AANPAK CYBERCRIMINALITEIT: VERDEEL EN HEERS

De heer Henk-Jan van der Molen, Sr. projectleider / ICT adviseur Inspectie Verkeer en Waterstaat

Henk-Jan van der Molen heeft in 1984 zijn KMA-opleiding afgerond, waarna hij tot 1998 zowel operationele als ICT-functies vervulde bij de KL. Na een uitstapje van ruim drie jaar naar het bedrijfsleven is hij sinds 2002 terug bij de overheid. Bij de Inspectie Verkeer en Waterstaat bestaat zijn werk uit projectleiding, ICT-beleid, informatiebeveiliging en privacybescherming. Vanuit zijn praktijkervaringen heeft hij diverse artikelen gepubliceerd, waaronder twee in Intercom over frequentiemanagement.

Misbruik van bankrekeningen en het verlies van (bedrijfs)informatie door malware-incidenten zijn aan de orde van de dag. Hier aan ten grondslag ligt de groeiende criminele bedrijfstak rondom malware, waar miljoenen in omgaan. Toch zie je dat veel organisaties allemaal dezelfde standaardproducten blijven gebruiken, terwijl dit de *return on investment* van malware maximaliseert. Dit artikel schetst de effecten van het veranderen van standaardsoftware.

Malware wordt hier gedefinieerd als programmatuur met kwaadaardige functionaliteit, zoals virussen, bots, wormen, Trojaanse paarden en spyware. Een cybercrimineel kan een systeem vanaf het internet met malware infecteren door kwetsbaarheden in software te misbruiken. Ook kan een gebruiker onbewust malware activeren door een besmette website of een besmet programma te openen. Zelfs een bestand met macro's, beeld, geluid of video kan malware bevatten. Malware valt steeds vaker de webbrowser aan, het aantal *'drive-by-infection'* sites groeit explosief. Het bezoek aan één geïnfecteerde website kan al voldoende zijn om een systeem te compromitteren.

Volgens het SANS Internet Storm Center kunnen cybercriminelen steeds sneller malware ontwikkelen doordat ze over meer kennis beschikken en onderling samenwerken. Voor het schrijven van de succesvolle Sobig worm werd bijvoorbeeld universitaire kennis ingezet, is de broncode van verschillende virussen hergebruikt en zijn er testversies uitgebracht.

Bijna alle software bevat fouten of kwetsbaarheden die een kraak mogelijk maken. Om fouten in uitgebrachte software te verhelpen verspreiden leveranciers zogenaamde patches via het internet. Het vermoeden bestaat dat cybercriminelen stelselmatig patches analyseren om daaruit nieuwe malware te ontwikkelen. Hierdoor loopt iedereen die te langzaam patcht, het risico dat zijn kwetsbare systemen worden gekraakt. Op de zwarte markt wordt malware per exploit verkocht, ook voor de nieuwste systemen. Botnets van pc's die via malware zijn overgenomen worden per uur verhuurd, bijvoorbeeld om een webwinkel plat te leggen en zo geld af te persen. De omvang van het 'Storm worm' botnet wordt geschat op anderhalf miljoen zombie computers; dit botnet zou momenteel 20% van alle wereldwijde spam versturen. Het recent ontdekte Conficker virus kan de miljoenen besmette pc's flexibel inzetten door de eigen broncode te vernieuwen. Cybercriminelen kunnen gekraakte systemen tevens misbruiken voor bedrijfsspionage of frauderen met opgeslagen creditcardgegevens. Daarnaast veroorzaakt malware voor organisaties indirecte schade door programmatuur of data te verminken en de continuïteit van bedrijfsprocessen te verstoren. Uit de ICT-barometer 2009 van Ernst & Young blijkt dat bedrijven veel last hebben van cybercrime.

