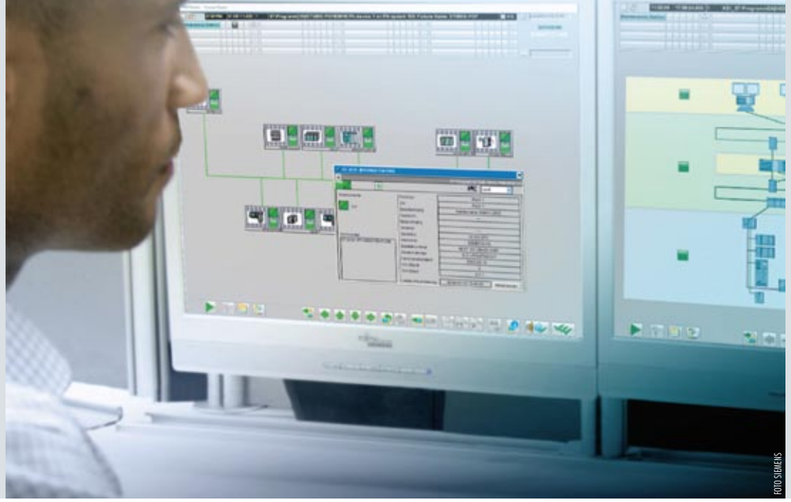
FOTO SIEMENS

Software van Siemens stuurt via PLC's fabrieksprocessen aan.

STUXNET ONTWORPEN OM FYSIEKE PROCESSEN IN FABRIEKEN PLAT TE LEGGEN

COMPLEXE COMPUTERWORM

De computerworm Stuxnet probeert in te grijpen op de fysieke processen van een specifieke centrale of fabriek. Het programma zit zo vernuftig in elkaar dat alles erop wijst dat er een grote organisatie achter de ontwikkeling zit. 'Na Stuxnet zal cyberspace nooit meer hetzelfde zijn.'

TEKST DR. JIM HEIRBAUT

'Stuxnet is het eerste kwaadwillende computerprogramma dat is ontworpen om de fysieke processen van een specifieke centrale te raken', zegt prof.dr. Sandro Etalle, hoogleraar Computerveiligheid aan zowel de TU Eindhoven als de Universiteit Twente en betrokken bij het bedrijf SecurityMatters. 'De worm is speciaal ontwikkeld om de software binnen te dringen die bepaalde typen Programmable Logic Controllers, PLC's, van Siemens aanstuurt.' Een PLC is een relatief ouderwetse, zeer degelijke microprocessor die in zowat alle hedendaagse fabrieken en energiecentrales voorkomt (zie het kader 'Programmeerbare microprocessor'). Hij kan van alles aansturen, van turbines en branders tot de kleppen in een pijpleiding en nucleaire centrifuges.

Stuxnet dringt Windows-computers voornamelijk binnen via geïnfecteerde USB-sticks, maar ook via een eventueel aanwezig netwerk. Daarbij maakt de worm gebruik van een aantal kwetsbaarheden in de programmatuur. Stuxnet, in juni openbaar gemaakt door een Wit-Russisch computerbeveiligingsbedrijf, gedraagt zich – in vaktermen – als *stealth*: het programma draait volledig op de achtergrond en is totaal onzichtbaar voor gebruikers. Het verschijnt bijvoorbeeld niet in de lijst van lopende processen van Windows. Stuxnet, dat zijn cryptische naam ontleent aan een regel code die de worm toevoegt, nestelt zich in een systeem door een *rootkit* te installeren, een soort achterdeurtje waarmee het blijvend toegang heeft tot het systeem. Via contact met andere computers of speciaal gebouwde websites kan het zich updaten.

De kerncentrale bij het Iraanse Bushehr vormt een mogelijk doelwit van Stuxnet.


