SECURITY IS EEN NOODZAAK, GOEDE IMPLEMENTATIE OOK

'Beter voorkomen dan genezen', klinkt het in de volksmond. We vinden het normaal om problemen te voorkomen en ons in te dekken voor als het toch misgaat. Neem nu uw wagen: u kiest een betrouwbare dealer en laat de wagen regelmatig onderhouden. U neemt er ook pechverhelping en een, weliswaar verplichte, verzekering bij. Allemaal logisch, toch? Voor IT-security blijkt die logica vaak niet op te gaan. We peilden bij diverse partijen naar tendensen en bijhorende kansen voor de reseller. ••• Wim Feyaerts

Wie zich niet bewust is van een potentieel gevaar, kan er zich ook niet druk om maken. Onze gesprekspartners beamen dat de Belgische KMO de veiligheidsrisico's vaak onvoldoende kent. "In bedrijven die IT beschouwen als een onderdeel van de bedrijfsvoering, zien we wel een sterker bewustzijn." stelt Patrick Casteels van Kappa Data. "In de kleinste KMO's daarentegen heerst nog vaak het motto 'zolang het maar werkt'." voegt Jean Loyens, CEO van distributeur Cherub, toe. "Men is zich redelijk bewust van de gevaren, maar security staat ver op de prioriteitenlijst zolang er geen echt probleem is." aldus Bram De Blander, presales & network security engineer bij Panda Security.

Mike Veeckmans, zaakvoerder van reseller Spizzy, ervaart dat heel wat klanten al wel beveiligingssoftware geïnstalleerd hebben. "Maar nader bekeken, gaat het dan om verouderde antivirussoftware, of een firewall die je binnen de kortste keren omzeilt. Wijs je de mensen op het gevaar, dan stoot je vaak op een 'dat zal ons niet overkomen'-attitude."

Volgens Eddy Willems, IT Security Evangelist bij Kaspersky en director bij EICAR, is de situatie zelfs slechter dan enkele jaren geleden: "Toen was er nog veel aandacht voor grote uitbraken, zoals die van het Iloveyou-virus, terwijl er tegenwoordig amper nog media-aandacht naar gaat."

Meer en andere malware

Het malware-landschap verschilt sterk met enkele jaren geleden. Om te beginnen is het aantal bedreigingen van een heel andere orde. Patrick Dalvinck, Benelux Regional Director van Trend Micro, haalt er cijfers bij: "Vroeger sprak je over een paar honderd of een paar duizend nieuwe bedreigingen per jaar. Nu halen we die aantallen per uur. De viruscollectie van AV-Test.org telde begin dit jaar al 5,5 miljoen bedreigingen." Eddy Willems bevestigt: "We voorspellen dat er tegen eind dit jaar 20 miljoen bedreigingen zullen zijn. Waanzinnig."

Jan Guldentops van reseller/consultant BA vindt een verklaring in het feit dat hackers over veel betere middelen beschikken om de zaken grootscheeps aan te pakken, zoals krachtige computers en tools en steeds meer breedbandconnecties. "Kijk maar eens naar het spamvolume. Wij beheren setups waar minder dan 5% van de binnenkomende e-mails nuttig is."

"We zien ook een verkorting van de levensduur van een aanval." vervolgt Patrick Casteels. Vroeger had een hacker of spammer dagen of weken nodig om alles uit te sturen. Vandaag gebeurt dat binnen een paar uur. De beveiligingssoftware moet dus razendsnel geüpdatet worden."

Hebben de mediagenieke Iloveyou's en Kournikova's ook plaats gemaakt voor andere types van bedreigingen? Eddy Willems somt op: "We zien vooral diverse vormen van trojans, doelgerichte aanvallen, rootkits en bedreigingen via webpagina's opduiken." "Een groot verschil is dat het nu gaat om echte criminelen, die uit zijn op je geld. Verder zie ik diefstal van identiteitsgegevens als de grootste bedreiging." stelt Jean Loyens. "Malware gaat tegenwoordig ook discreet te werk, zonder dat de gebruiker het merkt."