Het beeld dat malware over het algemeen op privé pc-gebruikers is gericht is niet altijd terecht, ook bedrijven worden er door geschaad. Om negatieve publiciteit te vermijden doen veel organisaties geen aangifte van een malwarebesmetting. Soms merkt een organisatie ook niets van een malwarebesmetting, bijvoorbeeld als malware wordt ingezet voor bedrijfsspionage. Wel zijn zakelijke systemen vaak beter beveiligd, bijvoorbeeld doordat medewerkers zelf geen software kunnen installeren. Ook overheden zijn betrokken bij cybercriminaliteit, zoals de Russische cyberoorlog tegen Estland in 2007. In april 2009 meldde de AIVD dat China en Rusland op grote schaal digitaal spioneren. Security.nl berichtte bovendien in mei 2009 dat China een veilig besturingssysteem (Kylin) en een veilige processor heeft ontwikkeld voor een cyberoorlog.

MAATREGELEN BIEDEN GEEN GARANTIES

Zelfs een ICT-infrastructuur met de meest veilige instellingen is niet immuun voor alle malware aanvallen. Om incidenten te voorkómen blijken de maatregelen die organisaties nemen tegen malware steeds minder effectief. 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 exploits als het operationele systeem. Back-up voorzieningen zijn dus ineffectief bij een malware aanval, omdat zogenaamde *Zero Day* exploits (hiertegen bestaat nog geen beveiliging) regelmatig voorkomen. Ook de veiligheid van extra maatregelen zoals *two factor* authenticatie (het gebruik van een token bij internetbankieren of telewerken) staat met de nieuwste browser plugin malware onder druk.

Jaarlijks overlijdt slechts 0,01% van de Nederlandse bevolking aan de gevolgen van griep. Daarentegen heeft de mens geen resistentie tegen een H5Nx virus, zoals vogelgriep. Het immuunsysteem herkent zo'n virus niet direct, waardoor het virus zich ongebreideld kan vermenigvuldigen. Het lichaam keert zich pas tegen de besmetting als de besmette persoon, vaak letterlijk, doodziek is. (Wikipedia)

Bij veel organisaties kan een malwarebesmetting bedrijfsprocessen verstoren, omdat systemen vaker gekoppeld worden via het internet (Web 2.0), zoals bij banken, verkoopsites en nutsbedrijven met sensoren en actuatoren aan het internet. Ook de overheid loopt meer risico: in 2007 is al minstens 65% van de dienstverlening via het internet verlopen. Het aantal gekoppelde systemen zal verder toenemen met de invoering van basisregistraties, zoals het GBA (Gemeentelijke Basis Administratie voorheen bevolkingsregister). Door toenemende centrali-

satie en uniformering zullen ICT-infrastructuren steeds meer op elkaar gaan lijken en neemt de afhankelijkheid van ICT toe.

