EICAR!

Voor dit securitynummer van LAN Magazine interviewde ik Eddy Willems van Kaspersky. Willems is naast zijn job bij dat IT-securitybedrijf ook Director Information and Press van EICAR. EICAR is niet iets nieuws, want het werd al opgericht in 1991, maar voor mij was deze organisatie toch een eyeopener.

EICAR is oorspronkelijk voortgekomen uit kringen van antivirusleveranciers. De letters staan dan ook voor Europian Institute for Computer Antivirus Research. Het unieke van EICAR zit hem vooral in het streven om een gemeenschappelijk platform te creëren voor onderzoekers uit de kringen van IT-securityleveranciers enerzijds en securityvorsers uit de academische wereld anderzijds.

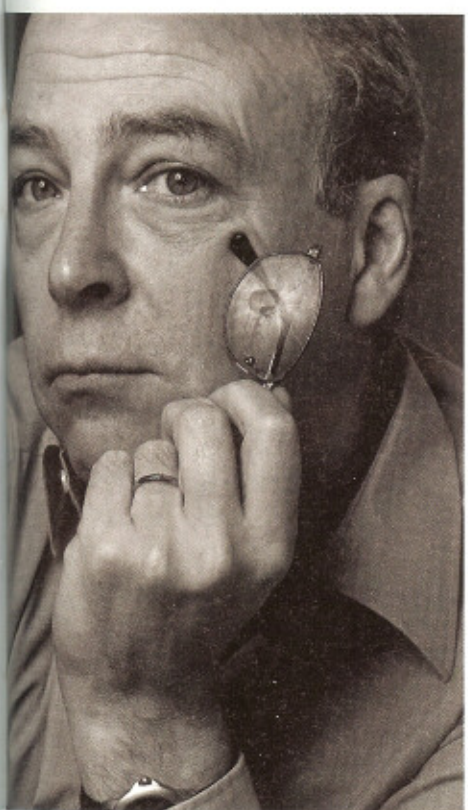
Bij hen die al wat langer meelopen in het antiviruswereldje zal EICAR vooral een belletje doen rinkelen, vanwege het EICAR-testvirus, een industriestandaard die werd ontwikkeld om eenvoudig te kunnen vaststellen of een antiviruspakket ook echt actief is nadat het is geïnstalleerd.

Dat zelf in vroeger tijden opgeplakte antivirusstempel is overigens iets dat de huidige organisatie actief probeert kwijt te raken, omdat de tegenwoordige activiteiten van EICAR het niveau van het virus ver zijn ontstegen. Men presenteert zich daarom tegenwoordig als European Expert Group for IT-Security. Het is een club waarvan zowel bedrijven als particulier geïnteresseerden lid kunnen worden. Jaarlijks wordt er ergens in Europa een conferentie georganiseerd. De laatste vond begin mei plaats in Berlijn. In mijn interview met Eddy Willems wordt er beknopt verslag van gedaan.

Met een vertraging van een maand worden de in Berlijn gehouden presentaties op de EICAR-website vrijgegeven, is mij door Willems beloofd. Gaat u als u geïnteresseerd bent in IT-security daar beslist eens kijken. Het is zeer zeker de moeite van een bezoekje waard.

Dat ik u dat kan voorspellen komt omdat mij door de organisatie reeds het boekwerk met papers ter hand werd gesteld. Ik kwam er academisch moeilijke stukken in tegen met intrigerende titels als 'Applied Parallel Coordinates for Logs and Network Traffic Attack Analysis' (EICAR 2009 Best Paper Award) en 'A Hardware-Assisted Virtualization Based Approach on How to Protect the Kernel Space from Malicious Actions'. Maar ook vlot leesbare lectuur met titels als 'From Virtual to Physical' en 'Malware in Men – Will You Be Protected', waarvan in het interview met Willems op pagina 12 tot en met 15 reeds beknopt verslag wordt gedaan.

