Cybersecurity

Relevante trends voor Defensie

Wereldwijd stijgt het aantal incidenten door cybercriminaliteit sterk. Door computers te besmetten kunnen criminelen deze computers inzetten voor eigen gewin. Hier worden miljoenen mee verdiend. Geleidelijk aan raken steeds meer zakelijke en privé computers besmet met virussen en wordt ontsmetting moeilijker. Daarnaast professionaliseert de cybercriminaliteit. De strijd tussen verdedigers en aanvallers is inmiddels een wedloop geworden. Kennis van het cyberdomein is voor de defensieorganisatie essentieel, omdat ze sterk afhankelijk is van informatiesystemen. Software met een groot marktaandeel is extra aantrekkelijk voor cybercriminelen. Het zou daarom goed zijn als Defensie de huidige IT-monocultuur doorbreekt door diversiteit te bevorderen en meer gebruik te maken van 'open source'-systemen.

*H.J. van der Molen**

Sinds 27 juni 2012 heeft Defensie een cyberstrategie. Hiermee onderkent zij de noodzaak van een effectieve inzet van digitale middelen om haar hoofdtaken uit te kunnen voeren.[1] De hoofdtaken uit deze strategie zijn als volgt samengevat: het beschermen van de vitale belangen van Nederland, het bevorderen van de (inter)nationale rechtsorde en het ondersteunen van civiele autoriteiten bij de bestrijding van rampen, zowel in nationaal als internationaal verband.

Behalve de capaciteit om effectief te kunnen opereren in het cyberdomein, moet Defensie dus ook adequaat en proportioneel kunnen reageren op cyberaanvallen die Nederlandse vitale belangen bedreigen of rampen (kunnen) veroorzaken. Daarnaast onderstreept de cyberstrategie dat Defensie zowel defensieve als offensieve cyberacties moet kunnen uitvoeren.

Inleiding

Of een cyberincident wordt beschouwd als een cyberaanval wordt onder meer bepaald door de impact. Zowel bij een cyberincident als bij een cyberaanval is het moeilijk om de inbraak te signaleren, de ingezette middelen vast te stellen, de aanvaller te identificeren en diens intentie vast te stellen. Doordat de meeste *malware* (een verzamelnaam voor programmatuur met een kwaadaardige functionaliteit) elke kwetsbare computer probeert te besmetten is het zelfs voor de makers moeilijk om de impact van hun malware te voorspellen.

Defensie is sterk afhankelijk van informatiesystemen die bijvoorbeeld de commandovoering ondersteunen. Het is inmiddels bewezen dat ook militaire systemen die de *Observe-Orient-Decide-Act* cyclus ondersteunen kwetsbaar zijn voor cyberaanvallen.[2]

Defensie moet kunnen beschikken over voldoende cyberkennis om het cyberrisico voor de eigen systemen te verminderen en om mee te kunnen denken over de bescherming van Nederlandse (civiele) vitale systemen.

* De auteur is freelance docent bij de Hogeschool Wageningen, onder meer op het gebied van informatiebeveiliging, *business intelligence*, verandermanagement en strategisch IT-management. Hij heeft diverse artikelen gepubliceerd op ICT-gebied en geeft regelmatig lezingen.

1 *Defensie Cyber*-strategie: www.rijksoverheid.nl.

2 Zie bijvoorbeeld hoofdstuk 4 'The Defense fails', in: *Cyber War*, R.A. Clarke.

Opzet artikel
Ik ga eerst in op trends van cyberincidenten en een economische model achter cyberaanvallen. Op basis daarvan geef ik aan waarom het risico van cyberincidenten moeilijk te verminderen is, onder welke omstandigheden dat risico het grootst is en welk effect beveiligingsmaatregelen hebben. De problematiek speelt voor zowel organisaties als Defensie als voor individuele computergebruikers. Het artikel is bedoeld voor beleidsmakers, IT-personeel en defensiemedewerkers. De context is waar mogelijk toegesneden op Defensie. Ik rond af met conclusies en aanbevelingen.

De kans op besmetting met malware

In de civiele wereld stijgt het aantal cyberincidenten momenteel sterk, vooral door de inzet van malware. Door computers met malware te besmetten kunnen cybercriminelen deze computers ongemerkt voor eigen gewin inzetten (zie tabel 1).

In 2010 bevatte 1 op de 284 e-mails (0,35 procent) malware. In 2011 nam dat toe tot 1 op 239 e-mails (0,42 procent) en steeg het aantal unieke malware-varianten met 41 procent tot 403 miljoen.[3] De criminele bedrijfstak rond malware groeit, omdat er miljoenen mee verdiend worden.[4] Bijvoorbeeld door verkoop van gevoelige bedrijfsinformatie, chantage, afpersing, frauderen met creditcardgegevens en click-fraude met online advertenties.

Steeds meer financiële schade
Cybercrime veroorzaakt hierdoor steeds meer financiële schade voor personen, organisaties en de samenleving als geheel. Daarnaast neemt de dreiging van een cyberaanval op vitale systemen toe. Al in 2003 was een alarmpaneel van een Amerikaanse nucleaire installatie vijf uur lang onbruikbaar omdat dit systeem met een worm was besmet.[5]

3 MessageLabs Intelligence: 2010 Annual Security Report, 7 december 2010: www.clearnorthtech.com; Internet security Threat Report 2011 Trends, www.symantec.com.
4 'How Cybercriminals Make Their Millions': www.escurityplanet.com, 22 december 2010.
5 Informatiebeveiliging juni 2008, 'Beveiliging procescontrole is onderbelicht onderwerp', Eric Luiijf, www.pvib.nl.

Categorie	Beschrijving	Mogelijke acties malware
Computer virus	Kan zichzelf vermenigvuldigen en verspreiden naar andere computers, bijvoorbeeld door koppelen aan bestaande software	• Bestanden downloaden, aanpassen of verwijderen • Schermafdrukken maken • Toetsaanslagen registreren (wachtwoorden!) • Op afstand de microfoon of de camera inschakelen • Mail (spam / malware) versturen • Privacygevoelige informatie uploaden • (verborgen) Accounts aanmaken • Besmetten verbonden computers via netwerk, USB-drives en Bluetooth • Communicatie afluisteren
Computer worm	Een op zichzelf staand computerprogramma, dat zich kan verspreiden naar andere computers binnen hetzelfde netwerk	
Trojaans paard	Malware vermomd als nuttige software, zoals anti-virussoftware	
Bot	Door een 'achterdeurtje' heeft de aanvaller via het internet volledige controle over alle besmette computers in zijn 'botnet'. Het 'Zwitserse zakmes' van de cybercrimineel	
Spyware	Stuurt identiteitsgegevens (zoals wachtwoorden en creditcard- gegevens) van de computergebruikers door naar de aanvaller	
Rootkit	Software met beheerdersrechten die zich verborgen kan houden voor normale detectiemiddelen, zoals anti-virussoftware	

Tabel 1. Verschillende soorten malware

Cybercriminelen kunnen computers met malware infecteren door kwetsbaarheden in de software te misbruiken.[6] Elk gedownload computerprogramma kan malware bevatten, maar ook bestanden met macro's, beeld, geluid of video. Een computer kan zelfs al een malwarebesmetting oplopen door één besmette website te bezoeken.