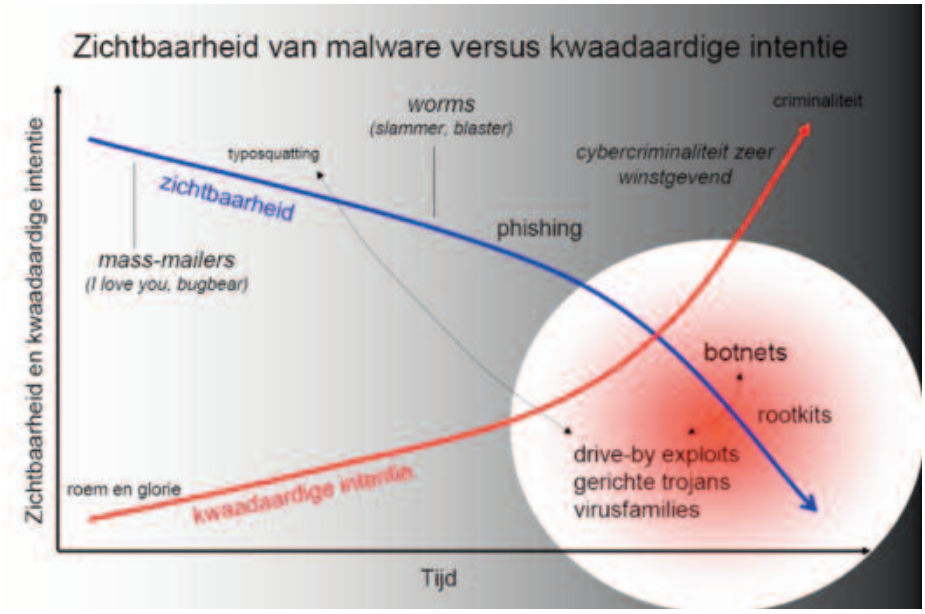
MALWARE GOES WHERE THE MONEY IS

Cyberbendes willen zoveel mogelijk geld 'verdienen'. Daarvoor moet de verspreiding van malware 24/7 door kunnen gaan en moet een malwarebesmetting zo lang mogelijk verborgen blijven. Deze bendes gebruiken bijvoorbeeld encryptie, stealth rootkits en verspreiden malware op roulerende webservers, zodat het uitschakelen van enkele servers geen effect heeft. Door voor elke besmetting unieke malware te genereren en selectief te richten op enkele bedrijven, verschijnt deze malware niet meer op de radar van de leveranciers van virusscanners. Volgens security.nl laten virusscanners 60% van alle nieuwe malware door. Er circuleert bovendien malware die niet gedetecteerd kan worden, omdat die sneller updates ophaalt van het internet dan dat virusscanners worden bijgewerkt. Antivirus softwareleverancier Kaspersky meldde hierover al in 2007: "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".
Bedrijven die aangifte doen van computercriminaliteit ervaren vaak dat de verantwoordelijke criminelen niet kunnen worden veroordeeld, omdat cyberbendes meestal vanuit het buitenland opereren en er alles aan doen om de dans te ontspringen. Door de lage pakkans en hoge inkomsten neemt cybercriminaliteit een enorme vlucht. Het bedrijf F-secure gaf onlangs aan dat waar de malwaregroei in 2007 is verdubbeld, deze in 2008 is verdrievoudigd.

Cybercriminelen moeten blijven investeren in de ontwikkeling van malware, omdat ze continue strijden tegen patches en anti-malware software. Omdat cybercriminelen die kosten terug willen verdienen, is hun inkomstenmodel samen te vatten met de volgende stelling:

> Stelling 1: Professionele cybercriminelen maximaliseren de 'omzet' van hun malware (= P x Q) door te focussen op (P)

Hierbij staat P voor het aantal computers dat per malware aanval wordt besmet en Q voor de gemiddelde opbrengst per besmette computer. Het focussen op Q vergt specifieke voorkennis en biedt minder zekerheid. Het kraken van één vitaal systeem kan veel geld opleveren, maar dergelijke systemen zijn vaak goed beveiligd.
Het focussen op P biedt meer zekerheid en dus ook inkomsten omdat veel computers onvoldoende zijn beveiligd en het is eenvoudiger, omdat alleen informatie nodig is over de verhoudingen in de softwaremarkt. Het is een bijkomend voordeel dat als duizenden gedupeerden aangifte doen van een kleine diefstal, vervolging voor justitie moeilijker is dan wanneer één partij aangifte doet van een groot misdrijf.



Malware Kwaadaardigheid

Veel cyberbendes maximaliseren daarom hun *return-on-investment* door hun exploits te richten op software die op dat moment marktleider is. Ze kunnen deze producten gewoon kopen, om daarna uitgebreid te onderzoeken welke kwetsbaarheden misbruikt kunnen worden. Malware voor deze software levert het meeste op, omdat in de beschikbare tijd (van uitgebrachte exploit tot geïnstalleerde patch) de meeste systemen worden besmet. Deze strategie maximaliseert ook de kans dat een gerichte exploit kan worden hergebruikt. Het marktaandeel van softwareproducten bepaalt dus welke producten cyberbendes onderzoeken op kwetsbaarheden. Hieronder staat per categorie het dominante softwareproduct.

