Door Jeroen Aijtink, CISSP en Jan Wiersma, Int. Director EMEA DatacenterPulse.

EEN VIRUS IN JE NOODSTROOMGENERATOR

In de zomer van 2010 werd bekend dat er een zeer geavanceerd wormvirus was gevonden. Doel van dit wormvirus was de Iraanse ultracentrifuges te saboteren. Het virus was geprogrammeerd om programmacode in PLC's van Siemens te wijzigen en zo de motoren van de centrifuges te beïnvloeden. Het virus kreeg de naam Stuxnet mee, en kwam bekend te staan als het eerste virus dat industriële besturingssystemen als specifiek doel had.

Tot voor kort was het algemene idee dat SCADA- en industriële besturingssystemen kwetsbaar waren voor een cyberaanval voor velen slechts een theoretisch probleem. Door de grote complexiteit van deze systemen en hun bijzondere communicatieprotocollen waanden leveranciers en gebruikers zich veilig. De redenering erachter was dat complexe, industriële besturingssystemen zoals PLC's simpelweg zo verschillend zijn van normale IT-systemen dat deze geen interessant doel zijn voor 'traditionele' hackers. Meer bepaald zijn die verschillen:

- Industriële besturingssystemen bevatten componenten zoals PLC's, motor controllers en intelligente automaten, waarover de kennis van de gemiddelde hacker niet toereikend is;
- De componenten van die besturingssystemen zijn uitgevoerd in wijdvertakte netwerken met honderden onderdelen; alleen ervaren engineers begrijpen de complexiteit ervan;
- Ook de gebruikte communicatieprotocollen zoals Modbus en BACNet, zijn voor de meeste hackers onbekend. Datapakketten in dergelijke omgevingen zijn zonder specifieke kennis niet te vertalen;
- Zonder gedetailleerde kennis van de specifieke systeemarchitectuur zegt het merendeel van de systeemdata de hacker niet veel;
- Industriële besturingssystemen bevatten geen financiële of persoonlijke data - informatie die normaliter het doel is van een hacker.

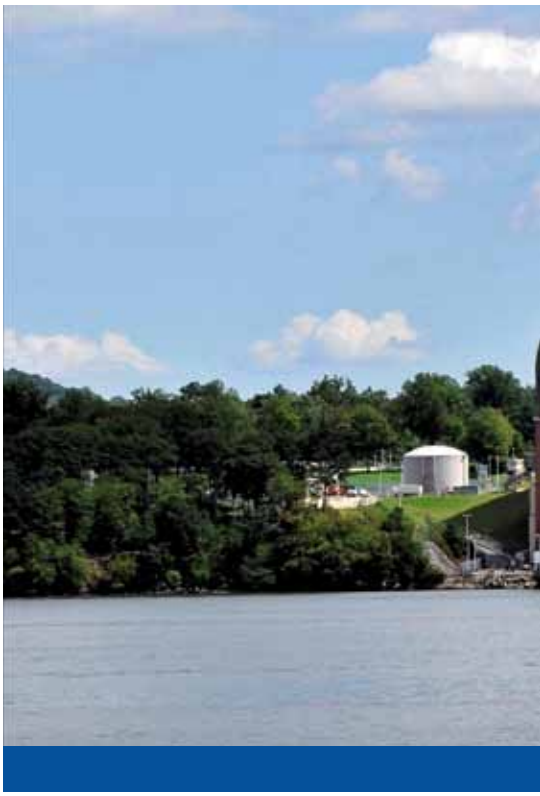
Een beveiligingsstrategie - als je het woord 'strategie' in deze context al kunt gebruiken - die puur is gebaseerd op systeemcomplexiteit en unieke systeemarchitecturen wordt door beveiligingsspecialisten ook wel 'security through obscurity' genoemd. Vaak zie je daarbij dat SCADA-netwerken slechts zijn beveiligd met een wachtwoord voor het bedienend personeel en niet veel meer.