Naast de diverse externe bedreigingen, wijzen meerdere gesprekspartners op het toenemende gevaar van risico's van binnenuit: Confidentiële gegevens die het bedrijf verlaten op usb-sticks of dvd's, werknemers die malafide software installeren, of het vrijgeven van persoonlijke gegevens op online community's. "Het kan gaan om bewuste acties – wrevel bij werknemers kun je niet uitsluiten – maar vaak

***Patrick Casteels** van Kappa Data: "Vroeger had een hacker of spammer dagen of weken nodig om alles uit te sturen. Vandaag gebeurt dat binnen een paar uur. De beveiligingssoftware moet dus razendsnel geüpdatet worden."*

is het gewoon een kwestie van ontbrekende kennis." analyseert Mike Veeckmans.
Jan Guldentops relativeert de litanie van bedreigingen dan weer een beetje: "De security-industrie lanceert om de zoveel tijd een nieuwe term. Maar het gaat in security niet om aparte problemen, maar om het totaalplaatje. De keten is maar zo sterk als de zwakste schakel."

Nieuwe remedies

Om het toenemende aantal bedreigingen het hoofd te bieden ziet Patrick Dalvinck vooral heil in een "in-the-cloud"-model waarbij de meeste bedreigingen al in een datacenter onderschept worden voor ze de gebruiker bereiken. "Het traditionele updaten van virusdefinities op de pc van de gebruiker is niet meer haalbaar. Dat model vergt te veel resources en moeite van de gebruiker."
"In-the-cloud"-protectie hoort ook bij de nieuwe technieken die Eddy Willems noemt. Hij heeft het ook over ingebouwde anti-rootkit-technologie, whitelisting en intrusion protection die volwassener geworden zijn.
"De vroegere antivirusprogramma's hebben plaats gemaakt voor ruimere beveiligingssuites." stelt Jean Loyens. Hij ziet werkgevers, onder impuls van de resellers, ook vaker beperkingen opleggen aan hun personeel: filters voor bepaalde sites, beperkte netwerktoegang, geen usb zonder toestemming, enzovoort.
Patrick Casteels beaamt dat: "Er is een duidelijke opkomst van 'user centric' beveiliging: authentificatie van gebruikers en toestellen op het netwerk. Daarnaast zien we een zeer sterke evolutie op het vlak van webbeveiliging. Webpagina's kunnen immers gebruikt worden voor professionele applicaties, maar ook voor gevaarlijke of nutteloze toepassingen. Degelijke intrusion prevention systems geraken dus steeds meer in trek."
Biometrische beveiliging ten slotte kan bij de verschillende gesprekspartners op wat scepsis rekenen of wordt omschreven als "interessant voor bepaalde niches". Mike Veeckmans past het wel al regelmatig toe, bijvoorbeeld bij klanten met medewerkers in de buitendienst, en heeft goede ervaringen.

100% veilig?

Hierover zijn onze securityspecialisten unaniem: 100% veiligheid bestaat niet. "Er is immers altijd nog de zwakke menselijke schakel." verklaart Bram De Blander. "Bovendien staan de ontwikkelingen bij hackers ook niet stil. Er is immers te veel geld mee gemoeid." vult Eddy Willems aan.
Natuurlijk mag dit niet tot berusting leiden: "Je kunt het risico wel enorm inperken door beveiliging in te bouwen op diverse niveaus en door een partner te kiezen die bij nieuwe bedreigingen snel genoeg reageert." zegt Patrick Dalvinck.

"De bedrijven zijn zich redelijk bewust van de gevaren, maar toch staat beveiliging ver op de prioriteitenlijst zolang er zich geen problemen voordoen."

Patrick Casteels maakt ook de link met het kostenplaatje: "Zoals vaak is het een kwestie van afwegen in wat je wilt investeren. De eerste 80% van de beveiliging kan vrij vlot en relatief goedkoop. Meer en meer bedrijven doen nu inspanningen om tot ongeveer 95% te komen. De laatste procenten zijn alleen nuttig voor bedrijven die over zeer confidentiële gegevens beschikken."