Een Amerikaans beveiligingsbedrijf constateerde in 2009 dat 60 procent van de onderzochte websites tenminste één ernstig beveiligingslek heeft.[7] In 2010 werden gemiddeld 3188 malafide sites per dag geblokkeerd, waarvan bijna 90 procent legitieme sites die waren gehackt. In 2012 had Nederland – na Rusland en de VS – de meeste websites die malware verspreiden.[8]

Ongerichte aanvallen

Hoewel malware-aanvallen soms worden gericht op individuele personen of organisaties, probeert de meeste malware ongericht alle systemen te besmetten waarmee het in contact komt. Cybercriminelen zijn geneigd om malware voor gerichte aanvallen waarmee geld werd verdiend, ook elders in te zetten. Malware is daarom afhankelijk van (kwetsbaarheden in) bepaalde software om zich te kunnen verspreiden naar onbesmette systemen.

Informatietechnologie (IT) maakt nog steeds een explosieve groei door en ijlt soms na op de ontwikkelingen. Daardoor bevat alle software fouten of kwetsbaarheden die een cyberaanval mogelijk maken. Van de kwetsbaarheden die bijvoorbeeld tussen juli 2011 en maart 2012 bekend werden, blijkt 55 procent relatief eenvoudig uit te buiten en is circa 90 procent van de kwetsbaarheden vanaf het internet uit te buiten.[9]

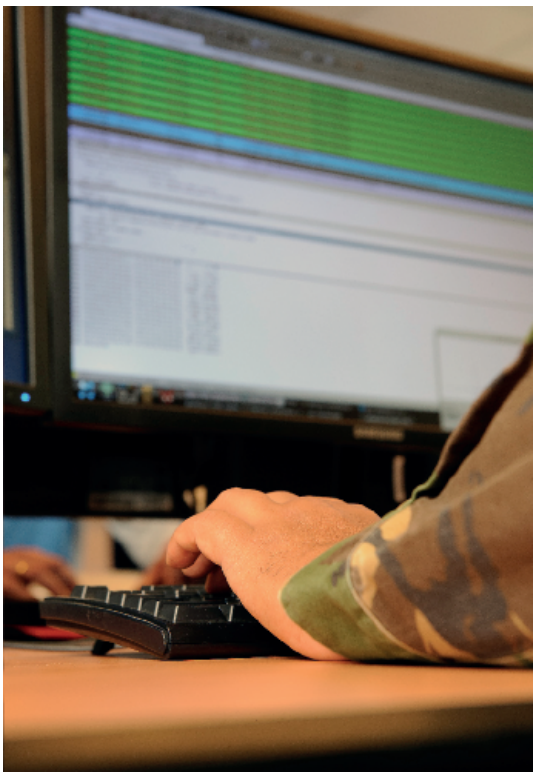

FOTO AVDD, H. LEBBE

Informatietechnologie maakt nog steeds een explosieve groei door. Defensie is sterk afhankelijk van informatiesystemen, bijvoorbeeld voor het ondersteunen van de commandovoering. Hierdoor is Defensie kwetsbaar voor cyberaanvallen

Om fouten in hun software te repareren verspreiden leveranciers updates (*patches*) via internet. In 2010 werd tot dan toe het grootste aantal kwetsbaarheden in software gepubliceerd, terwijl 44 procent van alle aan het licht gekomen kwetsbaarheden niet kon worden gerepareerd voor het einde van dat jaar. 95 Procent van deze kwetsbaarheden werd geclassificeerd als 'medium zwaar'.[10]

Door een uitgebrachte software-update te vergelijken met de oude software kan men eenvoudig signaleren welke kwetsbaarheden de update repareert. Het is een Amerikaanse universiteit gelukt om uit een software-update automatisch de malware te genereren die niet-geüpdate computers kan aanvallen.[11] Het vermoeden wordt steeds sterker dat cybercriminelen deze procedure stelselmatig kunnen toepassen. Zo werd in 2009 circa 60 procent van de gemelde kwetsbaarheden actief misbruikt.[12]

6 In dit artikel worden de termen 'malware' en 'exploits' gebruikt als synoniemen; meestal misbruikt een exploit een kwetsbaarheid in software en kan daardoor malware downloaden en installeren

7 'WhiteHat Security Statistics Report', 18 mei 2009, www.whitehatsec.com.

8 'Kaspersky Lab, IT threat evolution Q3 2012', 1 november 2012, www.securelist.com.

9 'Cyber Security Beeld Nederland' (CSBN-2) juni 2012 (nscs.nl), www.nctb.nl.

10 'Symantec Corp., Internet Security Threat Report' Vol. 16, april 2011, www.symantec.com.

11 *Automatic Patch-Based Exploit Generation*, Carnegie Mellon University, UC Berkeley, CMU, U. Pittsburgh, 2008, www.cs.cmu.

In 2011 verslechterde deze situatie: ongeveer 97 procent van alle kwetsbaarheden werd binnen twee weken na publicatie misbruikt.

Vrij spel

Totdat de kwetsbaarheden worden gerepareerd, heeft malware vrij spel. Zodra een softwareleverancier een update uitrolt, moeten gebruikers van deze software die zo snel mogelijk installeren. Hoe langer het duurt om kwetsbaarheden te repareren, des te groter de kans dat kwetsbare systemen ondertussen met malware worden besmet. Organisaties lopen soms achter bij het doorvoeren van updates, bijvoorbeeld omdat ze de uitgebrachte updates eerst willen testen of door slecht systeembeheer. Helaas komt dat laatste vaak voor: de zogeheten 'SQL Slammer'-worm met de bijbehorende reparatie-update verschenen al in 2003. Toch genereerden de systemen die nu nog met deze malware zijn besmet in 2010 het meeste verkeer van alle malware op het internet.

Uit onderzoek blijkt dat cybercriminelen steeds sneller malware kunnen ontwikkelen omdat hun kennis van IT toeneemt en omdat ze onderling samenwerken.[13] Al in 2003 werd bijvoorbeeld voor het schrijven van de succesvolle 'Sobig'-worm universitaire kennis ingezet, zijn delen van andere malwarevarianten hergebruikt en zijn er verschillende testversies uit-gebracht.[14]

Zwarte markt

Op de zwarte markt wordt malware verkocht, ook voor de nieuwste systemen. Een netwerk met 10.000 besmette pc's is ongeveer $ 800,- waard en kan per uur worden gehuurd, bijvoorbeeld om spam te versturen of een webwinkel plat te leggen en zo geld af te persen.[15]
De 'Storm'-worm malware heeft naar schatting anderhalf miljoen computers besmet; deze malware zou in 2007 20 procent van alle spam wereldwijd hebben verstuurd. Het 'Conficker'-virus kon in 2008 miljoenen besmette pc's flexibel inzetten doordat het virus nieuwe versies van zichzelf kon installeren.[16] In 2011 registreerde een beveiligingsbedrijf tot zijn verrassing 1,2 miljoen pc's die waren besmet met de 'Ponmocup'-malware – in 24 uur.[17]