> Stuxnet was het eerste virus met SCADA-systemen als doel

SCADA 2.0

In de afgelopen jaren is de wereld van industriële besturingssystemen en SCADA's echter behoorlijk veranderd. Oudere legacy-systemen bestonden nog uit speciale hardware, merkgebonden communicatieprotocollen en aparte communicatienetwerken. Moderne industriële besturingssystemen daarentegen bestaan uit standaard PC's en servers die communiceren via standaard IT-protocollen zoals IP, en delen hun netwerkomgeving met andere IT-eindgebruikernetwerken.
Deze verandering heeft diverse voordelen opgeleverd. Denk hierbij aan gereduceerde hardwarekosten en verhoogde flexibiliteit en bruikbaarheid.

Het bood de leveranciers van die industriële besturingssystemen bovendien de mogelijkheid om hun systeem te ontwikkelen op standaard Windows- of Unix-platformen. De systemen werden ook voorzien van 'features' om gemakkelijke data en rapportages te delen met andere IT- en netwerksystemen.
Gevolg hiervan is dat de grens tussen kantoorautomatiseringsomgevingen en de facilitaire industriële besturingssystemen in de afgelopen jaren vervaagde.

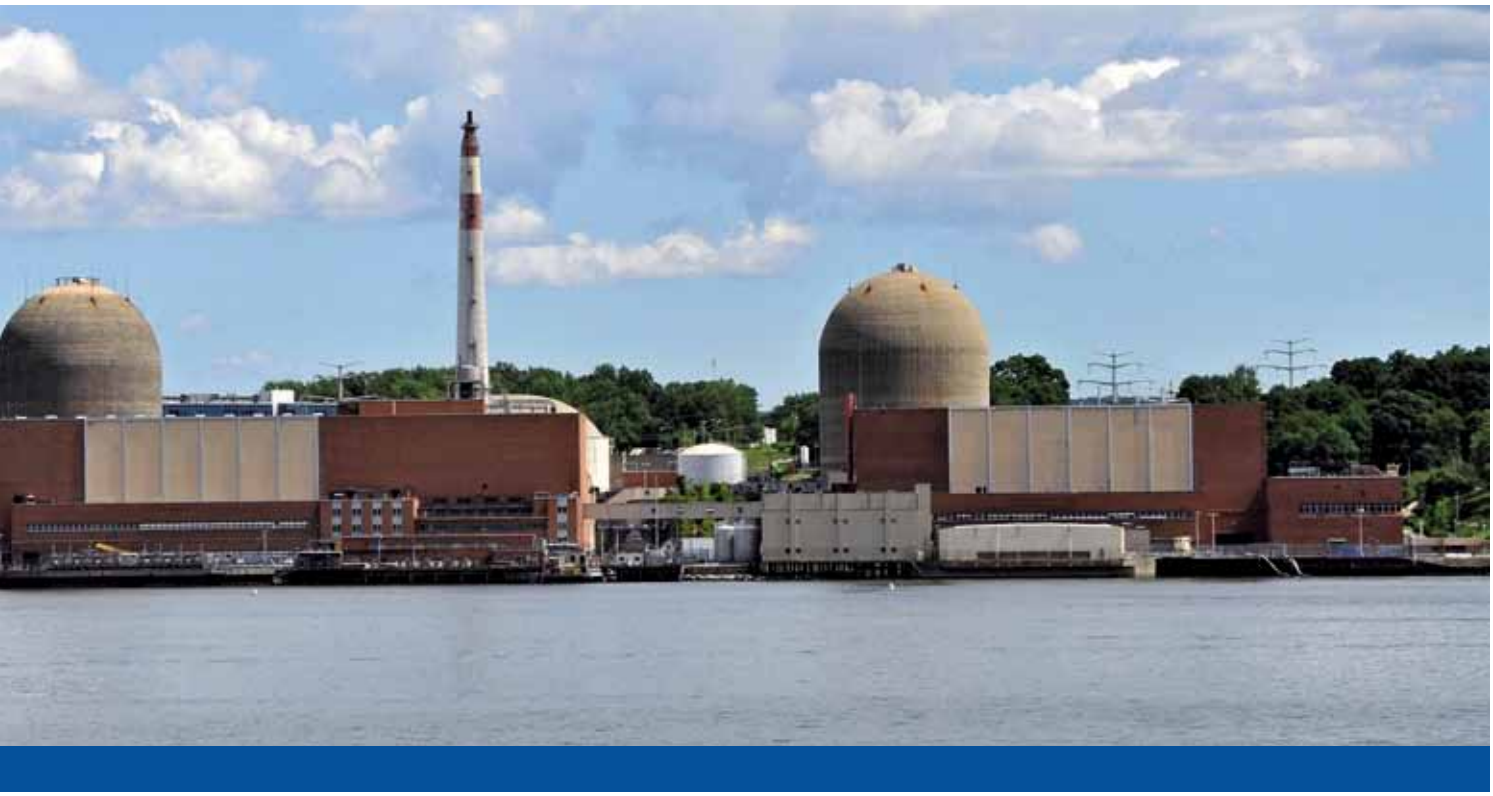


Dit had weer tot gevolg dat de nadelen van de traditionele IT-omgeving tastbaarder en groter werden, en met name de kans op 'cybercrime' toenam. In zijn 'Guide to Industrial Control System Security' waarschuwde het Amerikaanse National Institute of Standards and Technology (NIST) hier in 2008 al voor: "Widely available, low-cost Internet Protocol (IP) devices are now replacing proprietary solutions, which increases the possibility of cyber security vulnerabilities and incidents."

> Moderne SCADA-systemen bestaan uit standaard computers die communiceren via standaard protocollen

Het instituut had zich hierbij onder meer gebaseerd op het onderzoek dat een team 'Department of Energy' (DOE) engineers van het Idaho National Engineering Lab in 2007 had uitgevoerd in het kader van het Aurora Project. Samen met hackers van het Department of Homeland Security (DHS) startten de engineers een cyber-aanval met als doel een grote dieselgenerator te vernielen. Enkele minuten nadat de hackers toegang hadden