Tien trends in IT security

Ook het voorbije jaar heeft men in de securitywereld niet stilgezeten. Nieuwe platforms zorgden voor nieuwe kwetsbare plekken, die dan weer nieuwe opportuniteiten opleverden voor de nieuwe criminelen. Gelukkig blijven (oude en nieuwe) securityspecialisten waakzaam en snellen zij ons ook nu weer met nieuwe oplossingen ter hulp. Wij selecteerden voor u tien opvallende trends. STEF GYSSELS

TREND 1: LEK 2.0

Sociale netwerken zijn zo lek als een zeef. Dat lijkt de algemene teneur wanneer we beveiligingsexperts aan het woord horen. Het grote gevoel van vertrouwen dat mensen in sociale netwerken stellen ("We zijn toch onder vrienden") schept ook een vals gevoel van veiligheid. Niet alleen zorgt dat voor ontboezemingen die enkel voor die vriendengroep bedoeld zijn maar wel door iedereen gelezen kunnen worden (zie ook pagina 20), men springt ook veel slordiger om met bedreigingen.

En die bedreigingen zijn er steeds meer. "Logisch ook," vindt **Stefan Tanase**, onderzoeker bij Kaspersky Lab, "want kijk maar eens naar de populariteit van dat platform. Zelfs president Obama zet de *'stay connected'*-knoppen van Facebook, Twitter en andere netwerken hoger dan de link naar het budget voor 2010. En iedereen weet intussen: hoe populairder het platform, hoe groter het aantal aanvallen. Intussen zijn er tot eind 2008 al 43.000 verschillende gevallen van malware aangetroffen die zich via sociale netwerken verspreiden. En 26.000 daarvan werden in 2008 vastgesteld."

> "Hoe populairder het platform, hoe groter het aantal aanvallen."

De kans op verspreiding is ook zoveel groter, merkt Stefan Tanase op: "De kans op besmetting is 10% bij verspreiding via een sociaal netwerk, en maar 1% bij verspreiding door e-mail." Dat heeft dus met het valse gevoel van veiligheid te maken, maar bijvoorbeeld ook met het gebrek aan controle op de toepassingen die op Facebook verschijnen. Dat maakt het perfect mogelijk om gebruikers te lokken om een toepassing te installeren waarmee ze elke dag een nieuwe mooie foto zouden ontvangen, maar die tegelijk ook een pc kan overnemen om hem in een botnet in te schakelen. "Dat is trouwens geen theoretische mogelijkheid", waarschuwt Tanase. "Iemand heeft het experiment uitgevoerd, en met succes. Gelukkig was het alleen bedoeld als *'proof of concept'* om op de gevaren te wijzen."

Facebook heeft al gereageerd door een controleprogramma te lanceren waarmee applicaties gecertificeerd kunnen worden. Maar er zijn wel twee probleempjes. Ten eerste zijn ruim vijftigduizend toepassingen op Facebook, die door een beperkt team gecontroleerd worden. Ten tweede wordt er jaarlijks hernieuwbare bijdrage van 375 dollar gevraagd aan de ontwerpers van die toepassingen. De meerderheid van de bouwers van Facebook-toepassingen lijkt daar geen zin in te hebben, want voor hen is het meestal ook een vrijetijdsproject.

Andere oplossingen zijn bijvoorbeeld zogeheten *'virtual sandboxes'*, een virtuele omgeving die door antimalwareprogramma's kan worden opgestart en waarin browsers veilig kunnen draaien. "Het leuke daaraan is dat u bij het afsluiten van een browsersessie meteen ook alles sluit wat u tijdens die sessie hebt opgestart, zonder dat het een impact heeft op uw pc", vertelt **Eddy Willems,** security evangelist bij Kaspersky Lab. "Dat helpt overigens niet alleen tegen de gevaren op sociale netwerken, maar ook om gewoon een online gevonden toepassing eerst even uit te proberen, zonder dat die op uw systeembestanden kan ingrijpen."

Ook Twitter kent malwareproblemen. Er werd bijvoorbeeld een worm ontdekt die in elke entry het woord 'Mickey' toevoegde. Behoorlijk onschuldig, dat wel, maar evengoed had die worm inloggegevens kunnen onderscheppen. "Sociale netwerken kunnen de productiviteit van de medewerker verhogen, maar de risico's loeren om de hoek. En daar is niet iedereen zich even bewust van", besluit Stefan Tanase.