FOTO WWW.LITLITES.NAE.COM

Na het binnendringen van een Windows-computer gaat de Stuxnet-worm op zoek naar de programma's WinCC en Step 7, de software om een door Siemens geproduceerde PLC aan te sturen. Als die software niet aanwezig is, gebeurt er met die computer niets, maar kan die wel als kiem dienen voor een volgende besmetting. Vindt het de Siemens-software wel, dan begint de eigenlijke aanval: de worm wijzigt delen van de softwarecode in de PLC en voegt regels toe. Het lijkt erop dat de toegevoegde stukjes code de hoogste prioriteit krijgen en elke 100 ms draaien. Wat daarvan precies het doel is, is nog niet geheel duidelijk. Wel hebben enkele specialisten al laten weten dat de wijzigingen waarschijnlijk ingrijpen op kritische processen, die snel mis kunnen lopen en waarbij potentieel veel schade optreedt. 'Zaken die met hoge toerentallen draaien, zoals turbines, knallen bijvoorbeeld uit elkaar als er niet snel wordt gereageerd', aldus Eric Byres van Byres Security in het tijdschrift *Wired*, ervaringsdeskundige met Siemens-controllers.

Siemens heeft laten weten dat wereldwijd vijftien fabrieken een besmetting met Stuxnet hebben gerapporteerd. Volgens het bedrijf hebben zij de worm succesvol verwijderd en hebben hun processen er geen schade van ondervonden. Volgens hoogleraar Etalle zijn de PLC's van Siemens niet slechter dan die van bijvoorbeeld ABB, Hitachi of Honeywell. 'Dat wijst er dus op dat de makers van Stuxnet een specifieke fabriek of centrale hebben willen aanvallen, waar PLC's van Siemens worden gebruikt.' Welke dat is, is niet duidelijk.

FOUTJES

De specialisten zijn het over een ding eens: Stuxnet is niet geschreven door de eerste de beste hacker. Daarvoor zijn de slimmigheden die erin zitten te talrijk. Zo maakt Stuxnet gebruik van vier zogeheten *zero day vulnerabilities* van de Siemens-software. 'Dat zijn foutjes in de code die nog niet eerder zijn ontdekt', licht Etalle toe. 'Vier stuks is zeer uitzonderlijk.' Ook bevat Stuxnet twee gestolen softwarecertificaten, waarmee het Windows wijsmaakt dat het betrouwbare en door onafhankelijke bedrijven geteste programmatuur is. Daarnaast is de verspreiding slim aangepakt. 'PLC's hangen uit veiligheidsoverwegingen vaak niet aan het netwerk', zegt dr. Herbert Bos, universitair hoofddocent van de sectie Computer Systems aan de Vrije Universiteit Amsterdam. 'Systeembeheerders updaten deze door even met een USB-stick naar een machine te lopen. Daarom is Stuxnet zo duivels goed: het probeert zo veel mogelijk computers in een fabriek te besmetten, zodat uiteindelijk ook de USB-stick van de systeembeheerder besmet raakt.'

Het indrukwekkendste vindt Etalle dat de Stuxnet-worm zich in de controller nestelt en daar regels code verandert. 'Dat is heel moeilijk en specialistisch. De hackers hebben dat ongetwijfeld maandenlang op PLC's moeten testen.' Met 1,5 MB aan code is de worm volgens Etalle ook uitzonderlijk groot. Die code is overigens in verschillende programmeertalen geschreven, waaronder C en C++. 'Hier moeten tien man meer dan een jaar aan hebben gewerkt', aldus Etalle. 'Het is alsof cyberoorlogvoering de stap maakt van een tank naar een F-15.'

Het is een conclusie die vele computerbeveiligingsexperts in vakmedia en internetfora met hem delen. Daar doen ook veel speculaties de ronde over de herkomst van de worm. Aangezien naar verluid zo'n 60 % van de besmettingen in Iran is aangetroffen, lijkt de worm daar gericht te zijn verspreid. De speculaties richten zich vooral op twee locaties: de kerncentrale die bij de stad Bushehr in aanbouw is, en de fabriek met ultracentrifuges voor uraniumverrijking bij Natanz. Het moge duidelijk zijn dat buurland Israël, maar ook de Verenigde Staten daar niet op zitten te wachten. Maar of zij achter Stuxnet zitten, is puur speculatief.