Het is bekend dat medewerkers de meeste incidenten binnen organisaties veroorzaken. De gemiddelde computergebruiker weet weinig over beveiliging, waardoor privécomputers vaak en langdurig besmet zijn. Veel mensen gebruiken bijvoorbeeld thuis dezelfde kantoorsoftware als de zakelijke standaard. Als organisaties deze software niet gratis verstrekken, downloaden veel mensen illegale software, die vaak besmet is met malware. Bovendien verbeteren cybercriminelen continu hun zogeheten *social engineering*-technieken om personen te verleiden tot onveilig gedrag.[18] Als ondeskundigen malware langer in omloop houden is dat ook nadelig voor goed beveiligde systemen met dezelfde kwetsbaar-heden. Omgekeerd is het beter beveiligen van computers van ondeskundige eigen medewerkers ook voordelig voor de organisatie.[19]

Defensie

Defensie doet er goed aan om de privécomputers van medewerkers te beschouwen als mogelijk besmet met malware. Als een medewerker op zijn besmette computer thuis werkt aan een zakelijk document kan bedrijfsinformatie naar buiten lekken. De oplossing met de telestick van Defensie maakt het buitmaken van bedrijfsinformatie wel een stuk moeilijker maar niet onmogelijk (zie tabel 1). Daarnaast moeten medewerkers zich ervan bewust zijn dat een aanval op hun organisatie kan starten vanaf hun privécomputer. Zakelijke computers en privécomputers van medewerkers zijn vaak direct gekoppeld via e-mail en USB-drives. Dergelijke koppelingen kunnen malware overdragen. Voor de hand liggende maatregelen

12 Fortinet, Threatscape Report, juni 2009, www.fortiguard.com/report/roundup_june_2009.html
13 P. Bueno,'Malware Analysis—Lessons Learned', SANS Internet Storm Center, http://handlers.sans.org.
14 'Who wrote the Sobig?', Author Travis Group, 2003-2004, http://spamkings.oreilly.com.
15 Zie www.security.nl/artikel/30701/1/Besmette_Windows_computer_10_cent_waard.html
16 'Midyear Security Report: An Update on Global Security Threats and Trends', Cisco Systems Inc., 2009, www.cisco.com.
17 'How Big is Big? Some Botnet Statistics', 23 mei 2011, www.abuse.ch/?p=3294.
18 Social Engineering Fundamentals, Part I: Hacker Tactics, www.symantec.com.
19 'On the Malware Front', R.E. Kooij, H.J. van der Molen, *International Journal of Computer Networks* (IJCN), 4 (4) (2012) http://cscjournals.org.

zijn dan vreemde USB-apparaten te weren op de werkplek, en thuiswerken alleen toe te staan op zakelijke hard- en software.

Beveiliging is geen garantie

Steeds meer organisaties koppelen systemen aan het internet (Web 2.0), zoals internetbanken, webshops en online nutssystemen. Dit vergroot de kans dat malwarebesmettingen bedrijfsprocessen verstoren. Ook de overheid loopt meer risico: de ambitie was om in 2007 minstens 65 procent van de dienstverlening via internet te laten lopen. Het aantal gekoppelde overheidssystemen neemt verder toe door het wettelijk verplichte gebruik van Nederlandse basisregistraties, zoals de GBA en het KvK-register. Door de toename van systemen, centralisatie en uniformering van software lijken ICT-infrastructuren steeds meer op elkaar en neemt de afhankelijkheid van ICT toe.[20]

Grote organisaties zoals Defensie hebben hun computersystemen vaak beter beveiligd, bijvoorbeeld doordat medewerkers zelf geen software kunnen installeren. Daarom lijken incidenten met malware voornamelijk voor te komen bij individuele computergebruikers of kleine bedrijven, maar dat beeld is niet representatief. Het blijkt dat 16 procent van de Nederlandse organisaties al in 2008 last hadden van incidenten met malware.[21] In de VS was 50 procent van de cyberaanvallen (in 2011) gericht op organisaties met meer dan 2500 medewerkers. 42 Procent van de zogeheten *spear phising* aanvallen (persoonlijke e-mails van een 'kennis') werd gericht op seniormanagers en R&D-personeel.

Gerichte aanvallen

Overheden en de publieke sector kregen in 2011 25 procent van deze gerichte e-mail-aanvallen. Ook de systemen van de 'Fortune 500'- bedrijven zijn gehackt.[22] In 2011 maakten aanvallers de details buit van het zogeheten RSA-beveiligingssysteem, dat miljoenen medewerkers gebruiken om thuis veilig te kunnen werken. Zelfs de FBI gaf in maart 2012 aan dat de verdediging van IT-systemen niet is opgewassen tegen de tools die aanvallers gebruiken.[23]

Organisaties detecteren bovendien niet alle inbraken op hun systemen, bijvoorbeeld bij bedrijfsspionage. Ook doen weinig organisaties aangifte van cyberaanvallen omdat ze negatieve publiciteit willen vermijden. Inbraken die leiden tot een faillissement vormen echter geen uitzondering meer.[24] Hoewel de veiligheidsmaatregelen verschillen tussen de diverse organisaties en landen kunnen geslaagde aanvallen vaak met succes worden hergebruikt. Medewerkers en managers zijn zich vaak onvoldoende bewust van de waarde van de informatie waarover zij beschikken en het belang van informatiebeveiliging.

Daarom vraagt de AIVD sinds 2010 organisaties nadrukkelijk om een KWetsbaarheids Analyse Spionage (KWAS) uit te voeren en maatregelen te nemen.[25]

Wedloop

De strijd tussen verdedigers en aanvallers is een wedloop (zie de voorbeelden van acties en tegenacties in tabel 2). Zelfs een ICT-infrastructuur met de veiligste instellingen is niet immuun voor alle malware-aanvallen.[26] De maatregelen tegen malware blijken namelijk steeds minder effectief om incidenten te voorkómen. Zo wordt er regelmatig malware gevonden die kwetsbaarheden misbruiken, waartegen nog geen beveiligingsmaatregel bestaat, de zogeheten *Zero-day exploits*.[27] Ook beveiligingsmaatregelen zoals 'twee factor authenticatie' (naast een wachtwoord een *security token* invoeren, zoals bij internetbankieren of telewerken) is niet opgewassen tegen de nieuwste malware.

20 De rijksoverheid wil met het plan 'Compacte Rijksdienst' het aantal rekencentra terugbrengen van 64 naar vier à vijf.

21 'Resultaten ICT Barometer Over ICT-beveiliging en Cybercrime', Ernst & Young, 28 januari 2009, op www.ict-barometer.nl.

22 CNN, 28 oktober 2011 'Massive hack hit 760 companies', http://money.cnn.com.

23 'U.S. Outgunned in Hacker War', http://online.wsj.com.

24 'DigiNotar failliet verklaard', *NRC Handelsblad*, 20 september 2011, www.nrc.nl.

