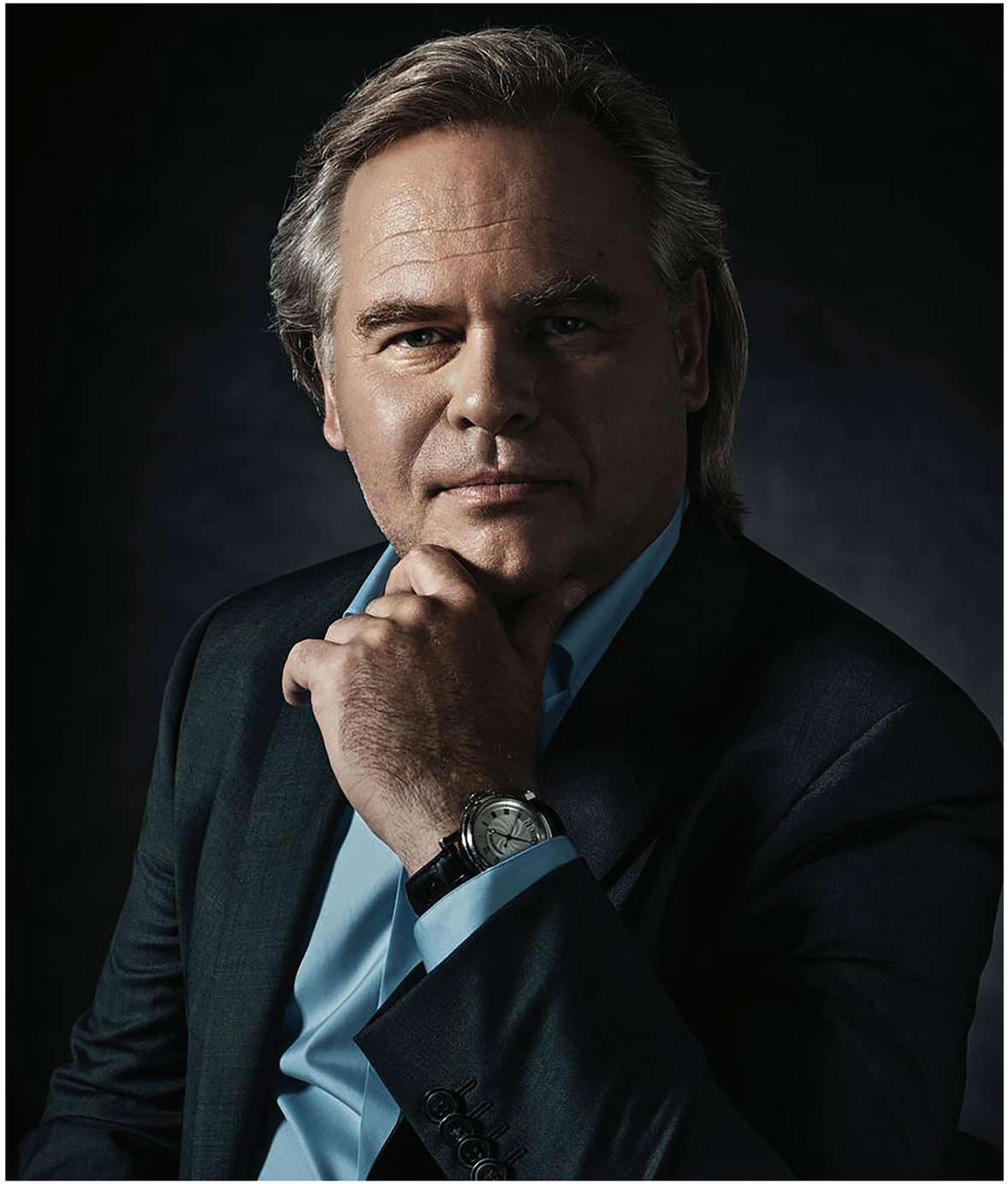
WERELDWIJDE
BEVEILIGINGSINTELLIGENTIE

DE BEVEILIGDE ONDERNEMING

#EnterpriseSec
kaspersky.com/enterprise



Eugene Kaspersky
Hoofd en CEO, Kaspersky Lab

Vandaag beschermen is de toekomst veiligstellen

Elke dag gebruiken en delen miljoenen mensen online informatie. Er worden voortdurend over de hele wereld gegevens verstuurd tussen bedrijven, werknemers, klanten en leveranciers.

Al deze connectiviteit brengt enorme commerciële voordelen met zich mee, maar vormt ook een aanzienlijk en steeds hoger risico voor de beveiliging. Er komen dagelijks nieuwe cyberdreigingen bij – dreigingen die een verwoestende invloed op ons als individuen, bedrijven en de maatschappij kunnen hebben.

