/24384/

[ISS12] 7 Steps to ICS Security
www.isssource.com/wp-content/uploads/2012/02/022912WP-7-Steps-toICS-Security-v1.0.pdf

[MiVo13] Ministerie van Volksgezondheid (2013). *Nationale Cybersecurity Strategie*, (2), 1–36.

[NCSC13] Nationaal Cyber Security Centrum (2013). *Cybersecuritybeeld Nederland*, (3).

[Virv13] Virvilis, N. and D. Gritzalis (2013). The Big Four – What We Did Wrong in Advanced Persistent Threat Detection? *2013 International Conference on Availability, Reliability and Security*, 248–254. doi:10.1109/ARES.2013.32

Over de auteurs

Ir. M.B. Paques CISSP CISA is manager in het 'Information Protection Services (IPS)'-team van KPMG Advisory N.V. Hij heeft ruime ervaring met interne en externe security-testen, social engineering en specialistische beveiligingsonderzoeken. Hij geeft colleges en workshops met betrekking tot legal hacking en technische security-onderwerpen. Hij is één van de organisatoren van de jaarlijkse internationale KPMG cyber security-conferentie 'Hacknet'.

Dennis Waalewijn is stagiair universitair in het 'Information Protection Services (IPS)'-team van KPMG Advisory N.V. Hij heeft een achtergrond in Business Information Technology en doet een afstudeeropdracht in Cybersecurity van Industrial Control Systems. Zijn onderzoek focust zich op de beveiliging van één van de belangrijkste componenten van een ICS, namelijk de Programmable Logic Controller, die bijvoorbeeld pompen en kleppen in grote petrochemische fabrieken aanstuurt.