25 'Weerbaarheid overheid en bedrijfsleven tegen spionage wordt vergroot', https://www.aivd.nl.

26 Incident Management broodnodig', *Computable*, 26 mei 2006; zie ook Govcert Trendrapport 2007

27 SearchSecurity.com, 'Exploit Code Targets Internet Explorer Zero-day Display Flaw', 23 november 2009; 'Microsoft Word Zero-day Being Actively Exploited', 8 juli 2008.

Beveiliging tegen malware	Tegenacties cybercriminelen
Verlagen besmettingskans Antivirussoftware, firewall, sterke wachtwoorden, beperkte gebruiksrechten, periodieke veiligheidsonderzoeken, betere beveiligingskennis	**Verhogen besmettingskans** Testen van malware, gerichte malware, imitatie van legale software, malware op vertrouwde websites, encryptie malware
Verbeter ontsmetting (detectie & correctie) Logging, Incident Management-procedures, betere beveiligingskennis, 'post mortem' onderzoeken	**Bemoeilijk ontsmetting** Encryptie communicatie, malware update sneller dan antivirussoftware, malware wist de sporen, continuïteitsplan voor botnets

Tabel 2. De wedloop tussen cybersecurity en cybercrime

Ook overheden zijn betrokken bij cyberaanvallen, zoals Rusland tegen Estland in 2007. In juni 2010 is het Stuxnet-virus ontdekt. Dit virus wordt beschouwd als het eerste strategische cyberwapen. Het kon specifieke Siemens-systemen saboteren die onder meer in Iran werden gebruikt voor nucleaire ultracentrifuges. Het Stuxnet-virus vermenigvuldigde zich onder meer via USB-drives en verborg zijn aanwezigheid op besmette computers. Het virus bevatte meerdere Zero-day exploits en een softwarecomponent die ondertekend was met gestolen certificaten.

Op basis van deze complexiteit schat men de benodigde tijd om Stuxnet te ontwikkelen op circa tien manjaren. Sinds 2010 staan de ontwikkelingen echter niet stil: de opvolgers van Stuxnet zijn al gesignaleerd.[28] De AIVD signaleerde in april 2011 dat de digitale spionage van onder meer China en Rusland toeneemt. Bij een destructieve cyberaanval in augustus 2012 werden er alleen al bij het Saoedische energiebedrijf Aramco meer dan 30.000 werkstations besmet. Op basis van de fouten in het virus worden de ontwikkelaars aangemerkt als 'getalenteerde amateurs'.[29] Ook cybercriminelen en anarchisten richten zich steeds meer op het hacken van industriële systemen die bijvoorbeeld kerncentrales, waterbedrijven en sluizen aansturen.[30]

Professionalisering van cybercrime

Criminelen willen ook in crisistijd veel geld verdienen, en cybercrime met zijn anonieme slachtoffers is dan een aantrekkelijke optie. Om de verdienste te maximaliseren moet malware verborgen blijven, moet de verspreiding van malware 24/7 doorgaan en moet een besmetting met malware zo lang mogelijk duren. Daarvoor worden bijvoorbeeld encryptie en roulerende webservers ingezet, zodat het uitschakelen van enkele servers weinig effect heeft.

Virusscanners

Al in 1992 was bekend dat detectiesystemen nooit de afwezigheid van alle malware kunnen aantonen; alleen de afwezigheid van *bekende* malware.[31] Cybercriminelen verifiëren tegenwoordig voorafgaand aan de verspreiding dat virusscanners hun malware niet herkent. Door voor elke besmetting unieke malware te genereren en deze selectief te richten op enkele organisaties verschijnt nieuwe malware niet

28 F-Secure 2 juni 2012, 'On Stuxnet, Duqu and Flame', www.f-secure.com.

29 'Shamoon Malware and SCADA Security – What are the Impacts', 25 oktober 2012, https://www.tofinosecurity.com.

30 'Hackers richten pijlen op kerncentrales', *Webwereld*, 26 oktober 2012, zie: http://webwereld.nl.

31 'Defense in Depth against Computerviruses', Cohen, F.B., *Computers & Security* 11 (6) 1992.

meer op de radar van de leveranciers van antivirussoftware. Volgens verschillende onderzoeken laten zelfs up-to-date virusscanners circa 60 procent van alle nieuwe malware door.[32]

Mede vanwege de tijd die nodig is om nieuwe antivirussoftware uit te rollen detecteren virusscanners in de regel pas malware als die meer dan vier weken oud is. Er circuleert al malware die niet gedetecteerd kan worden, omdat die sneller updates ophaalt van het internet dan dat virusscanners worden bijgewerkt. Het zogeheten heuristisch scannen – het bepalen van de waarschijnlijkheid dat een bestand een virus bevat – biedt hiervoor geen goede oplossing: het leidt tot (te) veel valse positieven. Dat zowel commerciële software als malware vaak is ingepakt in vercijferde zipbestanden maakt de detectie van malware veel moeilijker. Sommige virusscanners kunnen malware detecteren aan de hand van het gedrag, maar dan is het systeem al besmet en is de veiligheidssoftware mogelijk al uitgeschakeld. Natuurlijk bestaan er meer geavanceerde beveiligingssystemen, maar die hogere effectiviteit vergt een groot budget en veel kennis. Ook voor dergelijke systemen kunnen geen garanties worden afgegeven.

Lage pakkans, hoge inkomsten

Mensen die aangifte doen van computercriminaliteit merken vaak dat de daders niet worden veroordeeld, omdat het achterhalen van de daders moeilijk is, cyberbendes meestal vanuit het buitenland opereren en er alles aan doen om de dans te ontspringen. Door de lage pakkans en hoge inkomsten laat het aantal malwareprogramma's een exponentiële groei zien.[33] Het aantal virussen is zo groot omdat *one click* viruskits op het internet weinig of geen geld kosten en omdat criminelen hetzelfde virus opnieuw kunnen gebruiken door deze vercijferen met een unieke sleutel.

Antivirus-softwareleverancier Kaspersky meldde al in 2006: *'We're losing this game. There are just too many criminals active on the Internet underground, in China, in Latin America, right here in Russia. We have to work all day and all night just to keep up'*.[34] Het beveiligingsbedrijf F-Secure meldde daarna dat de hoeveelheid malware in 2007 verdubbelde en in 2008 nog eens verdrievoudigde. Vanwege de grote hoeveelheid malware die in omloop is, komt het regelmatig voor dat computers besmet zijn met meerdere virussen tegelijk.

Malware is gericht op het marktaandeel van de software

Aan het hand van deze gegevens kan het economische model van malware worden bepaald. Bijna alle software bevat kwetsbaarheden die uitgebuit kunnen worden door malware. Cybercriminelen moeten blijven investeren in de ontwikkeling van malware omdat ze continu nieuwe kwetsbaarheden moeten zoeken en de ontwikkelingen van antivirussoftware vóór moeten blijven. Omdat cybercriminelen de kans willen maximaliseren dat ze die investering terugverdienen is hun inkomstenmodel samen te vatten met de volgende stelling:

Stelling 1 – Professionele cybercriminelen maximaliseren de 'return-on-investment' van hun malware (P x Q) door te focussen op Kwantiteit (Q), niet op de Prijs (P) per besmette computer

Hierbij staat Q (Kwantiteit) voor het aantal computers dat per malware-aanval wordt besmet en P (Prijs) voor de gemiddelde opbrengst per gehackte computer. Focussen op P vergt specifieke voorkennis en biedt minder zekerheid. Het kraken van één systeem met waardevolle bedrijfsgeheimen kan weliswaar veel geld opleveren, maar dergelijke systemen zijn vaak goed beveiligd.