***Bram De Blander**, presales & network security engineer bij Panda Security: "De reseller kan de installatie, de configuratie en het beheer van de beveiliging volledig op afstand uitvoeren, in combinatie met SLA's. Dat biedt vele kansen om marge te halen."*

***Jean Loyens**, CEO van distributeur Cherub: "De klant mag niet te afhankelijk zijn van de reseller. Een goede reseller zou daarom zijn klant bijvoorbeeld een gesloten omslag met het hele beveiligingsplan moeten geven, inclusief codes. Dat geeft vertrouwen."*

Security als service

"Anti-malware-oplossingen zijn bij uitstek geschikt om een dienst mee op te zetten", stelt Bram De Blander. "De reseller kan bijvoorbeeld de installatie, de configuratie en het beheer volledig op afstand uitvoeren, in combinatie met SLA's. Dat biedt vele kansen om marge te halen."
"Het is voor een KMO onmogelijk om alle kennis zelf in huis te halen en het dagelijks beheer te verzorgen. Zeker in de KMO-markt zijn managed services dus de oplossing om een zeker niveau van veiligheid te bereiken", zegt Jan Guldentops. Hij benadrukt wel de nood aan controlemechanismen voor de klant, zoals rapporten of zelfs een neutrale audit. Dat vindt ook Jean Loyens: "Voor een klant is er het risico van een te grote afhankelijkheid van de externe partner. Een goede reseller zou dus zijn klant moeten voorzien van bijvoorbeeld een gesloten omslag met het hele beveiligingsplan, inclusief codes. Dat geeft vertrouwen."
Ook Patrick Dalvinck ziet kansen in gehoste diensten, die zelfs voor consumenten hun nut kunnen hebben, zoals "in-the-cloud" checken van e-mail en webverkeer. Toch lijkt voor hem en Eddy Willems een compleet gehoste beveiliging nog niet direct iets voor morgen. "Je zult toch nog altijd iets lokaal op je pc of ander toestel moeten installeren, ook al kan dat iets klein zijn." Ook voor Patrick Casteels zijn

***Eddy Willems**, IT Security Evangelist bij Kaspersky en director bij EICAR: "Prestaties zijn voor de klant zeer belangrijk, beveiliging mag het systeem niet te veel vertragen. Let ook op de mogelijkheden voor rapporten en statistieken, zodat u uw klant kunt informeren over wat er gebeurt."*

er nog obstakels: "SaaS-modellen werken, maar voor veel takken van security is dit moeilijker omdat ze diep in de netwerkarchitectuur genesteld zitten. Een Intrusion Protection System dat een aantal lokale servers afschermt van de rest van het netwerk kan bijvoorbeeld moeilijk uitbesteed worden."

Ook hardware?

Voor kleine KMO's is het vaak aangewezen een 'zorgenvrije' hosted oplossing te bieden. Maar toch vindt zowat iedereen dat de reseller ook de verkoop van hardware kan betrekken in het security-verhaal, tenminste vanaf een bepaalde omvang en afhankelijk van de noden van de klant. "Vaak is de beste keuze een mix van hardware en software." zijn Jean Loyens en Bram De Blander het roerend eens.

"Er is een duidelijke tendens naar appliances. Dat is zeker zinvol. In het algemeen zijn ze sneller te implementeren en ligt de performantie een stuk hoger." zegt Patrick Casteels. Ook Jan Guldentops ziet de voordelen: "Je weet dat de hardware 100% is afgestemd op de software en dat er tijdens de installatie geen fouten zijn opgedoken. Het is ook makkelijk: de oplossing is kant-en-klaar en de reseller weet precies wat hij moet ondersteunen."

Welke vendor kiezen?

Echt slechte pakketten zijn er niet meer, horen we verschillende partijen zeggen. Maar hoe kiest u dan als reseller met welke vendor(s) u in zee gaat? Mike Veeckmans: "Let uiteraard op kwaliteit, maar vergeet ook niet dat de prijs zeer belangrijk is voor KMO's. Check of het product configureerbaar is, of er cursussen zijn voor de reseller en of het gebruiksvriendelijk is voor de eindgebruiker."