PATCHES

Verrassend genoeg blijken de PLC's, die vaak cruciale processen aansturen in fabrieken of energiecentrales, slecht beveiligd tegen aanvallen van buitenaf. Volgens Etalle heeft dat te maken met de historie van de apparaten. 'PLC's stammen uit de tijd ver voor het internet. Toen waren computers nog niet met elkaar verbonden en was digitale veiligheid dus geen issue.' Daarnaast zijn er voor PLC's nauwelijks *patches* beschikbaar, digitale pleisters die dienen om foutjes in een besturingssysteem te herstellen. 'Bij een PLC zijn programmeurs daar niet erg happig op, omdat die vaak een kritisch proces aanstuurt. Ze willen van cruciale infrastructuur niet zomaar de programmatuur veranderen.'

Volgens de Duitse IT-veiligheidsexpert Ralph Langner is niet Stuxnet zelf de grootste bedreiging, maar juist de mogelijkheid dat de technieken die in de worm voor het eerst zijn gebruikt, gemeengoed worden onder hackers. 'Stuxnet is een blauwdruk voor een cyberaanval op geautomatiseerde processen. Dat maakt het voor mensen met plannen in die richting een stuk eenvoudiger', aldus Langner op zijn website. 'Nu Stuxnet overal rondzwerft, zijn cyberwapens geen kwestie meer van technologische knowhow, maar van geld.'

Toch is volgens Langner de dreiging van cyberaanvallen op kritische infrastructuur nu juist kleiner geworden. 'De ontwerpers van Stuxnet hebben geprofiteerd van een verrassingseffect. Niemand heeft de aanval zien aankomen en het beschermingsniveau van de systemen was dus nagenoeg nul. Dat is nu wel anders – althans, dat zou het moeten zijn.'

Overheden en commerciële beheerders van kwetsbare locaties als energiecentrales en olieleidingen moeten volgens Langner hard aan de slag hun systemen beter te beveiligen. Voor kritische infrastructuur is dat te doen, omdat de aantallen zijn te overzien. Meer risico lopen de minder cruciale targets, zoals fabrieken, verkeerslichten of liften. Langner: 'Die zijn zo talrijk dat we niet moeten denken dat die op korte termijn afdoende beveiligd zullen zijn.' Dat een enkel verkeerslicht plat is te leggen, is wellicht niet zo erg. Maar Langner waarschuwt dat een gecoördineerde aanval de economie net zo veel schade zou kunnen toebrengen als een aanval op een energiecentrale. 'De industrie heeft lange tijd in de luxe geleefd geen last te hebben van aanvallen op de geautomatiseerde processen. Dat is in één klap veranderd. Na Stuxnet zal cyberspace nooit meer hetzelfde zijn.'

WAKKER

'De gebruikers van PLC's moeten nu wakker schrikken', vindt ook Etalle. 'Hun kritische processen blijken kwetsbaar te zijn voor hackers.' Of bedrijven zelf de kosten kunnen opbrengen om hun computerbeveiliging naar een voldoende hoog niveau te tillen, is zeer de vraag. Etalle: 'Stuxnet bewijst dat er minstens één lab bestaat dat veel geld heeft om gerichte cyberaanvallen te doen. Misschien bestaan er al meer van dit soort labs, en anders zullen ze zeker worden opgericht. Bepaalde landen zullen niet willen achterblijven. Daarom denk ik dat Stuxnet het signaal moet zijn dat overheden cyberoorlogvoering moeten tegengaan.'

FOTO SIEMENS

De S7-300 van Siemens, een van de PLC-typen die de worm aanvalt.

PROGRAMMEERBARE MICROPROCESSOR

Een Programmable Logic Controller (PLC) is een elektronisch apparaat met een microprocessor, dat een industrieel proces aanstuurt. Om een PLC te programmeren wordt hij via een datakabel aangesloten op een gewone pc met de juiste software. De programmeur kan vanuit deze omgeving in het geheugen van de microprocessor kijken, de PLC herconfigureren, er een programma op laden of fouten uit het bestaande programma halen. Daarna functioneert de PLC weer zelfstandig.