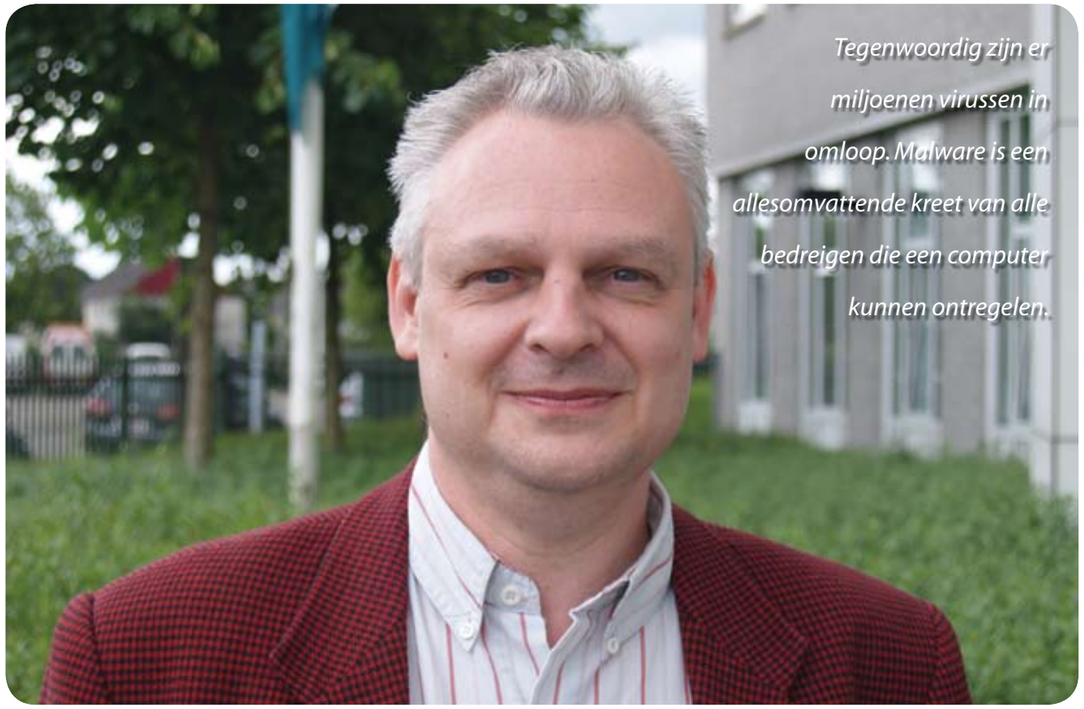


Interview: Eddy Willems, IT-Security evangelist

Kaspersky Lab biedt bescherming tegen virussen, spyware, spam en hackers

Kaspersky Lab is een internationaal softwarebedrijf dat geavanceerde Secure Content Management oplossingen aanbiedt, die thuisgebruikers en (grote) netwerkomgevingen beschermt tegen virussen, spyware, spam en hackers. De succesvolle detectie en het onderscheppen van virussen hangt volgens Kaspersky Lab van constant virusonderzoek af.
In 2006 kwamen er 500.000 nieuwe virussen bij. Dat zijn er evenveel als alle virussen van 1986 tot 2006 bij elkaar opgeteld. In 2007 vond er wederom een verdubbeling plaats naar een miljoen virussen. In het eerste half jaar van 2008 is het weer een optelsom en komen we uit op twee miljoen bedreigingen. De verwachting is dat er dit jaar tien miljoen virussen of malware in omloop komen. Hotspot neemt het zekere voor het onzekere en spreekt met IT-Security evangelist Eddy Willems van Kaspersky Lab over de internetbedreigingen, het wel en vooral wee van spam, maar ook over de kansen voor retail. In augustus komt Kaspersky Lab namelijk met een nieuwe Kaspersky Anti-virus, Kaspersky Internet Security en Kaspersky Mobile Security.

