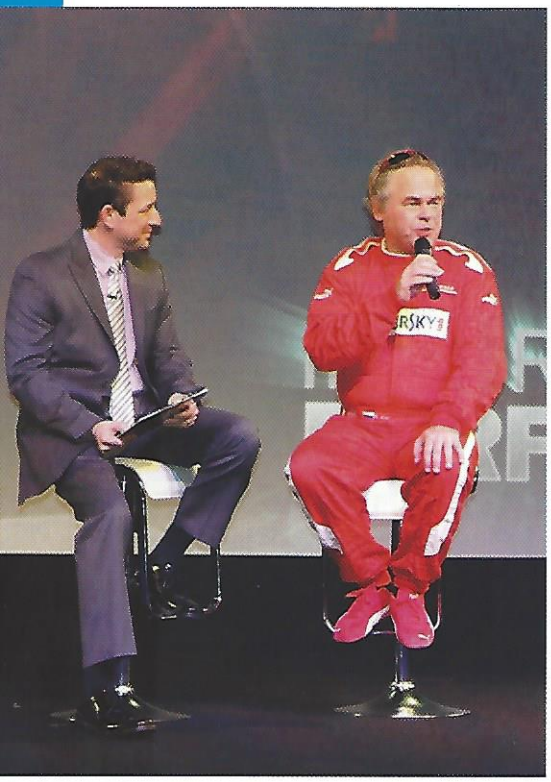
MARKT VOOR SECURITYOPLOSSINGEN WORDT VOOR RESELLER STEEDS LUCRATIEVER

Met Kaspersky in Dubai

Zowel de overheid als het bedrijfsleven moet dit jaar bedacht zijn voor toenemend cybergevaar. Dat was één van de boodschappen van Kaspersky tijdens haar partnerevent in Dubai. Tot zover het slechte nieuws. Het goede nieuws is dat niet alleen de cybercrimineel een steeds beter belegde boterham overhoudt aan beveiligingslekken, ook voor de reseller die zijn klanten moet helpen het gevaar te weren, zijn er mooie kansen weggelegd.



Eugene Kaspersky (rechts) kwam in Dubai op in het racepak van Ferrari, waarvan Kaspersky sponsor is.

TEKST: LAURENS VAN AGGELEN

De markt voor securitysoftware zal ook in 2012 voor nieuwe uitdagingen zorgen. Al was het alleen maar vanwege het grote aantal virussen (zo'n 70.000 nieuwe per dag) en de toename van phishing. IDC voorspelt dat in de IT security markt in 2014 maar liefst 38,4 miljard dollar om zal gaan. In het zonnige Dubai praatte Kaspersky zijn partners onlangs bij over nieuwe producten en vooral over het nieuwe partnerprogramma dat in de eerste twee maanden van 2012 uitgerold zal worden. "Het vorige partnerprogramma dateert van twee jaar geleden. Intussen hebben we veel feedback van onze partners gekregen dus er is alle reden om met een nieuw programma te komen", vertelt Martijn van Lom, managing director Kaspersky Lab Benelux.

Ondersteuning

Was het vorige partnerprogramma meer gericht op accreditatie, in de nieuwe opzet zal de focus meer liggen op prestaties en committent. Er komen bijvoorbeeld nieuwe certificeringen. Om de reseller te helpen, is er een speciale portal en consistente marketing en sales-tools. "We streven met het nieuwe partnerprogramma naar een intensievere samenwerking met onze partners", zegt Van Lom.
René Jansen, commercieel manager bij Datamex zegt goede ervaringen te hebben met de wijze waarop Kaspersky partner zoals hij ondersteunt. "Naast de producten en het vertrouwen in Kaspersky zijn het de leadgeneraties die het voor ons extra aantrekkelijk maken om zaken met hen te doen. Maar even-eens de manier waarop ze ons ondersteunen door snel opvolging te geven aan deals waar we mee bezig zijn zodat ons backoffice lekker loopt."