"Prestaties zijn voor de klant zeer belangrijk, beveiliging mag het systeem niet te veel vertragen. Let ook op de mogelijkheden voor rapporten en statistieken, zodat u uw klant kunt informeren over wat er gebeurt." voegt Eddy Willems toe. Support in de lokale taal, een compleet assortiment (software, hosted, appliances) en meedenken en begeleiden bij het opzetten van managed services, zijn argumenten die Bram De Blander naar voren schuift.

"Het hoeven niet altijd de meest bekende pakketten te zijn. Vertrouw op onafhankelijke barometers, zoals Virus Bulletin, als u echt eerlijk wilt vergelijken. Kies een leverancier die u als reseller goede voorwaarden biedt, zoals terugkerende commissies op verlengingen." adviseert Jean Loyens.

Belangrijke manieren om zich te onderscheiden zijn voor Patrick Dalvinck de beheersmogelijkheden voor de reseller: "Als de reseller steeds voor alles ter plaatse moet gaan bij klanten, botst hij al snel op zijn limieten. Kies dus een product dat vanop afstand kan geüpdatet en beheerd worden."

"Wat een goede oplossing onderscheidt van een minder goede heeft niet zozeer met de keuze van het product, maar vooral met de kennis en implementatie te maken."

Voor Patrick Casteels ligt het zwaartepunt van de kwaliteit trouwens bij de reseller zelf: "Wat een goede oplossing onderscheidt van een minder goede heeft niet zozeer met de keuze van het product, maar vooral met de kennis en implementatie te maken."

***Mike Veeckmans**, zaakvoerder van Spizzy: "Security zou voor KMO's verplicht moeten zijn. Van zodra er iets of wat gevoelige informatie op je netwerk staat, is het immers pure noodzaak."*

***Patrick Dalvinck**, Benelux Regional Director van Trend Micro: "Als de reseller steeds voor alles ter plaatse moet gaan bij klanten, botst hij al snel op zijn limieten. Kies dus een product dat vanop afstand kan geüpdatet en beheerd worden."*

Free lunch?

Hoe gaat u als reseller om met gratis software? Valt daar een strategie rond te bouwen? Open source is voor Jan Guldentops alvast een valabele piste. "Daar zitten programma's bij van buitengewone kwaliteit en wij brengen die als consultant samen tot één totaalproduct annex service. Hou er wel rekening mee dat u dan als reseller zelf de klant technisch moet ondersteunen en daarin dus moet investeren."

De andere gesprekspartners denken eerder aan de gratis antiviruspakketten die te downloaden zijn. "Scannen op virussen kunnen ze inderdaad," zegt Patrick Dalvinck, "maar security is meer dan dat." Bij Patrick Casteels klinkt het twijfelachtiger: "Hoe zit het support-verhaal ineen, welke garanties voor continuïteit zijn er, zal het product technologisch bijblijven, zal het gratis blijven? Dat zijn belangrijke vragen die onbeantwoord blijven bij gratis pakketten."

"Als de klant ernaar vraagt, tonen wij meestal een tabel die het verschil in reactiesnelheid toont." klinkt het schamper bij Mike Veeckmans. "Bij gratis is er altijd een addertje." zegt Eddy Willems, "Zit het niet in de engine, dan wel in het updaten." Diverse vendors verwijzen ook naar de enorme bedragen die ze in R&D investeren. "Gratis pakketten hebben niet die fondsen en kunnen dus niet op dezelfde manier evolueren. Vaak detecteren ze met achterhaalde technologie", luidt het oordeel van Bram De Blander.

Voor een uitgebreide vergelijkende test van de belangrijkste beveiligingspakketten, verwijzen we onze lezers graag naar PC Magazine nr. 119, dat vanaf 18 november in de winkels ligt.