Wat houdt dat nu precies in: IT-Security evangelist?
"Ik behoor tot de groep van analisten die als taak heeft om in eenvoudige taal uit te leggen wat er op het vlak van beveiliging van computers speelt. Dit doe ik zowel richting bedrijven als de media. Het is belangrijk dat er duidelijke communicatie is over de beveiliging van bijvoorbeeld een bedrijfsnetwerk, een computer, notebook of handheld. De voorlichting aan bedrijven is vaak wel technischer, omdat daar ook mensen werkzaam zijn met een technische achtergrond."

Kaspersky Lab is als bedrijf voor velen misschien nog wat onbekend als aanbieder van Anti-virus en Security oplossingen?
"Kaspersky is een bedrijf dat enorm in opmars is. Wereldwijd zijn we een Top 5-speler. We nemen in de consumentenmarkt in veel landen de tweede en derde plaats in. Ook in de zakelijke markt doet Kaspersky Lab het bijzonder goed met wereldwijd een soms een nummer 5 en dan weer 4 notering. Het is niet voor niets dat 14 van de 27 ICT-bedrijven aan de Nasdaq kiezen voor Kaspersky als engine voor hun security."

Wat maakt Kaspersky Lab dan onderscheidend?
"Kaspersky heeft een duidelijke focus op security. Je ziet vaak concurrenten die bijvoorbeeld software-ontwikkelaars kopen. Zij komen dan met een hele waaier aan producten. Kaspersky heeft een duidelijke focus op anti-virus en mallware. Alles-in-een producten hebben vaak het nadeel dat ze geen duidelijke focus hebben. Het is een van-alles-en-nog-wat pakket. Je kunt een analogie trekken. Bij een muziekinstallatie leveren losse componenten een beter resultaat op dan louter een stereotoren."

Is het nu zo dat door die enorme stijging van virussen het bestrijden van virussen verandert?
"Bij het nieuwe Kaspersky Anti-virus 2009-pakket maken we gebruik van nieuwe technologie om virussen buiten de deur te houden. De virus-scanner zit er natuurlijk in. Dat is de vertrouwde technologie. We maken nu gebruik van vier soorten technologie: één handtekening, twee behaviour blocking, drie heuristics en vier desktop firewall. Daarboven heeft het nieuwe pakket ook nieuwe technologie aan boord, maar daarover later meer."

Heuristics?
"Heuristics een speciale manier om een nieuw virus dat nog niet bekend is te detecteren zonder gebruik te maken van de virushandtekeningen. Via een analyse wordt er gekeken of er gevaarlijke bestanden tussen zitten. Heuristics werkt op een vergelijkbare manier als een scanner, maar dan veelzijdiger en intelligenter."

En wat doet behaviour blocking?
"Bij behaviour blocking wordt er gekeken naar het gedrag dat een programma vertoont. En behoort te vertonen. Behaviour blocking voorkomt bijvoorbeeld dat de harde schijf zo maar wordt geformateerd."

De vierde technologie, desktop firewall, wordt toch vaak standaard geleverd bij een nieuwe computer?
"Er wordt inderdaad vaak bij de aanschaf van een nieuwe computer of notebook wel een firewall geleverd, maar dit basisprogramma komt niet tegemoet aan alle aanvallen die er momenteel zijn. In veel gevallen houdt zo'n firewall aanvallen van buitenaf wel tegen, maar niet van binnen naar buiten. Zo voorkomt een dergelijke basis desktop firewall niet dat er spontaan e-mails worden verstuurd."

Kan er niet een soort virtuele portier bij een computer worden gezet om al die virussen en zo tegen te houden?
"Het vooraf signaleren en detecteren van virussen heet intrusion prevention. Intrusion prevention voorkomt een aanval van buitenaf en blokkeert een aanval voordat die de pc binnenkomt. Er wordt de aanval een halt toegezegd. Overigens verlangt deze technologie, het buiten de deur houden van virussen, een heel andere aanpak dan alleen het signaleren van een aanval. Maar goed: dat is een technisch verhaal."