Focussen op kwantiteit biedt meer zekerheid qua inkomsten omdat veel computers onvoldoende zijn beveiligd. Bovendien is het eenvou-

32 'Do Anti virus Products Detect Bots?', Staniford, S., FireEye Malware Intelligence Lab, 20 november 2008, http://blog.fireeye.com. Zie ook *Retrospective/Proactive Test, AV-Comparatives.org, May 2011*, www.av-comparatives.org.

33 F-Secure, 'F-Secure IT Security Threat Summary for the Second Half of 2008', www.f-secure.com.

34 'The Zero-Day Dilemma', Naraine, R., eWeek.com, 24 januari 2007, www.eweek.com.

Categorie	Softwareproduct	Markt % (schatting)	Datum en bron schatting	Populariteit bij criminelen
Office suite	MS Office	88 (v)	mei 2010 Webmasterpro.de	zeer hoog
Operating system	Windows	85 (i)	mei 2012 Marketshare.com	zeer hoog
Web client	Internet Explorer	54 (i)	mei 2012 Marketshare.com	zeer hoog
Web server	Apache	65 (i)	januari 2012 Netcraft	hoog
Database server	Oracle	49 (v)	maart 2012 Gartner	hoog

(v = aantal verkocht, i = internet onderzoek)

Tabel 3. Marktaandeel software en aantrekkelijkheid voor cybercriminelen

diger omdat alleen informatie nodig is over de verhoudingen in de softwaremarkt. Bijkomend voordeel is dat als er duizenden gedupeerden aangifte doen van een kleine diefstal, vervolging voor justitie moeilijker is dan wanneer één partij aangifte doet van een groot misdrijf.

Volgens het *Nationale trendrapport Cybercrime en Digitale Veiligheid 2010* bestaan er in Nederland monoculturen voor pc-besturingssystemen, webbrowsers, pdf-readers en Adobe Flash.[35] Veel cyberbendes richten hun malware op de software die op dat moment marktleider is. Ze kunnen deze producten gewoon kopen, om daarna uitgebreid te testen welke kwetsbaarheden ze kunnen misbruiken. Malware voor deze software levert het meeste op, omdat in de beschikbare tijd (van de uitrol van de mailware tot de 'ontsmetting') de meeste systemen worden besmet. Deze strategie maximaliseert ook de kans dat gerichte malware kan worden hergebruikt. Het marktaandeel bepaalt dus welke software cyberbendes onderzoeken op kwetsbaarheden. In tabel 3 staat per categorie het dominante softwareproduct.

Op veel computers van Defensie en de thuiscomputers van defensiemedewerkers draait software van marktleiders, bijvoorbeeld Microsoft. Door de commercialisering en professionalisering van cybercrime kan iedere partij die een cyberaanval wil lanceren, daarvoor vrij eenvoudig de benodigde deskundigen, de kennis en de middelen inkopen. Defensie moet dus regelmatig haar informatiesystemen onderzoeken om inbraken tijdig te kunnen detecteren, om hacken zo moeilijk mogelijk te maken en om de impact van een geslaagde aanval te minimaliseren.

Erop vertrouwen dat beveiliging superieur is en alle besmettingen kan voorkomen, is niet meer realistisch. Organisaties moeten een plan maken voor wat hen te doen staat als hun systemen besmet raken. Zo'n *Incident Response Plan* vermindert de impact van een besmetting, maar alleen als dit plan regelmatig wordt getest op actualiteit en effectiviteit.

Het kiezen van software

Uit diverse onderzoeken blijkt dat het marktaandeel van een softwareproduct niet correleert met het aantal gesignaleerde kwetsbaarheden. Wel lijkt er een sterke relatie te bestaan tussen het marktaandeel en de hoeveelheid malware in omloop.[36] IBM stelt dat het veelgebruikte *Common Vulnerability Scoring System* blind is voor de economische motieven van hackers om software te kraken.[37] Dit klopt met het veelgehoorde argument dat de grote hoeveelheid malware voor bijvoorbeeld Windows, voornamelijk ligt aan het hoge marktaandeel en minder aan de vaak bekritiseerde kwaliteit van die software.

35 Het trendrapport 2010 is te vinden op www.govcert.nl.

36 Know Your Enemy: Malicious Web Servers', The Honeynet Project, 7 augustus 2007, www.honeynet.org.

37 IBM Global Technology Services, IBM Internet Security Systems: X-Force® 2008 Trend & Risk Report, January 2009, www-935.ibm.com.

FOTO AVDD, W. SALIS

Softwareproducten met een groot marktaandeel, zoals Microsoft, zijn aantrekkelijk voor cybercriminelen. Meer diversiteit in IT is daarom wenselijk. Op de foto: het 'Network Operations Centre' van IVENT

Kwaliteit

De kwaliteit van software wordt vaak aangeduid met het aantal fouten per duizend regels programmacode. De complexiteit en omvang van een computerprogramma bepalen het aantal fouten en daarmee de kansen voor malware. De kwaliteit van verschillende softwarepakketten objectief vergelijken is om verschillende redenen lastig. Zeker als de programmacode niet openbaar is, moeten moeizame voorzorgsmaatregelen worden getroffen om ervoor te zorgen dat niet-openbare programmacode geheim blijft.

Bedrijven die gesloten software verkopen willen meestal zelf de *reviewers* selecteren, eisen van hen geheimhouding en beïnvloeden de onderzoeksresultaten. Daarnaast zijn onderzoeksrapporten van gesloten software direct verouderd zodra er een nieuwe versie op de markt komt.

'Open source' software

Dat cybercriminelen de programmacodes van open software (de zogeheten 'open source software') kunnen naspeuren op kwetsbaarheden, beschouwt men over het algemeen niet als een hoger veiligheidsrisico. Dat komt omdat open source producten in alle openheid worden gebouwd en getest. In een interne studie van Microsoft staat dat open source softwareprojecten het niveau van commerciële software kunnen evenaren of zelfs overtreffen.[38] Openbare reviews maken objectief duidelijk of producten al dan niet veilig genoeg zijn. Zo is de AES encryptie, bekend van Winzip, destijds ontwikkeld als open technologie. Bovendien blijkt altijd achteraf dat vertrouwen op de geheime werking van een systeem (*security by obscurity*) onterecht is.[39]

Daarnaast wordt open source software vaak geroemd om de snelle reparatie van tekortkomingen. Deze snelheidswinst is mogelijk doordat de programmacode van alle versies openbaar is, en iedereen suggesties voor verandering direct in programmacode formaat kan aanleveren. Dit voordeel geldt overigens alleen voor open source producten met een actieve ontwikkelgroep.