MEER OMZET HALEN UIT SECURITY

TIP 1 Maak de klant bewust

Informeer de klant over de gevaren en de mogelijke gevolgen: als hij het probleem niet kent, zal hij ook geen oplossing zoeken. Informeren betekent echter niet bang maken. Schets wat de gevaren zijn, maar pols ook naar de situatie en de behoeften van de klant. Toon concreet aan dat ook in zijn geval zaken als gegevensverlies of identiteitsdiefstal erg vervelend zouden zijn.

Leg de link naar herkenbare, dagdagelijkse zaken: een auto onderhoud je ook preventief, een huis verzeker je ook tegen brand, 'voor het geval dat'.

Denk aan de verzekeringssector: een verzekeringsagent moet in een commercieel gesprek aantonen wat de mogelijke risico's zijn, wat de gevolgen kunnen zijn en hoe de klant zich daartegen kan indekken. Voor security is dat niet anders.

TIP 2 Trek de vraag open

Komt de klant met een specifieke nood, toon dan het ruimere plaatje. Vraagt hij bijvoorbeeld anti-spam, wijs dan op andere aspecten: beveiliging tegen andere e-mailbedreigingen, scannen van uitgaand verkeer, ... Vaak heeft de klant dat ook nodig, maar had hij er nog niet aan gedacht. Voor bedrijfsklanten kunt u zo een project als het ware naar u toe trekken, met als gevolg dat het geen prijzenslag wordt. Echter niet overdrijven: met eerlijke argumenten en een aanbod op maat van de klant, kunt u het verst.

TIP 3 Overtuig met een demo

Overtuig de klant door een testconfiguratie te plaatsen. Laat die alles registreren en leg de prospect een rapport voor van alles wat er binnen- en buitengaat. Negen op tien keer trekt u hem zo over de streep. Wel opletten dat u kort op de bal speelt: laat geen vijf weken voorbijgaan voor u de klant confronteert met het rapport. Dit vraagt een kleine investering in enkele hardware firewalls, maar dat verdient u snel terug. Misschien valt er met je distributeur wel een deal te maken dat u die apparaten in consignatie krijgt.

TIP 4 Volg renewals op

Houd een historiek bij van de licenties die op vervallen staan. Biedt uw vendor of distributeur u deze dienst niet, laat dan niet na om het zelf te doen. Wist u dat het aantal renewals, zeker voor pakketten die men ook elders kan kopen, kan vervierdubbelen als u dit goed opvolgt?

TIP 5 Bied dienst na verkoop

Bedrijfssecurity stopt niet bij de verkoop; het draait ook om service daarna: updates, controles, enzovoort. Security die niet onderhouden wordt, is snel verouderd. Kies voor bedrijfsklanten wel liefst een oplossing die u (deels) remote kunt beheren en updaten. Op die manier kunt u met dezelfde personeelsbezetting veel meer klanten bedienen.

TIP 6 Doe audits

Voer bij uw klant regelmatig een controle of audit uit. Enerzijds herinnert u de klant zo aan het nut van je oplossing en bewijst u uw meerwaarde. Anderzijds kan het kansen blootleggen om bijkomende oplossingen of diensten te bieden (cross- en upselling). Wijs ook op de interne beveiliging: een kassabediende hoeft niet aan de boekhouding te kunnen.

TIP 7 Benut managed services

Een gehoste oplossing is perfect voor een kleine KMO. Het is een ideale manier om een langdurige klantrelatie op te bouwen en een mooie, weerkerende marge te realiseren. Soms krijgt u te maken met klanten die angstig zijn om zaken uit handen te geven ("Kunt u dan mijn mails lezen?"). Ook hier kan wat educatie op zijn plaats zijn.

TIP 8 Ken uw product

Ga niet voor een eindeloos gamma aan concurrerende producten. Voer liever een beperkter aanbod, bouw een relatie op met de vendor en ken uw producten – dat schept ook vertrouwen bij de klant. Security kan zorgen voor goede marges en een langdurige inkomensstroom, maar als reseller moet u wel de nodige kennis verwerven om daarin te slagen.