Is er nu een goed voorbeeld van een virus waarvan we wakker zouden kunnen liggen?
"Een vervelend virus is de Gpcode.ak. Gpcode.ak versleutelt bestanden met verschillende extensies zoals .doc, .pdf, .xls, .jpg door het gebruik van een RSA-encryptie-algoritme met een 1024-bits sleutel. Nadat Gpcode.ak bestanden heeft versleuteld op de computer van het slachtoffer, verandert het de extensie van deze bestanden naar ._CRYPT en plaatst een tekstbestand genaamd !_READ_ME!.txt in dezelfde map. In het tekstbestand vertelt de cybercrimineel het slachtoffer dat de bestanden versleuteld zijn en biedt tegen betaling een decryptor (ontsleutel-bestand) aan. Op de koop toe verwijdert het virus zichzelf achteraf om onderzoek door specialisten te bemoeilijken."

Fijne jongens.
"De schrijver van Gpcode heeft er twee jaar over gedaan om het virus te verbeteren. De voorgaande fouten zijn gecorrigeerd en de sleutel is verlengd tot 1024-bits in plaats van 660-bits. De virusonderzoekers zijn tot nu toe in staat geweest om sleutels tot 660-bits te ontmantelen. Dit was het resultaat van gedetailleerde analyse van de RSA algoritme-uitvoering. Naar schatting kost het 1 PC met 2.2 Ghz, als het algoritme goed is uitgevoerd, maar liefst 30 jaar om een 660-bit sleutel te kraken."

En is een 1024-bits te ontsleutelen?
"Het kraken hiervan is een zeer gecompliceerd cryptografisch probleem. Voor het kraken van de sleutel moeten minstens vijftien miljoen computers één jaar draaien."

Wat moet iemand nu doen wanneer zo'n virus wordt opgemerkt?
"In geval van infectie raadt Kaspersky slachtoffers aan contact op te nemen met Kaspersky door gebruik te maken van een andere computer. Start de geïnfecteerde computer niet opnieuw en sluit hem niet af."

Gelden dit soort dreigingen nu ook voor de nieuwe generatie smartphones, met besturingssystemen als Windows Mobile?
"Op dit moment zijn er 500 bedreigen voor de mobiele telefoon. Ten opzichte van de malware in totaliteit is dat aantal verwaarloosbaar. Op dit moment zijn er een miljoen malware actief. Dit aantal groeit dagelijks enorm hard."

Is er een overeenkomst tussen mallware voor pc en smartphone?
"Het aantal malware voor de mobiele telefoon nu is vergelijkbaar met de opkomst van de personal computer in 1991, 1992. Toen waren er voor de pc ook slechts 500 malware in omloop. Daarna was er een exponentiële groei in het aantal bedreigingen. De verwachting is dat dit ook voor de mobiele telefoon gebeurt. Zeker met de opkomst van smartphones en besturingssystemen zoals Windows Mobile die veel raakvlakken hebben met het desktop besturingssysteem."

En Kaspersky is daar als één van de eerste bij?
"Bij het signaleren van malware voor mobiele telefoons is het belangrijk om daar als specialist een product voor te hebben. Natuurlijk moet er wel relevantie voor zijn. Feit is dat malware voor mobiele telefoons sneller zal evolueren dan malware voor de pc omdat deze markt en masse in beweging is en uiteindelijk groter is dan de pc-markt."

Nu zou je denken: iedereen heeft anti-virus op zijn pc, zowel consumenten als ondernemers?
"20 procent van de particulieren en ondernemers heeft geen interesse in wat voor vorm van beveiliging ook. Zo'n 80 procent heeft bij de ➲

aanschaf van een nieuwe computer een anti-viruspakket op de computer staan die vaak zo'n 6 tot 12 maanden werkzaam is. Daarna laten ze vaak achterwege om het abonnement te verlengen. Slechts 25 procent van de computers is goed beveiligd. Driekwart van de computers is dus niet beveiligd tegen malware en andere bedreigingen."