TREND 2: MOBIELE MALWARE

Net als de sociale netwerken worden ook de smartphones steeds populairder. En ook daar heeft dat gevolgen voor het aantal virussen. In vergelijking met ongeveer drie jaar geleden is het aantal nieuwe virussen bijna verdrievoudigd. Intussen zijn ook gewone gsm's vaker het mikpunt van malwareaanvallen. Daarbij verschuift de aandacht van de Symbian-toestellen naar J2ME, het Java-platform voor mobiele toestellen. Ook Windows Mobile begint eindelijk erkend te worden door de malwareschrijvers.

Opvallend detail: voor de nochtans steeds populairder wordende iPhone valt voorlopig geen malware te bespeuren. Maar dat hoeft niemand te verbazen, want in tegenstelling tot bij Facebook wordt bij Apple (voorlopig?) wel een politiek gehanteerd waarbij enkel geautoriseerde toepassingen hun weg naar dat mobiele platform kunnen vinden. Dat maakt de bewegingsruimte voor malwarebouwers bijzonder klein.

belangrijk verschil met de malware in de sociale netwerk is dat er al een hele business is ontstaan rond het schrijven malware voor gsm's. Enerzijds met het schrijven van spamdschappen die zich onder meer via het altijd beschikbare programma ICQ verspreiden. Anderzijds met het installen van *trojans* die ervoor zorgen dat de gsm of smartphone bellen of sms'jes sturen naar betaalnummers. Voorlopig dt daartegen weinig ondernomen door bijvoorbeeld de operators. Zij knijpen gemakkelijk een oogje dicht, volsommigen omdat een groot deel van de winst uit zulke de ook naar hen vloeit.

REND 3: MALWARE LOONT

t voorbeeld hierboven toont aan dat malware schrijven eds minder tot het domein van de *geeks* en de grappenmabehoort. Malware is *big business* en wordt steeds meer speelterrein van de georganiseerde misdaad. Misdaad trouwens almaar minder verborgen blijkt. Op sites als al cash.com kunt u de tarieven nalezen voor het omzetten spam in betalende klanten. Een ander vaak voorkomend omeen is de worm die malware installeert en vervolgens gebruiker op de hoogte stelt van de aanwezigheid van die ware. Dan krijgt de gebruiker de kans om door te klikken een site waarop hij antivirussoftware kan kopen om van malware af te geraken. Een gijzeling op klaarlichte dag dus, n zowat 10% van de gevallen ook daadwerkelijk een aanopoplevert.

bijkomende reden voor het succes van zulke acties is de oud waarmee geld van de gebruiker kan worden afgetrog-Betalingen per gsm, per kredietkaart, gewone overschrijgenenzovoort, alles kan naar één centrale (internet)rekening den gestuurd waarvan de eigenaar vaak moeilijk te achterer is. En als dan eens een malwareschrijver of hacker wordt ekend, blijft het grote brein achter de organisatie meestal kend of kan hij wegens gebrek aan bewijslast niet ingend worden.

Volgens **Eugene Kaspersky**, oprichter en CEO van Kaspersky Lab, is cybercriminaliteit een nieuw speelterrein, met dus ook totaal nieuwe spelers. Cybercriminelen zijn geen onderdeel van de traditionele georganiseerde misdaad. Bestaat dan niet de mogelijkheid dat de cybermisdadigers weldra worden opgeslokt? "Absoluut niet", lacht Kaspersky. "De sommen die wereldwijd met cybercriminaliteit worden verdiend, zijn vele malen groter dan wat met de traditionele misdaad wordt binnengerijfd. Het zullen dus eerder de cybercriminelen zijn die de traditionele bendes opslorpen dan omgekeerd."

EUGENE KASPERSKY,
oprichter en CEO van Kaspersky Lab:
"De sommen die wereldwijd met cybercriminaliteit worden verdiend, zijn vele malen groter dan wat met de traditionele misdaad wordt binnengerijfd."