Categorie	Softwareproduct	Markt % (schatting)	Populariteit bij criminelen
Office suite	MS Office	95%	++
Besturingssysteem	MS Windows	90%	++
Webclient	MS IE	79%	++
Mailserver	MS Exchange	78%	+
Mailclient	MS Outlook (Express)	62%	+
Webserver	Apache	53%	+
Database server	Oracle	44%	+

Het najagen van marktleiders lijkt op de Varkenscyclus, het economische verschijnsel dat aanbieders massaal reageren op de hoogte van de vraagprijzen. Tegen de tijd dat deze reactie doorwerkt op het aanbod, is de prijs alweer omgeslagen. Het resultaat is dat vraag en aanbod golfbewegingen zijn, waarbij het aanbod na-ijlt op de vraag.
Het vraag-en-aanbod mechanisme is ook toepasbaar op de malware situatie. De 'vraag' bestaat uit het marktaandeel van de software waarop de malware zich kan richten. De exploits voor die software vormen dan het aanbod.

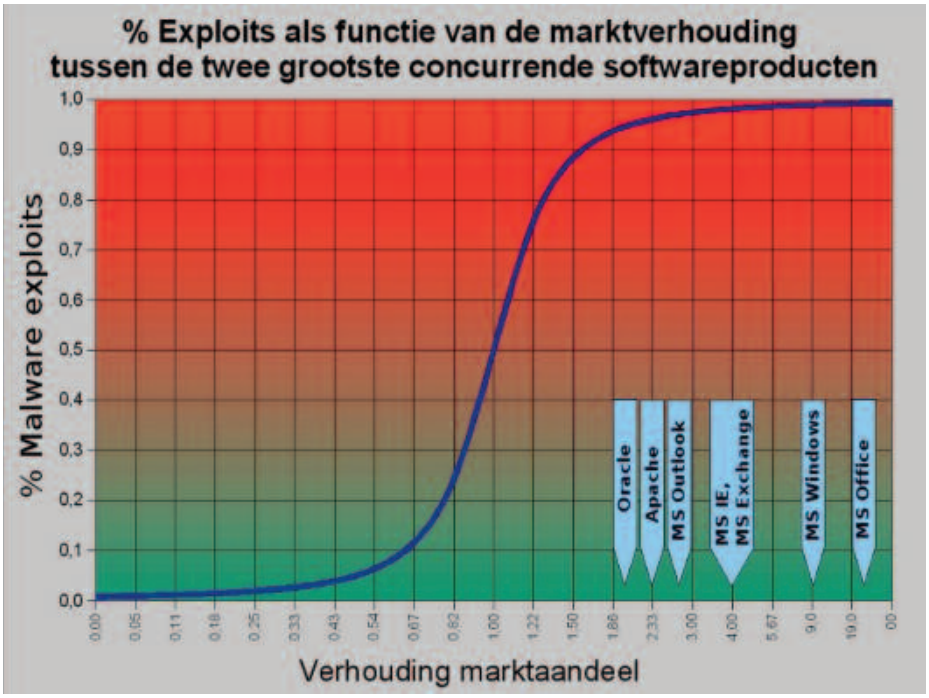
> *De landbouw kweekt tegenwoordig vanuit efficiency relatief weinig gewassoorten in grote monoculturen. Moderne gewassen met steeds meer uniforme karakteristieken vervangen traditionele gewassen in de hele wereld en vormen daarmee een bedreiging, omdat de genetische basis smaller wordt. De gekweekte gewassen worden steeds kwetsbaarder voor ziekten en plagen. (World Resources Institute, 2001*

MARKTAANDEEL EXPLOITS

De softwaremarkt kent echter weinig golfbewegingen – omdat enkele producten de markt domineren, vormt het pc-landschap een monocultuur.
Als systemen met de zelfde software werken, zijn ze gevoelig voor de zelfde malware. De meest succesvolle softwareproducten trekken daarbij onevenredig veel exploits aan. Een geschikt model om vanuit het marktaandeel van software het aandeel van de exploits te schatten dat voldoet aan dit economische principe, is de S-kromme. De figuur geeft deze functie vereenvoudigd weer.