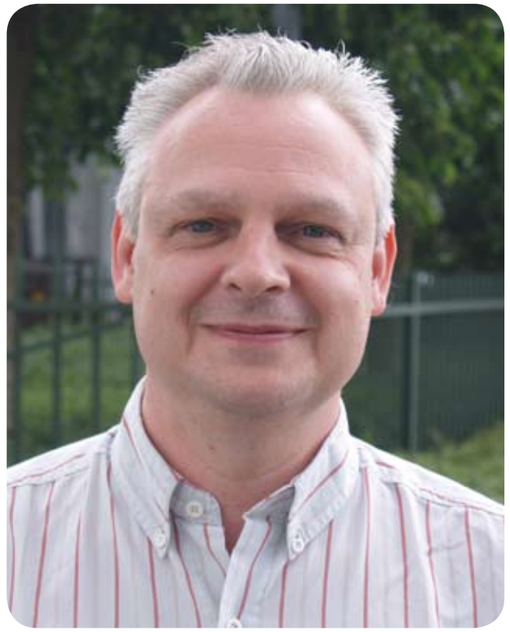
Wat voor gevaar loopt een niet-beveiligde pc?
"Een gevaar is dat de computer een onderdeel wordt van een botnet. Bij een botnet maakt de hacker gebruik van iemands computer om bijvoorbeeld spam te versturen. De problematiek van botnets kan ver gaan. Er zijn botnets bekend waar zo'n 100.000 tot 500.000 computers worden gebruikt, of beter gezegd misbruikt, om spam te versturen. Het heeft dan vaak geen zin om een site waar spam vandaan wordt gestuurd, plat te leggen."

Spam is ongewenste mail, maar bevatten ze ook altijd virussen?
"Grofweg zijn er twee soorten spam. Spam zonder virussen en spam met virussen. Er wordt ook veel geld verdiend met spam zonder virussen. De Rolex en Viagra spam-berichten doen het goed. Met een minimale respons kunnen er per saldo toch nog een heleboel reacties komen op een spam-bericht. Zeker als deze enkele honderdduizenden keren wordt verstuurd. Verhoudingsgewijs zijn de kosten dan laag. Wat opvalt, is dat alles wel steeds vaker met elkaar verweven is. Spam is bijvoorbeeld ook een methode om het botnet netwerk verder uit te breiden."

Een ander gevaar is ongetwijfeld phishing?
"Via een phishing link wordt de gebruiker naar een website geleid die er bijvoorbeeld uitziet als die van de Rabobank of de Postbank. Via de link worden allerlei vertrouwelijke gegevens achterhaald. Bij het monitoren van sites van de 'onderwereld' zien we soms dat verschillende credit card gegevens te koop worden aangeboden. En daar geldt natuurlijk wel dat de ene creditcard meer waarde heeft, dan de ander. De credit card gegevens van een 'Bill Gates' leveren nu eenmaal meer op dan die van Jan met de Pet."

Is er geen methode om gegevens veilig in te voeren?
"Een plezant voorbeeld is het virtuele keyboard. Deze virtuele keyboard is ideaal voor het invoeren van beveiligde gegevens, bijvoorbeeld pin codes. Het virtueel keyboard voorkomt 1. dat tijdgegevens weg gaan en 2. voorkomt het stelen van een password. Het virtueel toetsenbord van Kaspersky heeft geen vaste plaats op het scherm dus de toetsaanslagen zijn niet te achterhalen. Hackers kunnen, mochten ze de informatie op de één of andere manier toch in handen krijgen, dus niets met dergelijke informatie."

Kaspersky kiest bij de 2009-versies ongetwijfeld voor veel nieuwe technieken?
"De verbeteringen die Kaspersky in de 2009-versies heeft doorgevoerd hebben allemaal betrekking op de ontwikkelingen die bij deze tijd horen. Een belangrijke vernieuwing is bijvoorbeeld de hybride protectie. Aan de ene kant werkt deze protectie als bij de bekende anti-virus. We maken echter nu ook gebruik van white listing. Bij het bestrijden van virussen werd er natuurlijk al gewerkt met black listing."