Op basis van een ander onderzoek neemt men aan dat het aantal kwetsbaarheden voor open en gesloten source software per kilobyte programmacode ongeveer gelijk is.[40] Open source software is qua veiligheid dus geen panacee; ook hiervoor blijven updates nodig om fouten te verhelpen. Het is dus niet onmogelijk om malware te ontwikkelen voor bijvoorbeeld het Linux of MacOS besturingssysteem, maar met een marktaandeel dat veel kleiner is dan Windows zullen de inkomsten voor malware even-redig minder zijn.

Het is aannemelijk dat als het MacOS of Linux besturingssysteem marktaandeel wint, meer malware zal volgen. Massale migraties van een marktleidend softwareproduct naar een alternatief verhogen dus niet de veiligheid, volgens dit argument. De focus van malware zal dan namelijk verschuiven naar de nieuwe marktleider.

Diversiteit is wenselijk

Deze redenering verklaart weliswaar de onbeweeglijkheid van de huidige monocultuur,

38 'Halloween Document I (Version 1.17), Open Source Software: A (New?) Development Methodology', Raymond, E.S., www.catb.org.

39 Kerckhoffs' principle in 'Secrecy, Security, and Obscurity', www.schneier.com.

40 'Tale of Four Kernels', Spinellis, D. ACM, Germany, 2008, www.spinellis.gr.

maar is tegelijk geen goed argument tegen IT-diversiteit. Het is bijvoorbeeld onwaarschijnlijk dat marktaandelen in de softwaremarkt zullen omslaan, laat staan snel zullen wijzigen. Het aantal gebruikte applicaties op een platform, lopende investeringen, gesloten of 'semi-open' standaarden, onbekendheid van alternatieven, de benodigde nieuwe kennis voor behoudende gebruikers, gekleurde 'feiten' en de angst voor verandering remmen migraties naar andere software af. Het voordeel van migratie blijft dus sowieso langer bestaan dan deze redenering doet vermoeden.

Stelling 2 – Als organisaties standaardiseren op software introduceren ze een 'single point of failure' dat misbruikt kan worden door malware. De hoogte van dat risico hangt af van het marktaandeel van de gebruikte software.

Ondanks alle goede bedoelingen, zoals het actieplan 'Nederland Open in Verbinding' uit 2007, is Nederland sterk afhankelijk geworden van enkele dominante softwareleveranciers.[41] Open standaarden worden wel breed ondersteund, maar te weinig gebruikt. Van gebruikte software wordt zelden geverifieerd of deze open standaarden correct toepast, zonder deze standaard te 'verrijken' met gesloten technologie. In de praktijk vermindert de afhankelijkheid van dominante softwareleveranciers hierdoor nauwelijks.

Uniformering en diversificatie van software

In de landbouw is al eeuwenlang bekend dat een monocultuur ziektes en plagen aantrekt. Als een gewas in een monocultuur eenmaal is besmet, gaat een groot deel van de oogst verloren omdat de kans dat een besmetting wordt doorgegeven maximaal is. Erop gokken dat schaalvergroting goed blijft gaan, is zeer risicovol gebleken, zeker wanneer de belangen van de hele samenleving op het spel staan.[42] Daarom verbouwen boeren niet op alle percelen hetzelfde gewas en wisselen ze elke paar jaar per perceel van gewas.

Monocultuur

De huidige IT-monocultuur maakt dat het cyberrisico voor de Nederlandse samenleving maximaal is. De kans is namelijk maximaal dat Nederlandse systemen malware oppikken, omdat voor marktleidende software verreweg de meeste malware circuleert. De impact is eveneens maximaal, omdat een besmetting kan worden doorgegeven aan het merendeel van de systemen. Als een virus een groot aantal systemen kan besmetten, kunnen cascade effecten ontstaan. Omdat er binnen vitale sectoren veel computersystemen zijn die werken met marktleidende software, is dit voor Nederland een reëel risico. Reeds in 1999 zei congreslid Curt Weldon: *'It's not a matter of whether America will have an electronic Pearl Harbor... it's a matter of **when**'*.

FOTO ANP

In augustus 2012 besmette het Dorifel-virus zo'n drieduizend Windows-systemen bij dertig Nederlandse organisaties

In augustus 2012 besmette het Dorifel-virus zo'n drieduizend Windows-systemen bij dertig Nederlandse organisaties, waaronder veel gemeenten. Het bleek dat alle systemen al (veel) eerder ongemerkt besmet waren met het Citadel-virus, die het Dorifel-virus uitrolde. Als Dorifel niet zo opzichtig de inhoud van programma's en MS-Officebestanden had vercijferd, was de besmet-

41 Ministerie van EZ, 'Nederland Open in Verbinding: een actieplan voor het gebruik van Open Standaarden en Open Source Software in de (semi) publieke sector', november 2007, http://noiv.nl.

42 Zie de grote hongersnood van 1845 in Ierland: http://history1800s.about.com.

ting waarschijnlijk pas veel later opgemerkt.[43] Maar helaas leren ook cybercriminelen van hun fouten.

Een gangbare maatregel om de beschikbaarheid van systemen te verbeteren is het inrichten van back-up voorzieningen. Reservesystemen met dezelfde software zijn echter vatbaar voor dezelfde malware als het operationele systeem en zijn dus ineffectief bij een cyberaanval. Organisaties kunnen nog steeds standaardsoftware kiezen, maar een samenleving wordt kwetsbaar als alle organisaties dezelfde software (blijven) gebruiken. Om binnen Defensie en de vitale sectoren het cyberrisico te spreiden moeten organisaties onderling verschillende software gaan gebruiken (diversificatie).

Stelling 3 – De impact van malware vermindert door software te kiezen:
- met een klein marktaandeel,
- waarvoor fouten en kwetsbaarheden snel gerepareerd worden,
- waarvan de programmacode klein en hoogwaardig is,
- die open standaarden correct gebruikt.

Effecten van diversificatie

De effecten van diversificatie kunnen met een eenvoudig netwerkmodel globaal worden berekend.[44] Een organisatie die overstapt van het marktleidende product A naar een alternatief product B met een lager marktaandeel, zal daardoor minder geraakt worden door malware. Daarnaast remt diversiteit ook de verspreiding van malware af, aangezien de kans op een 'vruchtbaar contact' vermindert. Hierdoor verbetert de balans tussen besmetting en ontsmetting en kan malware (veel) minder systemen besmetten. Software diversiteit kan zo malware epidemieën voorkómen.[45]

Organisaties die migreren naar andere software maken éénmalig extra kosten voor opleidingen en conversie. Dat geldt ook als een organisatie bijvoorbeeld wil overstappen naar een volgende versie van Office-software. Hiermee is diversificatie een beveiligingsmaatregel als elke andere: een investering. Het Amerikaanse *Department of Defense* is daarom deels overgestapt op Applecomputers.[46] Ook het KNMI heeft voor een belangrijk systeem een back-up met een ander besturingssysteem, andere hard- en software en door een andere leverancier gebouwd.[47]

Voor Defensie is relevant dat potentiële aanvallers (veel) moeilijker twee verschillende systemen gelijktijdig uit kunnen schakelen. Tijdens de Koude Oorlog hadden de NAVO-landen een nucleaire *Second Strike Capability*, maar die risicospreiding vergde een strategische voorbereiding en een daarvoor toereikend budget. Met een risicoanalyse kan Defensie vaststellen waar het cyberrisico op deze manier moet worden gespreid.