Uit diverse lijsten met beveiligingsadviezen 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 het aantal verspreide exploits. Dit klopt met het veel gehoorde argument dat het grote aantal exploits, van bijvoorbeeld MS Windows, aan het marktaandeel van 90% ligt en niet zozeer aan de kwaliteit van de software.



Malware Marktaandeel

De kwaliteit van software wordt vaak aangeduid met het aantal fouten per 1000 regels code. De complexiteit en omvang van een computerprogramma bepalen het aantal fouten en daarmee de kansen voor malware. Een objectieve kwaliteitsvergelijking tussen de open en gesloten broncode van besturingssystemen is lastig. Je moet dan aannemen dat het aantal kwetsbaarheden per kilobyte broncode ongeveer gelijk is. Open source is qua veiligheid geen silver bullit, ook hiervoor blijven patches nodig om fouten te verhelpen. Het is dus niet onmogelijk om malware te ontwikkelen voor Linux of MacOS, maar met een marktaandeel dat 20 keer lager ligt, zullen de inkomsten per exploit evenredig minder zijn.
Je kunt dan redeneren dat als MacOS of Linux marktaandeel wint, meer exploits zullen volgen. Migreren van een marktleidend softwareproduct naar een alternatief verhoogt dus niet de veiligheid, volgens dit argument.

Deze redenering verklaart weliswaar de onbeweeglijkheid van de huidige monocultuur, maar toch is dit geen goed argument tegen softwarediversiteit. Het is bijvoorbeeld onwaarschijnlijk dat de marktaandelen in de softwaremarkt zullen omslaan, laat staan snel wijzigen. Het aantal gebruikte applicaties op een platform, lopende investeringen, gesloten standaarden, onbekendheid van alternatieven, de benodigde nieuwe softwarekennis, behoudende gebruikers, gekleurde informatie en de angst voor verandering remmen vaak een migratie. Het veiligheidsvoordeel van zo'n productverandering blijft dus sowieso langer bestaan dan algemeen wordt aangenomen.

De druifluis is zeer schadelijke voor druivenplanten. In de negentiende eeuw vernietigde deze bladluizensoort veel Europese wijngaarden, in Frankrijk wel zo'n 70% van alle planten. Het bestrijden van de druifluis was vrijwel onmogelijk. Men ontdekte dat de wijnrankfamilies in Noord-Amerika wel resistent waren tegen de druifluis. De oplossing was deze wortelstokken te importeren en Europese varianten hierop te enten. (Wikipedia)

EFFECTEN VAN DIVERSIFICATIE

Om de effecten van diversificatie ruwweg te schatten, stellen we vooraf dat het onwaarschijnlijk is dat productmigraties het aantal uitgebrachte exploits zal vergroten. Het lijkt namelijk onlogisch dat cyberbendes meer activiteiten gaan ondernemen, zonder dat daar een goed rendement tegenover staat. Er zal eerder sprake zijn van een varkenscyclusachtige verschuiving van de focus.

Een organisatie die overstapt van het marktleidende product A naar een alternatief product B, zal minder geraakt worden door exploits - zoals het lagere marktaandeel van B dicteert. Stel het extreme geval dat alle migraties van A naar B ervoor zorgen dat de markt uiteindelijk 50/50 verdeeld wordt tussen beide producten. De S-kromme geeft dan aan dat 50% van de exploits zich zal richten op product A en 50% op product B. Zelfs in deze situatie vermindert op die manier het aantal exploits per organisatie dus met de helft. Vanuit deze optiek kunnen organisaties dus beter niet-marktleidende software als standaardproduct kiezen.