DICK SCHIEVELS



LAN MAGAZINE Voor professionals in systeem- en netwerkbeheer; www.lanmagazine.nl

UITGEVER Drs. Werner M. Schoots

REDACTIE Dick Schievels (hoofdredacteur), Michael van Vliet (eindredacteur), Floris Hulshoff Pol (nieuwsredacteur), Mirjam Kraaij, Ivette Domburg (redactiesecretariaat)
E-mail: lanmagazine@array.nl

AAN DIT NUMMER WERKTEN MEE
Bram Dons, Jozef Schildermans, John Vanderaart, Terry Waltertang, Johan Zwiekhorst

VORMGEVING Studio Mischa Smit Kleine (mischask@xs4all.nl)

ILLUSTRATIES EN FOTOGRAFIE
Anneriek Schuurman, Mischa Smit Kleine (omslag)

DRUKWERK Thieme Media Center Nijmegen

ABONNEMENTEN
Klantenservice: Postbus 8632, 3009 AP Rotterdam
Telefoon: 010-2894008 (van 09.00 tot 12.00 uur)
Fax: 010-2894073
Aanvraag abonnement: www.lanmagazine.nl
E-mail: abonnementen@array.nl
Abonnementsprijs: € 105,50 (incl. btw)
Buitenland: € 115,50 (excl. btw)
Losse nummers: € 12,95 (incl. btw)
Abonnementen kunnen met elk nummer ingaan en worden jaarlijks automatisch verlengd. Opzeggingen, uitsluitend schriftelijk, dienen acht weken voor het verstrijken van de abonnementsperiode in ons bezit te zijn. Bij niet tijdige betaling worden herinneringskosten in rekening gebracht.

ADVERTENTIE-EXPLOITATIE
Bart Arkesteijn, Dorien Leonora, Tom van Tol (salesmanager)
Telefoon: 0172-469030

MEDIAORDER Monique Snikkers
Telefoon: 0172-469046

INTERNATIONAL REPRESENTATION
IDG Global Solutions, 29-31 Kingston Road, TW18 4LH Staines, Middlesex, United Kingdom
Telefoon: +44 1784210210
Fax: +44 1784210202

Array PUBLICATIONS
Array Publications b.v., Lemellerberg 19, Postbus 2211, 2400 CE Alphen aan den Rijn
Telefoon: 0172-469030 (algemeen), 0172-469050 (redactie)
Fax: 0172-424381
Internet: www.array.nl

HQ 2009 PRINT

 ISSN: 1574-115X

TRENDS IN BEVEILIGING

SECURITY-EVANGELIST VOORSPELT DOORBRAAK MOBIELE MALWARE

Hij rolde eigenlijk bij toeval de IT-securitywereld binnen. In 1989 werd zijn computer besmet met een Trojan-achtig ding dat de gegevens op zijn computer versleutelde. Ontsleutelen kon alleen via een betaling op een Panamese bankrekening. Eddy Willems liet zich echter niet afpersen en schreef er zelf een deëncryptie-oplossing voor. Het markeert het begin van een IT-securityloopbaan die hem drie jaar geleden bij Kaspersky Lab Benelux deed belanden.

We treffen elkaar in de vestiging van Kaspersky Lab in Den Bosch. Hij is net terug van de jaarlijkse EICAR-conferentie, dit keer gehouden in Berlijn, waarover we in de loop van het gesprek nog het nodige te horen zullen krijgen. Eddy Willems is 'IT-security-evangelist' bij Kaspersky. Zijn taak is vooruitkijken. Wat zijn op korte en lange termijn de belangrijkste dreigingen; het is díe vraag waarop hij dag in dag uit een antwoord tracht te vinden.

Gevraagd naar de belangrijkste nieuwe securityuitdaging die ons op korte termijn te wachten staat, hoeft Willems geen seconde na te denken. "Waar ik me op dit moment vooral zorgen over maak, is de groeiende malwaredreiging voor de mobiele telefoon. Wat dat betreft voorspel ik dat 2010 het kantelpunt gaat zijn. Er bestaan op dit moment al meer dan duizend virussen voor mobiele telefoons. Als je dat vergelijkt met de ruim twintig miljoen bestaande malwarevarianten voor computers, zul je misschien denken: dat stelt nog niets voor. Maar vergis je niet. Als je het vergelijkt met de opkomst van het computervirus, dan zitten we nu in het jaar 1993. Ook toen zaten we rond de duizend virussen en als je dan bedenkt hoe snel dat aantal in de jaren erna is gegroeid..."