Niet alle organisaties dezelfde standaardsoftware

Meer standaardiseren op marktleidende software is vergelijkbaar met bezuinigen op branddeuren in gebouwen – terwijl bekend is dat de wijk steeds meer pyromanen aantrekt. Meer diversiteit in standaardsoftware verbetert de veiligheid, omdat het risico van malware wordt gespreid over verschillende producten en de besmettelijkheid van malware wordt verminderd.

Nederland kan de impact van cyberincidenten verminderen als organisaties niet allemaal dezelfde standaardsoftware gebruiken. De impact vermindert het meest als de markt evenwichtig verdeeld is. Als bijvoorbeeld twee producten elk vijftig procent marktaandeel hebben, neemt de *return-on-investment* voor malware met vijftig procent af omdat een malware-programma maar maximaal de helft van de systemen kan

43 'XDocCrypt/Dorifel – Document encrypting and network spreading virus', Fox-IT, 9 augustus 2012, http://blog.fox-it.com.
44 'Math on Malware', *ISACA Journal* (3) 2011, www.isaca.org.
45 'Security through Network-wide Diversity Assignment', O'Donnell, A.D., september 2005, http://idea.library.drexel.edu/bitstream.
46 'Apples For The Army', Greenberg, A., Forbes.com, 21 december 2007, www.forbes.com.
47 Zie: www.knmi.nl.

besmetten. Ook hergebruik van gerichte malware wordt moeilijker als de softwaremarkt meer verdeeld is. Het dwingt cybercriminelen om meer nieuwe malware te ontwikkelen, die per stuk ook nog eens minder opleveren. Diversificatie raakt de internetmaffia dus waar het zeer doet: het reduceert de inkomsten van malware.

Voor softwareleveranciers zal meer diversiteit in de markt naar verwachting het aantal openstaande *Zero-day exploits* per product verminderen en daarmee meer tijd opleveren om kwetsbaarheden in software te repareren. Dit geldt ook voor meer softwarebedrijven in de markt, aangezien die bedrijven de neiging hebben hun kostbare programmacode zoveel mogelijk opnieuw te gebruiken in verschillende producten. Dit versterkt het veiligheidseffect, omdat de periode waarin kwetsbaarheden kunnen worden misbruikt korter wordt. Vanuit het oogpunt van veiligheid is diversificatie dus een maatregel die een voordeel oplevert dat op andere manieren moeilijk te behalen is.

Als de software een klein marktaandeel heeft en kwetsbaarheden snel worden gerepareerd, kan de daarop gerichte malware minder computers infecteren. Als een softwarepakket bovendien een compacte programmacode heeft met een hoge kwaliteit, wordt het voor cybercriminelen moeilijker en dus duurder om malware te maken voor deze software. Dit verlaagt de *Business Case* voor dergelijke malware.

Naar een veiliger cyberdomein

Organisaties die back-upsystemen uitrusten met andere software dan productiesystemen verminderen daarmee het cyberrisico, maar verhogen tegelijkertijd hun beheerskosten. Migreren naar een alternatief besturingssysteem is daarom alleen te overwegen bij vitale systemen. Organisaties kunnen makkelijker overstappen op alternatieve standaardsoftware voor websurfen, Office en e-mail. Dergelijke migraties zijn voor gebruikers relatief laagdrempelig: de meeste softwareproducten bieden dezelfde functionaliteit, alleen de bediening verschilt (zoals een computer met Windows, een Apple-iPad en een Android-tablet onderling verschillen).

Als de hele organisatie op alternatieve standaardsoftware overstapt, roept dat in eerste instantie weerstand op, bijvoorbeeld omdat gebruikers en beheerders nieuwe kennis moeten opbouwen. Migreren naar andere standaardsoftware kan daarom het beste samenvallen met het uitfaseren van oude softwareproducten. Het nadenken over een exit-strategie maakt echter zelden deel uit van het aanschaftraject voor nieuwe software. Veel organisaties onderschatten de impact van softwaremigraties. Als een organisatie niet kan loskomen van het oude standaardproduct, krijgt het nieuwe product vaak de schuld. Alleen met een goede voorbereiding en het gebruik van open standaarden, kunnen organisaties de afhankelijkheid van leveranciers verminderen.

De gemiddelde computergebruiker gebruikt thuis graag dezelfde software als op kantoor. Organisaties die het thuisgebruik van nieuwe standaardproducten mogelijk maken, verhogen daarmee het draagvlak voor de verandering. Bovendien elimineert dit het risico dat thuiswerkers illegale software gebruiken, die vaak geïnfecteerd is met malware.

Het is voor organisaties dus financieel aantrekkelijk om te standaardiseren op gratis software

Maatregelen als diversificatie van software moeten worden gecoördineerd boven het niveau van individuele organisaties. De *European Network and Information Security Agency* (ENISA) bepleit het internationaal oppakken van meerdere lange-termijnmaatregelen tegen cybercrime (zie tabel 4).

Om een goede variatie in softwareproducten te bereiken is het noodzakelijk dat internationaal

Acties en maatregelen	Effect
• Harmonisatie van wetten om de samenwerking te verbeteren bij de opsporing en aanhouding van cybercriminelen; isoleren van besmette computers en uitschakelen van malafide servers • Filtering, blokkering en infiltratie van besmette computers • Gestructureerd aanpakken waardeketen van cybercrime • Coördinatie van research om IT kwaliteit, veiligheidskennis en bewustwording te verbeteren	Betere preventie van infecties met malware
• Verbeteren detectie, identificatie en analyse van malware • Ondersteun eigenaren van besmette computers bij de ontsmetting • Harmonisatie van wetten voor het neutraliseren van besmette computers • Coördinatie van acties op malware ontwikkelingen • Coördinatie van research voor een betere beveiliging	Betere ontsmetting van besmette computers

Tabel 4. Internationale coördinatie van cybersecurity

het marktaandeel van softwareproducten en de hoeveelheid malware per softwareproduct objectief worden bewaakt en gepubliceerd. Momenteel is het marktaandeel en de hoeveelheid malware per softwareproduct moeilijk vast te stellen. Dat komt omdat voor veel onderzoeksrapporten geld wordt gevraagd, de schattingen van marktaandelen sterk uit elkaar kunnen lopen en informatie gekleurd kan zijn.[48] Voor alle relevante bronnen is informatie over de onderzoekscontext nodig om de statistieken goed te kunnen interpreteren.

Bij gelijke geschiktheid is het wenselijk een standaardproduct te kiezen dat correct werkt met open standaarden, zodat gegevensuitwisseling met andere software beter gegarandeerd is en afhankelijkheid van leveranciers wordt verminderd. Uitgesloten moet worden dat softwareproducten open standaarden 'verrijken' met gesloten technologie. Hierdoor is migratie naar andere producten in de toekomst ook beter mogelijk.