gekregen tot het SCADA-systeem, hadden ze de generator al onder controle. Op een video die in 2009 werd getoond in het Amerikaanse CBS-programma '60 Minutes' was te zien dat de 27 ton wegende generator werd gestart, flink begon te schudden en na enkele seconden volledig in rook gehuld was. De generator overleefde de cyber-aanval niet.
Dit Aurora Project toonde daarmee aan dat het voor hackers mogelijk was via een netwerktoegang fysieke schade toe te brengen aan een generator. De hackers hadden hierbij kwetsbaarheden gebruikt die vandaag de dag in de meeste industriële besturingssystemen aanwezig zijn.

Beveiligen van een SCADA-netwerk
Maar zoals zo vaak heeft elk nadeel zijn voordeel. Het feit dat leveranciers van moderne SCADA-systemen deze hebben gebaseerd op standaard IT-onderdelen en -protocollen, heeft logischerwijs ook als voordeel dat er al veel kennis is over de beveiliging van dergelijke omgevingen.
Net als in de 'echte IT-wereld' begint een goed beveiligde omgeving bij het bepalen van de bedreigingen en risico's voor de organisatie en haar infrastructuur. Als de facilitaire systemen worden gecombineerd met de IT-omgeving is de stelling "we hebben toch een firewall" niet meer afdoende. Wat nodig is, is goed ontworpen zonering, zodat de buitenwereld - en ook de datastromen voor kantoorautomatisering - en de facilitaire systemen van elkaar zijn gescheiden met eigen zones. Hier hoort ook inspectie van de communicatiestromen bij met behulp van 'intrusion detection-systemen'.
Naast beveiligingsmaatregelen binnen een netwerk is het van belang servers, besturingssystemen, applicaties en databases goed te beveiligen en te voorzien van de laatste 'patches' en antivirussoftware. Niet alleen na installatie, maar in een doorlopend proces.
Tot zover de beveiliging die een organisatie zelf helemaal in de hand kan houden. Maar steeds meer facilitaire systemen hebben ook remote-support vanuit de leverancier. Het is hierbij zaak goed na te denken over welke informatie de organisatie mag verlaten. Daarnaast is het de overweging waard de leverancier alleen toegang te geven wanneer er daadwerkelijk een probleem ís. Het oplossen van storin-