Toch is het niet zo dat we ons vandaag al heel ernstig zorgen moeten maken, geeft Willems toe. De infectiemogelijkheden zijn op dit moment minimaal en het zijn nog relatief onschuldige probeersels. Gevraagd naar enige voorbeelden van reeds bestaande malware begint echter ook ons mobieltje in de binnenzak snel onrustig te worden. Willems schetst: "Er bestaat malware die via Bluetooth op je toestel terechtkomt en vervolgens om een confirmatie vraagt om iets te mogen downloaden. Nu zal natuurlijk vrijwel niemand daarop ingaan. Eenieder klikt dus op nee! Maar als je dat doet, krijg je direct die vraag weer terug. Het merendeel van de mensen klikt, als hij die vraag vijf keer gezien heeft, vervolgens wél op ja, om er maar van af te zijn, terwijl de remedie natuurlijk is: weglopen! Want die Bluetooth-dingen hebben maar een bereik van vijftig meter. Maar in plaats van zo die aanval te onderbreken, klikt men op ja! En dan is het onheil geschied en begint die mobiele telefoon op zijn beurt dat ding verder te verspreiden. Dat loopt op de achter-

ILLUSTRATIE: MISCHA SMIT KLEINE

grond, maar kost heel veel energie omdat die Bluetooth-connectie telkens gebruikt wordt. Dat is zó'n belasting dat het je mobiele telefoon binnen een half uur kan uitputten."

Het is een gevaar, benadrukt Willems, dat nu nog relatief meevalt en bovendien kun je het vrij eenvoudig verwijderen, maar je hebt er wel degelijk last van. En er zijn ook bedreigender zaken die op de loer liggen. Zo vertelt Willems over het bestaan van een soort van spyware dat, eenmaal op je mobiele telefoon geplaatst, de sms'jes kan onderscheppen en deze naar een aparte server kan sturen. Je kunt volgens hem zelfs zover gaan dat ook een gesprek dat je voert, gemonitord wordt en naar een server wordt gesluisd. "Dat is nu nog zogezegd legitieme software", vertelt Willems, "maar je weet natuurlijk dat als zoiets eenmaal bestaat het ooit misbruikt zal gaan worden."

Diefstal

Kaspersky brengt reeds antivirussoftware uit voor mobiele telefoons, maar dat is nu nog niet het belangrijkste, laat Willems desgevraagd weten. "Waar wij nu vooral wat aan proberen te doen, is de diefstal van mobiele telefoons." Kaspersky blijkt daarvoor een antidiefstalmodule te hebben ontwikkeld. Als een dief een mobiele telefoon steelt en zijn eigen simkaart erin steekt, zorgt het betreffende diefstalsysteem ervoor dat het telefoonnummer van de dief wordt verstuurd naar een voorgeprogrammeerd nummer. Via dat telefoonnummer kan het toestel vervolgens geblokkeerd worden en kunnen gegevens die erop staan worden gewist. Dat is belangrijk, want er zijn natuurlijk diverse zaken in je mobieltje opgeslagen waarvan je niet wilt dat een ander daarover de beschikking krijgt. "Je kunt binnenkort ook heel effectief de politie inschakelen", vertelt Willems, "omdat in het nieuwste pakket van ons nu een mogelijkheid zit om de GPS-coördinaten van je gestolen telefoon automatisch te laten doormailen."

Sociale netwerken

Een andere trend die volgens Willems van securityspecialisten de nodige aandacht vereist, is de snelle opkomst van de socialenet-

Eddy Willems van Kaspersky Lab Benelux: "Waar ik me op dit moment vooral zorgen over maak, is de groeiende malwaredreiging voor de mobiele telefoon. Wat dat betreft voorspel ik dat 2010 het kantelpunt gaat zijn."

'Waar wij nu vooral wat aan proberen te doen, is de diefstal van mobiele telefoons'

werksites. Dit zijn volgens Willems 'prachtige' nieuwe wegen voor het verspreiden van malware. "Neem bijvoorbeeld Facebook. Daarin kunnen links toegevoegd worden van een zogenaamde vriend, die in feite een malwareschrijver blijkt te zijn. Dat zijn bijvoorbeeld links van zogenaamd interessante sites die er heel normaal uitzien als je er een bezoek aan brengt. Indien je onvoldoende beschermd bent, krijg je vervolgens echter een download op je computer gepusht waar een virus inzit of spyware, en dat gaat zo verder en verder. Het is in feite een combinatie van social engineering en techniek."