Vanwege de huidige IT-monocultuur is het cyberrisico voor de Nederlandse samenleving maximaal. Het Amerikaanse ministerie van Defensie is daarom deels overgestapt op Apple-computers

48 Zie bijvoorbeeld de schattingen van de marktaandelen van Adobe Reader en MS Exchange vs. Lotus Notes.

Conclusies en aanbevelingen

Door IT breed toe te passen en systemen online te koppelen zijn bedrijfsprocessen veel efficiënter geworden. Om de concurrentie in the *global village* in de toekomst aan te kunnen, zal Nederland steeds meer processen digitaal moeten

koppelen. Daardoor zal de afhankelijkheid van ICT-systemen nog meer toenemen. Om informatie te kunnen delen is overigens alleen het gebruik van dezelfde interfacestandaard nodig, het gebruik van dezelfde software is niet vereist. Het internet met zijn open standaarden is daar zelf het beste voorbeeld van.

De netwerksamenleving is echter een tweesnijdend zwaard. Door de uniformering van software, meer online toepassingen, de autonome groei van het internet en de gevolgen van de financiële crisis stijgt het risico op malwarebesmettingen. Reguliere beveiligingsmaatregelen zoals firewalls en antivirussoftware zijn steeds slechter opgewassen tegen infecties met malware. Zelfs een optimale beveiliging kan besmettingen met malware niet uitsluiten, zodat elke organisatie een Incident Response Plan moet hebben voorbereid.

Om het risico op aanvallen met cyber te verminderen, kunnen organisaties procedures en beveiligingsregels aanscherpen en medewerkers gratis de zakelijke software verstrekken voor thuisgebruik, inclusief beveiligingssoftware. Organisaties die hiervoor geen licentiekosten willen maken, standaardiseren op gratis software. Ook het verminderen van besmette privécomputers door het bevorderen van veiligheidsbewustzijn levert de samenleving als geheel voordeel op.

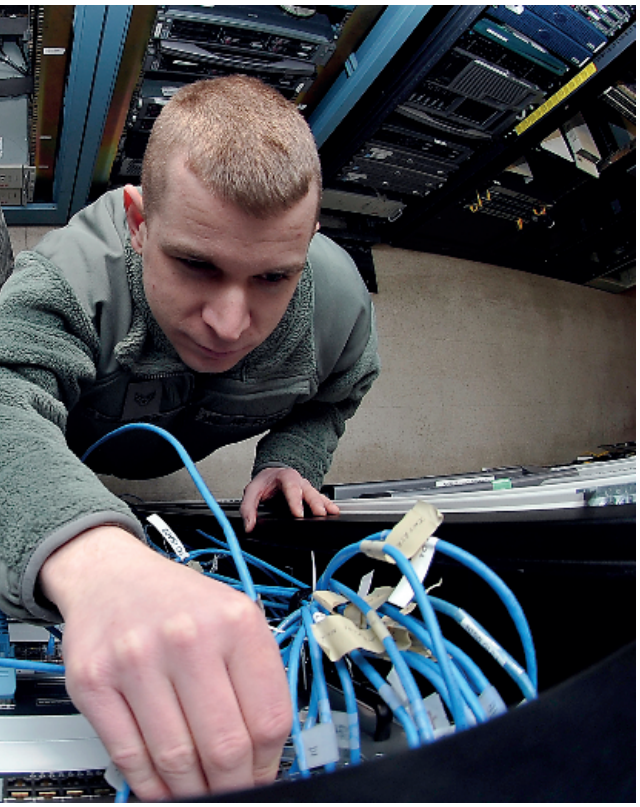

FOTO US DEPARTMENT OF DEFENSE

Open software en IT-diversiteit bevorderen

Elke organisatie kan zelfstandig standaardsoftware kiezen, maar een samenleving wordt kwetsbaar als de meerderheid van de systemen dezelfde software gebruikt. Verschillende onderzoeken hebben al gewaarschuwd tegen de risico's van een (te) uniform IT-landschap, maar de afgelopen jaren waren de veranderingen van de marktaandelen in de softwaremarkt gering.[49]

In tegenstelling tot de *Convention on Biological Diversity*, is het nog ongewoon het gebruik van open standaarden en ICT diversiteit met beleid af te dwingen.[50] Hoewel iedereen het logisch vindt dat de hardware van vitale systemen dubbel is uitgevoerd, worden back-upsystemen meestal voorzien van dezelfde software. Vasthouden aan marktleidende software die het meest aantrekkelijk is voor cybercriminelen betekent echter (impliciet) instemmen met een hoger risico op cyberaanvallen.

Goede voorbereiding

Aan de andere kant wordt het onacceptabel geacht als een cyberaanval nucleaire systemen, havens, het betalingsverkeer, telecommunicatiesystemen, de drinkwatervoorziening, ziekenhuizen, de energievoorziening of Defensie grootschalig lam legt. Tijdens een cyberaanval kan niet onmiddellijk een vervangend systeem met andere software uit de grond worden gestampt. Om te vermijden dat een cyberaanval een domino-effect van vitale voorzieningen veroorzaakt is een strategische voorbereiding vereist.

49 ENISA, 'Security Economics and The Internal Market' (hoofdstuk 7), www.enisa.europa.eu. Zie ook: 'Perspective: Massachusetts Assaults Monoculture', Greer, D., CNET News, http://news.cnet.com.

50 'Convention on Biological Diversity', www.cbd.int.

Defensie loopt in vredestijd het risico dat met een cyberaanval logistieke en financiële informatiesystemen worden gesaboteerd. In conflictsituaties kunnen gehackte operationele militaire systemen mensenlevens kosten.

De kennis en betrokkenheid van Defensie is nodig om cyberaanvallen op Nederlandse vitale belangen zo moeilijk mogelijk te maken en capaciteit op te bouwen om aanvallen snel te kunnen pareren. Defensie kan daarmee de invulling van haar hoofdtaken en de communicatie daarover verbeteren, zodat realistische verwachtingen ontstaan over wat wel en niet binnen de verantwoordelijkheid van Defensie valt.

Internationale coördinatie

Betere maatregelen, meer deskundigen en internationale coördinatie zijn nodig om het cyberdomein veiliger te maken. Het is belangrijk om het gebruik van open standaarden te bevorderen, om 'single points of failure' door dezelfde software te vermijden. Daarnaast moeten landen hun wetten internationaal harmoniseren, om de waardeketen van cybercriminelen multinationaal aan te kunnen pakken.

Meer research kan de veiligheid van systemen verhogen en de bestrijding van malware verbeteren. Omdat malware steeds meer schade veroorzaakt aan de samenleving moeten alle effectieve tegenmaatregelen worden ingezet. ■

FOTO US DEPARTMENT OF DEFENSE

Een Amerikaanse luchtmacht-generaal houdt een pleidooi voor meer samenwerking en betere internationale coördinatie tijdens een cyberconferentie in Stuttgart