"Het is niet voor niets dat 14 van de 27 ICT-bedrijven aan de Nasdaq kiezen voor Kaspersky als engine voor hun security."

Waarom naast black listing ook white listing?
"Bij white listing worden programma's op de computer eerst goed geanalyseerd. Kaspersky beschikt over een grote database waaraan deze programma's allemaal moeten voldoen. Als deze programma's eenmaal zijn gescand dan komen ze op de white list. Alleen als er aanpassingen zijn in het programma voert Kaspersky 2009 een nieuwe controle uit. Uiteraard wordt er continu gekeken waar een programma voor is en waar eventueel misbruik gemaakt kan worden."

En dat bespaart tijd bij het scannen op virussen en andere gevaren?
"Eén check op veranderingen is handiger dan kijken of één van de 600 of 700 duizend mallwares actief is in een programma. Ieder programma is een soort van som. Kaspersky kijkt en vergelijkt en zoekt naar afwijkingen. Het zoeken naar een afwijking neemt, zoals zojuist al aangehaald, bij een scan minder tijd in beslag dan een heel programma doorzoeken."

Er wordt dus wat afgescand?
"Inderdaad. Een andere volledig complete vernieuwing bij scanners is de Vulnerability scanner. De Vulnerability scanner signaleert dus ontbrekende updates en daarmee dus ook beveiligingsrisico's. Het programma informeert ➲

de pc gebruiker over ontbrekende updates, bijvoorbeeld als er een nieuwe Adobe patch is."

Bij Security komt dus heel wat kijken.
"Beveiliging is belangrijk. Ondernemers kunnen ook flink wat geld besparen als zij al die spam-berichten buiten de deur houden. Kasperksy heeft sowieso producten die ondernemers tegemoet komen. Zo maakt Software as a Service (SaaS) een enorme ontwikkeling door bij MKB of, zoals we in België zeggen, KMO. Kasperky heeft daarvoor een speciaal pakket: Kaspersky Hosted Security Services."

Kaspersky Hosted Security Services?
"Kaspersky Hosted Security Services heeft drie technologieën aan boord: 1. e-mail technologie, 2. web protectie en 3. instant messaging. In het eerste geval zorgt Kaspersky dat alle spam op de server wordt gemonitoord en dat spam automatisch wordt verwijderd. Dat scheelt heel wat spam en zorgt voor schonere mail boxen. Ook zorgt het voor meer bandbreedte op het netwerk. Web protectie zorgt ook voor een optimale beveiliging bij webmail. En 3. zorgt voor beveiliging bij instant messaging zoals MSN en Live Mail. Belangrijk is vooral het feit dat al deze activiteiten buiten het bedrijf of de gebruiker gebeuren op de servers bij Kaspersky lab zelf wat de garantie van veiligheid en gemakkelijkheid van installatie garandeert. Je ontlast het (bedrijfs)netwerk in feite van al deze instellingen en installaties."

Ondernemers moeten dus overal rekening mee houden?
"Voor ondernemers spelen steeds meer zaken. Volgens de Europese Richtlijnen zijn ondernemers straks verplicht om drie jaar hun e-mails te bewaren. Deze optie zal standaard binnenkort aangeboden worden bij Kaspersky Hosted Security Services, ook weer iets waar de ondernemer van ontlast wordt zodat hij zich kan richten op zijn core-business."

Tot slot: wat maakt Kaspersky nu onderscheidend ten opzichte van de concurrent?
"Kaspersky zorgt ieder uur voor een automatische upload. Het is het standpunt van Kaspersky dat er elke seconde een nieuwe bedreiging is. Zeker met de productiviteit van malware is een dagelijkse update echt ontoereikend. Uiteindelijk is ook onze hybride protectie (cfr. Whitelisting) uniek in de anti-viruswereld wat een goede performantie oplevert voor onze pc. We willen toch allemaal een goede bescherming met een nog goed presterende computer? " □

COLUMN