Dreigingen op termijn

Wat zijn de dreigingen als we wat verder vooruitkijken? Ook daarover heeft Willems het nodige te melden. Willems is namelijk een man met twee securitypetten op. Naast zijn functie bij Kaspersky blijkt hij een van de founding members van EICAR. EICAR werd opgericht in 1991 en stond oorspronkelijk voor European Institute for Computer Antivirus Research. Die benaming is volgens Willems echter niet meer helemaal adequaat. Men presenteert zich tegenwoordig als EICAR the European Expert Group for IT-Security, een meer algemene IT-securityorganisatie, dus met securityspecialisten afkomstig uit zowel het bedrijfsleven als de academische wereld.

EICAR is met name bekend van het EICAR-testvirus, een industriestandaard die stamt uit 1993. Het is in feite een testfile die door elke antivirusvendor gebruikt wordt. Je kunt ermee uitvinden of een antiviruspakket ook echt werkt nadat je het hebt geïnstalleerd. Het is een testvirus dat niet repliceert; een piepkleine teststring die wordt gedetecteerd als zijnde de EICAR-teststring. Iedereen kan die teststring van de EICAR-website downloaden en elk antivirusproduct kan ermee worden getest.

EICAR organiseert elk jaar een conferentie, ergens in Europa. Dit jaar vond die begin mei plaats in Berlijn. Als Director Information and Press was Eddy Willems vanzelfsprekend ook van de partij. Dé publiekstrekker was dit jaar de keynote van Fred Cohen, vertelt hij. Fred Cohen definieerde in zijn proefschrift in 1984 als eerste de term 'computervirus'. Dat was dus nog voor het eerste computervirus überhaupt bestond, want dat stamt uit 1986. Zijn conclusie: computervirussen en aanverwanten zullen nooit meer verdwijnen en de tijd is gekomen dat we eens heel goed gaan nadenken over hoe we onze cyberspace en de kwetsbare infrastructuur daarachter in de toekomst gaan beschermen. Willems: "Er worden steeds meer apparaten in een netwerk gekoppeld. Neem een nieuwe tv, wat zit daaraan vast? Een Ethernet-verbinding! Een flatscreen wordt er standaard via een Ethernet-verbinding mee verbonden. Dat gaat natuurlijk ooit voor problemen zorgen. Dus moeten we daarop voorbereid zijn en onze infrastructuur daartegen wapenen, hetgeen op dit moment nog te weinig gebeurt, zegt Cohen. Ik ben het daarmee eens."

Kalkuhl

Waar we in de wat verdere toekomst qua dreigingen allemaal mee te maken kúnnen krijgen, was het onderwerp van twee presentaties van respectievelijk Magnus Kalkuhl van Kaspersky Lab en Babu Nath Giri van McAfee Avert Labs, waar Willems ons op verzoek wat uitgebreider verslag van uitbrengt. We vatten hier allereerst de belangrijkste mógelijke ontwikkelingen samen die Kalkuhl, een jaar of tien vooruitkijkend, zijn Berlijnse gehoor voorschotelde.

Volgens Kalkuhl zal de hele internetinfrastructuur sterk veranderen, vertelt Willems. De huidige structuur is veel te open en daardoor te kwetsbaar. Van vele kanten is reeds het idee geopperd een internetpaspoort in te voeren en volgens Kalkuhl is het nog maar een kwestie van jaren voordat we bepaalde webservices alleen nog kunnen benaderen via een unieke identificatie. Dat zal er toe leiden dat het internet zal worden opgesplitst in een aantal virtuele eilanden, hetgeen hoogstwaarschijnlijk weer een te-

gencultuur zal oproepen van volledig ongecontroleerde netwerken, die in bepaalde landen verboden zullen worden maar waarvan niettemin uitgebreid gebruik zal worden gemaakt door mensen die van het officiële internet zijn verbannen.