Het is bekend dat de aanschafprijs van hard- en software ongeveer 20% van de Total Cost of Ownership omvat. Omdat de ondersteuning en het beheer van de infrastructuur de resterende 80% vormen, zal een lagere impact van exploits dus sterk doorwerken in de ICT beheerkosten. Daar staat tegenover dat een organisatie die migreert naar andere software éénmalig extra kosten heeft voor opleidingen en conversie. Maar dat geldt meestal ook voor een productupgrade. Hiermee is diversificatie een beveiligingsmaatregel als elke andere: een investering. Het Amerikaanse *Department of Defense* (DoD) heeft dit goed begrepen en zij diversifiëren door deels over te stappen op Apple computers.

WEL STANDAARDISEREN, NIET ALLEMAAL DEZELFDE STANDAARD

Diversificatie van standaardsoftware voor kantoorautomatisering functioneert macroscopisch als compartimentering tegen exploits. Wanneer de softwaremarkt beter verdeeld is tussen verschillende producten, spreidt dat het risico van malware. Men kan verwachten dat de B.V. Nederland veiliger wordt als organisaties niet allemaal dezelfde standaardsoftware kiezen. Deze vermindering van de impact van malware is het grootst als de markt gelijk verdeeld is. Als de markt bijvoorbeeld 50/50 tussen twee producten verdeeld is, neemt de *return-on-investment* per exploit met 50% af, omdat een exploit maar maximaal de helft van de systemen kan besmetten. Ook hergebruik van gerichte exploits wordt moeilijker als de softwaremarkt meer verdeeld is. Het dwingt cybercriminelen meer nieuwe malware exploits te ontwikkelen, die per stuk ook nog eens minder opleveren.
Voor softwareleveranciers zal meer diversiteit in de markt naar verwachting resulteren in minder openstaande *Zero Day* exploits per product en daarmee minder achterstand bij het ontwikkelen van patches. Dit versterkt het veiligheidseffect verder, omdat de periode korter wordt waarin kwetsbaarheden kunnen worden misbruikt.
Diversificatie van standaarden raakt de internetmaffia waar het zeer doet: de reductie van malware inkomsten. Vanuit het oogpunt van veiligheid is diversificatie dus een maatregel die voordeel oplevert die op een andere manier moeilijk te behalen is. In stelling 2 is samengevat met welke software het risico van malware vermindert.

Stelling 2: De impact van malware vermindert door software te kiezen:
- met een klein marktaandeel;
- waarvoor snel patches beschikbaar komen;
- waarvan de broncode klein en kwalitatief hoogwaardig is.

Door een klein marktaandeel en een snelle patchcyclus zijn er minder besmette computers, waardoor de malware omzet (P x Q) klein is. Als de broncode klein en hoogwaardig is, zal het ontwikkelen van een exploit voor die software meer moeite en dus meer geld kosten.

AANBEVELINGEN VOOR DIVERSIFICATIE

Om een goede variatie in softwareproducten te bereiken, is het noodzakelijk dat wereldwijd de marktaandelen van softwareproducten en het aantal uitgebrachte exploits per softwareprodukt objectief worden bewaakt en gepubliceerd. Momenteel is dat lastig te bepalen. Bij gelijke geschiktheid is het wenselijk een standaardproduct te kiezen dat werkt met open standaarden, zodat gegevensuitwisseling met andere software gegarandeerd is en *vendor lock-in* wordt voorkomen. Hierdoor is migratie naar andere producten in de toekomst ook beter mogelijk. Het actieplan 'Nederland Open in Verbinding' – in de volksmond 'Plan Heemskerk' – is een positieve eerste stap om daarvoor de juiste voorwaarden te scheppen.

Softwarediversiteit binnen één organisatie conform de Amerikaanse DoD-visie vermindert de kwetsbaarheid van een organisatie wel, maar verhoogt de beheerskosten. Als de hele organisatie op alternatieve standaardsoftware overstapt, heeft dat in eerste instantie een grote impact maar op de lange termijn is dat minder kostenintensief.