KRIS SCHELKENS, channel manager van Checkpoint Software Belux: *"USB wordt door mensen uit het beveiligingsmilieu vaak 'unintentional security breach' genoemd."*

TREND 4: TERRORISTEN AAN DE NETWERKPOORT

Eugene Kaspersky maakt zich wel zorgen over de gevolgen op een ander vlak. Als malware tot zulke winstgevende activiteiten kan leiden, kan het ook gebruikt worden voor andere doeleinden, zoals terrorisme. "Dat staat eraan te komen", zegt hij overtuigd. "Als je ziet waar nationale overheden mee bezig zijn. Zo bestaan er al verschillende bewijzen van Amerikaanse aanvallen op de netwerken van onder andere Estland, Georgië en Iran. Als nationale overheden dat kunnen, kunnen terroristen dat ook. En wat nog erger is: Hollywood toont hen overduidelijk hoe het moet."

TREND 5: CONFICKER

Misschien kun je Conficker niet echt een trend noemen, maar de komst van de worm heeft het hele securitywereldje toch geruime tijd beziggehouden, en doet dat nog altijd. Conficker bleek een uiterst goed ontworpen worm die zich niet alleen razendsnel verspreidde, maar ook bijzonder goed geëncrypteerd is en alle mogelijkheden om de worm snel uit te schakelen (Windows updater, surfen naar antivirussites) volledig blokkeert. Op 1 april zou de besmette pc's iets dramatisch overkomen, zo werd gevreesd, maar uiteindelijk bleek het nogal onschuldig: gebruikers kregen hooguit de boodschap om valse antivirussoftware te kopen om hun pc schoon te maken. Maar er werd wel duidelijk meer contact gemaakt met andere servers, wellicht om nieuwe malware te downloaden. Veel van de pc's zijn intussen al gedesinfecteerd, maar er blijven naar schatting nog enkele miljoenen besmette pcs over. "Maar dat is enkel van één type van de Confickerworm", waarschuwt Eugene Kaspersky. "Als je de twee andere types erbij telt, kom je wellicht aan een tiental miljoen. Dat is dus een botnetsupermacht van tien miljoen pc's. Als die gelijktijdig worden ingezet, zijn de gevolgen nauwelijks te overzien."

TREND 6: USB = UNINTENTIONAL SECURITY BREACH

Alsof het aantal bedreigingen nog niet volstond, is er ook nog de USB-stick. Dat kleine, meestal onschuldige stukje metaal baart beveiligingsexperts bijzonder veel zorgen. Vooral de wildgroei aan USB-sticks veroorzaakt nachtmerries. Daardoor weten mensen niet meer of een stick van hen is of van iemand anders. Het Nederlandse actualiteitenprogramma Nova nam de proef op de som, en slingerde in een aantal organisaties enkele USB-sticks op de grond. In één geval op vier werden die opgeraapt en in een pc gestoken, waarna een eenvoudig programmaatje allerlei cruciale gegevens over de pc naar hun kon doorsturen.

"USB wordt door mensen uit het beveiligingsmilieu dan ook *'unintentional security breach'* genoemd," vertelt **Kris Schelkens**, channel manager van Checkpoint Software Belux, "want naast dat experiment van Nova zijn er ook minder openbare maar wel geslaagde pogingen door cybercriminelen geweest."

TREND 7: CLOUD VERSUS ENDPOINT

Net als bij alle andere types software wordt ook voor securitysoftware de vraag gesteld of ze niet beter *'in the cloud'* kan worden gezet. Daar zijn goede argumenten voor. Neem bijvoorbeeld spamfilters: als die buiten het bedrijfsnetwerk worden gezet, is de mail al gefilterd nog voor hij het bedrijf bereikt en wordt die extra belasting van de eigen servers weggehouden.