Een ander belangrijk aspect waar Kalkuhl tijdens zijn lezing op inzoomde, was privacy. Wat je niet onder controle hebt, kun je niet beschermen en dat is precies wat er aan de hand is met onze privacy in de eenentwintigste eeuw, aldus Kalkuhl. "Sommige websites eisen tegenwoordig gewoon de invoer van persoonlijke data en wat er daarna mee gebeurt, onttrekt zich aan je controle. Daarnaast: persoonlijke gegevens die eenmaal op internet belanden, zijn daar nooit meer van af te krijgen. Eén gedachteloze opmerking in een weblog kan je dus tot in lengte van dagen blijven achtervolgen. Je kunt nergens heen vluchten als je je reputatie te grabbel hebt gegooid op internet." Kalkuhl ziet maar één oplossing voor dit probleem: meervoudige persoonlijkheden, ook wel bekend als avatars. Hij acht het niet onwaarschijnlijk dat we binnen tien jaar bij onze geboorte nog zullen worden uitgerust met één hoofdidentiteit, maar dat dat niet langer meer onze enige identiteit zal zijn en dat we straks diverse subidentiteiten zullen hebben voor zaken als werk, winkelen, et cetera. Als een daarvan om wat voor reden dan ook onbruikbaar is geworden, kun je gewoon een nieuwe aanvragen, net zoals je nu een nieuw paspoort kunt aanvragen als je het oude kwijt bent.

Een derde belangrijke nieuwe dreiging komt voort uit het feit dat onze huiselijke omgeving in de toekomst meer en meer gedigitaliseerd zal worden en via Ethernet of draadloos verbonden zal zijn met internet. "Een gehackte koffiemachine, inmiddels geen fictie meer, zal misschien alleen je dag bederven, maar als de controle over je gehele huis in handen van iemand anders belandt, ben je een gevangene binnen je eigen muren", aldus Kalkuhl in Berlijn. "Staat HIPS straks voor House Intrusion Prevention System?"

Nath Giri

Onder de titel 'Malware in Men – will you be protected?' hield ook Babu Nath Giri van McAfee Avert Labs een voordracht waarin een blik werd geworpen op de mogelijke securityproblemen waarmee we in de toekomst te maken kunnen krijgen. De kern van de boodschap van Nath Giri luidt volgens Willems: computers zullen hun invloed op onze maatschappij steeds verder uitbreiden, ontregelende malware dus ook. "Computers vind je tegenwoordig overal in terug, van satellieten en mobiele telefoons tot auto's en koffiezetapparaten. Was het voorheen zo dat mensen zich toegang verschaften tot computers om ze te besturen en te repareren, tegenwoordig beginnen computers zich toegang te verschaffen tot de mens", aldus Nath Giri. "Hoe wapenen ons daartegen?"

Nath Giri schetst ontwikkelingen als een digitale miniatuurcamera die in het oog van een blinde wordt gemonteerd, waarbij elektrische signalen via een microprocessor op de zenuwuiteinden in de visuele cortex worden overgebracht. En iedereen kent de ontwikkeling die we in de meer bekende wereld van de kunstmatige ledenmaten doormaken. Door middel van de miniaturisering van draagbare devices en verbeteringen in draadloze connectiviteit kunnen doktoren de conditie van een patiënt steeds beter in de gaten houden. BAN's (Body Area Networks) en PAN's (Personal Area Networks), zowel in bedrade als in draadloze vorm, liggen op dit vlak in het verschiet. Zodra dit echt tot wasdom komt, zal ook misbruik in dit domein de kop op steken. Verzekeringsmaatschappijen en de farmaceutische industrie zullen bijvoorbeeld zeer geïnteresseerd zijn in de data die over dit soort BAN's en PAN's rouleren. Als dit soort systemen zich een blijvende plaats willen veroveren in kritieke omgevingen als de medische wetenschap, zullen ze daarom vanaf het allereerste design moeten worden ontworpen vanuit een securityperspectief, vat Willems de slotconclusie van Nath Giri samen. Willems zelf tot slot: "Daarvoor zijn wel nieuwe wetten en standaarden nodig, typisch een gebied waarvoor met name een organisatie als EICAR de nodige impulsen kan leveren."

EICAR is met name bekend van het EICAR-testvirus, een industriestandaard die stamt uit 1993