gen vanuit de locatie lijkt ouderwets, maar geeft wel de meeste controle. Zeker wanneer de monteur wordt begeleid door iemand die inhoudelijk kan beoordelen wat hij uitvoert. Bovenstaande lijkt af te wijken van de visie van het Jericho Forum. Jericho gaat uit dat netwerken strikt genomen zonder 'firewall-slotgrachten' kunnen. Dit vanuit de overtuiging dat beveiliging wordt aangebracht daar waar dat nodig is op de servers en werkplekken. De traditionele firewall zou hierdoor overbodig worden. Wanneer de beveiliging op alle systemen integraal is geregeld, kan de firewall helemaal uit. Maar voordat dit moment is aangebroken voor SCADA-systemen, hebben veel organisaties en leveranciers nog een lange weg te gaan.

Kort over Jeroen Aijtink
Jeroen Aijtink is senior ontwerper bij de overheid. Hij houdt zich bezig met het ontwerpen van netwerkbeveiliging en veilige koppelingen naar externe netwerken. Aijtink is opgeleid in de Informatie- en Communicatietechnologie en heeft naast zijn CISSP-certificering veel detailkennis van security componenten.

Kort over Jan Wiersma
Jan Wiersma is technisch manager bij EvoSwitch, een toonaangevend, hypermodern datacenter in de regio Amsterdam dat geheel CO2 neutraal opereert. Wiersma is opgeleid in zowel de Informatie- en Communicatietechnologie als in de proces- en milieutechnologie. Hij vertegenwoordigt EvoSwitch in diverse nationale en internationale normencommissies zoals de ASHRAE (TC9.9), Open Datacenter Alliance (ODCA) en NEN (NC381888). Jan Wiersma is ook de internationale directeur EMEA voor DatacenterPulse, het platform voor eindgebruikers en exploitanten van datacenters. Jan is te bereiken via j.wiersma@evoswitch.com

> De generator werd gestart, begon te schudden en was na enkele seconden gehuld in rook

Stuxnet
In de lente van 2010 ontdekte de beveiligingsfirma VirusBlokAda een virus dat was geschreven om kwetsbaarheden in industriële besturingssystemen te exploiteren. Men vond een stuk malware in het industriële besturingssysteem van een Iraanse klant, verborgen in de programmacode dat de naam Stuxnet kreeg. Een analyse van Stuxnet door de beveiligingsfirma Symantec bracht aan het licht dat het een computerworm betrof die de mogelijkheid had om zich zelf van PC naar PC te verplaatsen en zich te vermenigvuldigen zonder menselijke interventie. Stuxnet heeft zelfs de mogelijkheid zich te verspreiden zonder een netwerkconnectie. Het analysedossier van Symantec beschrijft de worm als "een van de meest complexe die men ooit heeft geanalyseerd".

De complexiteit en het raffinement van het Stuxnet-virus maakte het al bijzonder, echter het doel van het virus maakt het echt uniek. Daar waar traditionele malware IT-systemen als doel had, was Stuxnet specifiek geschreven voor het aanvallen van industriële besturings- en SCADA-systemen. De worm vermenigvuldigde zichzelf via het internet van PC naar PC tot deze uiteindelijk via de PC, laptop of zelfs USB-disk van een nietsvermoedende onderhoudstechnicus toegang kreeg tot de juiste faciliteit. Zodra Stuxnet het juiste systeem kon infecteren, opende het virus een 'back door' waardoor ongeautoriseerde personen toegang kregen tot het facilitaire systeem. Op deze manier kon men gegevens van de lay-out en parameters van het SCADA-systeem downloaden. Daarnaast kon Stuxnet ongemerkt programmacode van PLC's herschrijven die onderdeel waren van de communicatie in het industriële besturingssysteem. Alle intelligentie voor deze actie was onderdeel van Stuxnet, en daarbij was geen externe toegang of hulp nodig. Op deze manier kon men de controle van het industriële besturingssysteem ongemerkt overnemen en enorme schade aanrichten in een bedrijfskritische omgeving.