Maar dat heeft dan weer andere implicaties. Zo is de trend hierboven er al een perfecte illustratie van waar security in the cloud' tekortschiet. Als u alles controleert in de wolken heeft u namelijk geen controle over de zogeheten 'endpoints' in het bedrijf. USB-poorten zijn daar één voorbeeld van, maar

ele toestellen en al het andere digitale materiaal dat het ofsnetwerk verlaat en terug binnenkomt, ontsnappen ook controles in de wolken. "Steeds vaker zit gevaar voor uw frastructuur binnen de bedrijfsmuren, en dat kan met een ging 'in the cloud' nooit ondervangen worden", vat Kris kens samen.

zowat iedereen het erover eens dat u een beveiligingsin de wolken kunt overwegen, als het een intern draaibeveiligingsinfrastructuur ondersteunt of aanvult. "Als curitysoftware in de cloud één van de verdedigingslinies kan het wel," vindt **Luc Dooms**, CEO van C-Cure, "maar daarop vertrouwen is zeker geen goed idee, ook al omtotaal geen controle meer hebt over je beveiligingsinctuur."

aast blijft de vraag of ook de toepassingen in de cloud voldoende beveiligd zijn. Daar hangt uiteraard alles af de leveranciers van die toepassingen. Zij zullen natuurlijk een dat ze extra goed beveiligd zijn, maar nu al klinken men uit de industrie om daarvoor een externe audit in te en zodat leveranciers hun beveiligingspolicy kunnen laten oeren.

END 8: VIRTUEEL VEILIGD?

virtualisatie is een allesbehalve evident gegeven voor wie beveiliging bezig is. Enerzijds moet u kunnen beveiligen et niveau van elke virtuele module. "Dat is nodig om de uriteit te bewaren," merkt Luc Dooms op, "want anders t je de strengst mogelijke beveiliging hanteren voor de gevirtualiseerde omgeving, terwijl dat niet voor alle toegen noodzakelijk is." Anderzijds moet u ook opletten et verschuiven van bestanden van de ene naar de andere op een beveiligde manier gebeurt, dus eigenlijk is er veiliging op hardwareniveau nodig.

beide types beveiliging zijn er al heel wat oplossingen baar, maar dat maakt het geheel er niet goedkoper op. een factor die bij de TCO-berekening van virtualisatie vergeten wordt, en dus niet altijd even warm wordt ontwanneer beveiligingsspecialisten erover beginnen.

END 9: MANAGEMENT ZOCHT

wat hierboven al werd beschreven, zal het niemand en dat IT-managers en zelfs securitymanagers binnen ven het almaar moeilijker hebben om het geheel aan igingsmiddelen nog te overzien, laat staan het onder controle te houden. Dat verklaart waarom bij veel securityleveranciers ook managementtools te verkrijgen zijn. Enerzijds om de wildgroei aan beveiligingsoplossingen onder controle te houden. "Geen overbodige luxe," zegt ook Kris Schelkens, "want de meeste pc's zitten vol *'agents'* - meestal minimaal vijf - die zorgen voor een lange opstarttijd, en vaak ook voor crashes wegens een foute volgorde van opstarten."

> "Het gevaar voor uw IT-infrastructuur zit vaak binnen de bedrijfsmuren."

Maar er is nog een ander niveau waarop een goed overzicht het verschil kan maken. Wie de informatie over de activiteiten van alle beveiligingspakketten kan verzamelen en analyseren, krijgt soms een inzicht dat met elke afzonderlijke oplossing nooit zou worden bereikt. "Stel dat je een poortscan op je firewall vaststelt," geeft Luc Dooms als voorbeeld, "en daarna een bevraging van de mail server, vervolgens van de web server, en daarna van de DNS server. Elk afzonderlijk zeggen die events weinig, maar als je ze kunt combineren, kun je wel besluiten dat er een ernstige aanval in de maak is." Dat soort beheer heet *SIEM*, kort voor *security information and event management*. "Het helpt bovendien niet alleen voor externe bedreigingen maar kan ook wijzen op minder deontologische activiteiten binnen het bedrijf, een toegevoegde waarde die vooral grotere bedrijven appreciëren", aldus Luc Dooms.

TREND 10: WINDOWS 7

Tot slot kunnen we ook niet voorbij aan de komst van Windows 7 dit najaar. Dat wordt de versie waarin de gebruiker eindelijk niet meer met die schijnbaar eindeloze reeks van bevestigingsschermen wordt geconfronteerd. "En maar goed ook," meent Eddy Willems, "want dat zorgde bij veel eindgebruikers voor een verkeerde reflex. Niemand dacht nog na over wat hij nu eigenlijk aan het bevestigen was. Met de komst van Windows 7 zal dat hopelijk weer een stuk bewuster gebeuren."