Bewustzijn

Terug naar de gevaren. Bij Kaspersky houdt men het voor zeer aannemelijk dat een breder scala aan organisaties slachtoffer zal worden van cyberaanvallen. "Momenteel doen de meeste incidenten zich voor bij bedrijven en overheidsinstellingen die betrokken zijn bij wapenontwikkeling, financiële operaties of hightech en wetenschappelijke onderzoek. In 2012 zullen daar bedrijven bijkomen die zich richten op het delven van natuurlijke bronnen, energie, transport, voeding en de farmaceutische industrie, maar ook internetdiensten en informatiebeveiligingsbedrijven", waarschuwt Alexander Gostev, auteur van het rapport 'Cyberthreat Forecast for 2012'. Aanvallen zullen volgens hem verspreid zijn over een groter deel van de wereld dan in het verleden het geval was. Naast West-Europa en de Verenigde Staten zullen ook Oost-Europa, het Midden-Oosten en Zuidoost-Azië doelwit zijn. Geen voorspelling om vrolijk van te worden. Cyberaanvallen zullen in de toekomst immers niet alleen een gevaar opleveren voor de bedrijfscontinuïteit, maar ze worden ook een direct gevaar voor het functioneren van voorzieningen waar we met z'n alleen niet buiten kunnen. Experts van Kaspersky Lab voorspellen dat aanvallers hun methodes moeten aanpassen om een antwoord te geven op de IT-beveiligingsbedrijven. De conventionele manier van kwaadaardige bijlagen toevoegen aan e-mails wordt

steeds minder effectief, aanvallen via de browser zullen in populariteit toenemen.
Voor resellers is het goed om te weten dat wereldwijd ongeveer 44 procent van de werknemers op de hoogte is van IT-bedreigingen die een impact kunnen hebben op hun werk, maar er zijn ook landen waar slechts één op de drie werknemers iets weet van potentiële bedreigingen. "Het creëren van meer bewustzijn, is dus een taak die de reseller in ieder geval voor zijn rekening zou moeten nemen", aldus Van Lom.

Smartphone

Zodra een apparaat iets met het IP-protocol van doen heeft, is het een interessant doelwit voor hackers. Zo viel ooit een insulinepomp ten prooi aan een aanval. De pomp die werd aangestuurd vanuit een WiFi-verbinding leverde daardoor een fatale dosis aan een patiënt. Dit voorbeeld kwam ter sprake in het interview dat we in Dubai hadden met Ryan Naraine, 'senior security evangelist' bij Kaspersky. "Gebruikers zijn zich meer bewust van de gevaren die zij lopen dan pakweg vijf jaar geleden, maar het web verandert snel en ook de gevaren nemen andere vormen aan. Daarbij worden ook de sociale netwerken steeds vaker misbruikt voor identiteitsdiefstal, een fenomeen dat zich moeilijk laat bestrijden", aldus Naraine. "Het gevaar is dat er bij diefstal ogenschijnlijk niets aan de hand lijkt. De gebruiker merkt immers niets, maar op termijn kunnen al die verzamelde gegevens wel tegen hem gebruikt worden."
Beveiligingssoftware kan, zo weet Naraine, niet voorkomen dat de gebruiker zelf uit onwetendheid of naïviteit bestanden opent of op links klikt waarmee hij het onheil tegemoet treedt. "De zogenaamde shortlinks die bijvoorbeeld op Twitter gebruikt worden om URL's in zo weinig mogelijk karakters weer te geven, zijn een stap terug. Wie er op klikt heeft geen idee waar hij terecht zal komen."
Naraine adviseert om telebankieren niet via een smartphone te doen. "Het meest veilige is daarvoor een aparte pc te gebruiken. Werken in de cloud mag dan misschien veiliger lijken omdat gegevens dan niet lokaal bij de gebruiker opgeslagen zijn, volgens Naraine is het vooral vanuit het beheersperspectief misschien veiliger, maar de gebruiker geeft daarmee wel het risico niet meer in eigen hand."

Mobiel

Als het gaat om mobiele dreigingen ziet Naraine vooral Android, het meest gebruikte mobiele besturingssysteem ter wereld, als het favoriete doel van de mobiele malware-markt. Ook verwacht hij de opkomst van de eerste mobiele 'drive-by'-aanvallen en mobiele botnets. "Mobiele spionage gaat zich verder uitbreiden en resulteert in datadiefstal van mobiele telefoons en het volgen van mensen via hun telefoons en geo-locatiediensten."
Kaspersky heeft als remedie Endpoint Security 8 for Smartphone op de markt gebracht om smartphones te beveiligen tegen diefstal, onrechtmatige toegang tot data, verlies en mobiele malware. Deze software is ontwikkeld om bedrijven een oplossing te bieden voor de beveiliging van mobiele apparaten van medewerkers in geval van verlies of diefstal. De software bevat verschillende anti-diefstalfuncties. Zo kan het apparaat met behulp van GPS gelokaliseerd worden en kan data op afstand versleuteld, gewist of geblokkeerd worden. Ook worden smartphones beschermd tegen SMS-spam, malware en andere aanvallen via internet.