Overstappen op een alternatief besturingssysteem is erg ingrijpend en alleen te overwegen bij vitale systemen. Een organisatie kan makkelijker overstappen op alternatieve software voor websurfen, kantoortoepassingen en e-mail. Dergelijke migraties zijn relatief laagdrempelig: de meeste softwareproducten bieden dezelfde functionaliteit, alleen de bediening kan verschillen.

Migratie naar een ander standaardproduct wekt vaak weerstand op, bijvoorbeeld omdat gebruikers en beheerders nieuwe kennis moeten opbouwen. Dat betekent dat migreren naar andere standaardsoftware het beste kan worden doorgevoerd bij het uitfaseren van oude softwareproducten. De gemiddelde pc-gebruiker heeft thuis vaak dezelfde software als op kantoor. Een organisatie die het thuisgebruik van nieuwe standaardproducten faciliteert, verhoogt daarmee de acceptatie van de productverandering. Bovendien elimineert dit het risico dat thuiswerkers softwarepakketten gebruiken uit het illegale circuit, die vaak geïnfecteerd zijn met malware. Het is dan financieel aantrekkelijk om te standaardiseren op *open source software*.
De marktverhoudingen zijn al jaren min of meer constant, dus weinig bedrijven veranderen van standaardsoftware. In tegenstelling tot de *'Convention on Biological Diversity'* is het nog ongewoon ICT-diversiteit als beleid tegen digitale verlamming te ontwikkelen. Vasthouden aan standaardproducten die zich bevinden in het vizier van de meeste cybercriminelen, betekent echter impliciet instemmen met een hoger veiligheidsrisico. Tegelijkertijd wordt het onacceptabel geacht als een cyberaanval vitale overheidssystemen, het betalingsverkeer, telecommunicatiesystemen of de energievoorziening grootschalig lamlegt. De *North American Electric Reliability Corporation* (NERC) heeft gemeld dat – na de massale uitval van elektriciteitscentrales in 2003 – maatregelen tegen cybercrime nog op de agenda staan. Zolang computersystemen kwetsbaar blijven voor malware, kan een betere spreiding van standaardsoftware een onverwacht uitvallen van vitale voorzieningen voorkomen en cybercriminaliteit verminderen.

Met dank aan Douwe Leguit en Erik de Jong (teammanager, resp. adviseur bij GOVCERT.NL, het Computer Emergency Response Team van de Nederlandse Overheid).

BRONNEN:

1. http://spamkings.oreilly.com/WhoWroteSobig.pdf
2. Govcert Trendrapport 2007
3. 'Incident Management broodnodig', Computable 26 mei 2006
4. 'The Zero-Day Dilemma', www.eweek.com/article2/0,1759,2087034,00.asp
5. 'Malicious Web Servers' (The Honeynet Project, 7 augustus 2007)
6. 'Apples for the Army', www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx_ag_1221army.html
7. 'Nederland Open in Verbinding', MinEZ http://www.minez.nl/content.jsp?objectid=153180

VERENIGING OFFICIEREN VERBINDINGSDIENST

BD-EVENT 5 NOVEMBER SOESTERBERG

Ook in 2009, wordt voor de b.d. leden van de VOV – voorafgaand aan het Regimentsdiner op donderdag 5 november – een eigen event georganiseerd. Dit jaar wordt de inleiding verzorgd door lkol b.d. Gerrit Jan Huijsman. Het onderwerp zal zijn: Het ontstaan van ZODIAC.

De inleiding zal worden afgesloten met een hapje en een drankje.

Tijdschema:
16.00 uur ontvangst
16.30 uur aanvang lezing
17.45 uur einde en gelegenheid tot omkleden voor het Regimentsdiner

Lokatie: Het officierscasino te Soesterberg.

Point of Contact BD-event: kolonel b.d. Willems (j.l.willems@xmsnet.nl)