Ik werk al jaren nauw samen met overheden en wetshandhavers over de hele wereld om te adviseren over de gevaren waarmee we te maken hebben en het cruciale belang van cyberbeveiliging. Helaas worden de dreigingen steeds geavanceerder. De termen cyberoorlog en cyberterrorisme staan tegenwoordig dan ook hoog op de agenda van onze wereldleiders. Het is nu tijd voor ondernemingen om hun IT-beveiligingsstrategieën aan te scherpen zodat ze de problemen van de hedendaagse omgeving het hoofd kunnen bieden.

Wij van Kaspersky Lab vinden het niet voldoende alleen te reageren op nieuwe bedreigingen als ze zich voordoen. Om die reden investeren we veel mankracht en tijd in ons toonaangevend onderzoek van dreigingen. We stoppen nooit met het anticiperen op en voorkomen van IT-beveiligingsdreigingen en onze technologieën zijn ontworpen om gebruik te maken van onze uitgebreide wereldwijde beveiligingsintelligentie. De benadering van Kaspersky Lab is eenvoudig: betere intelligentie gecombineerd met betere technologie leidt tot betere bescherming.

Het is onze missie de voordelen van deze beveiliging wereldwijd aan ondernemingen aan te bieden om ze zo te helpen bij de verdediging tegen alle soorten cyberdreigingen – nu en in de onzekere toekomst.

"Wij staan altijd klaar om cybercriminaliteit te bestrijden, ongeacht oorsprong, doel of raffinement. Wij bieden uiterst effectieve oplossingen, doordat wij bewezen technologische ontwikkelingen paren aan diepgaand onderzoek van dreigingen – een combinatie die resultaten oplevert die door geen enkele andere IT-beveiligingsorganisatie worden geëvenaard."

Nikita Shvetsov,
Acting Chief Technology Officer,
Kaspersky Lab

Malware treft iedereen – van individuen tot grote ondernemingen en overheidsinstanties. Cybercriminelen gebruiken steeds geavanceerdere wapens om bedrijven op te lichten, gegevens te stelen en financieel gewin te behalen. Een groeiend aantal cyberaanvallen is politiek of sociaal gemotiveerd – cyberterrorisme en cyberoorlog zijn nu realiteit.

Internationale organisaties zijn slachtoffer van gerichte aanvallen, zogenaamde 'advanced persistent threats' (APT's), van bepaalde groepen criminelen. Sommige van deze groepen zijn bekend en krijgen veel aandacht, maar de trend is dat aanvallers steeds beter maskerende technieken gebruiken om anoniem te blijven wanneer ze toegang tot vertrouwelijke en vaak commercieel waardevolle gegevens krijgen.

ONZE FOCUS EN STRATEGIE

De strategie en R&D van Kaspersky Lab zijn gericht op mogelijke nieuwe dreigingen en op plaatsen waar organisaties het kwetsbaarst zijn. Bij onze inspanningen in het verleden en expertise zijn wij er altijd op gericht geweest endpoints te beschermen en de hedendaagse endpoints zijn gevarieerder en kwetsbaarder dan ooit. Endpoints kunnen vandaag de dag mobiel of virtueel zijn, en kunnen zelfs een essentiële nationale infrastructuur vormen.

Deze gebieden worden door IT-beveiligingsproducten bijna het slechtst bediend. Ons doel is grote organisaties helpen zichzelf op deze kwetsbare gebieden te beschermen met een nieuwe benadering – een benadering waarbij ze gebruikmaken van onze geavanceerde dreigingsintelligentie om een betere bescherming te realiseren.

TECHNOLOGISCH LEIDERSCHAP VAN KASPERSKY LAB

Hoewel deze dreigingen een apart fenomeen zijn, kunnen ze niet als geïsoleerde problemen worden beschouwd. Ze maken samen deel uit van een groter beveiligingslandschap en kunnen alleen effectief worden bestreden door ze allemaal te begrijpen.

De wereld heeft beveiligingsoplossingen nodig die zijn gebaseerd op uitgebreide en voorspellende beveiligingsintelligentie – geen aanbod dat voor slechts één doel is ontwikkeld en een beperkt doel dient. En het is onze overtuiging dat het ontwikkelen van dergelijke oplossingen het breedst mogelijke perspectief vereist.

Dit principe is de leidraad voor onze technologiestrategie en resulteert in organisch gebouwde, geïntegreerde oplossingen die superieure bescherming en betere prestaties bieden. Ook nu geldt weer: betere intelligentie gecombineerd met betere technologie betekent betere bescherming.

Eén basisonderdeel van onze beveiligingsintelligentie is het Kaspersky Security Network (KSN). Het ontvangt uit alle hoeken van de wereld enorme hoeveelheden cyberdreigingsgegevens over allerlei soorten opkomende malware. Samen met de analyses van ons wereldbefaamde Global Research and Analysis Team (GReAT) stelt dit Kaspersky Lab in de unieke gelegenheid oplossingen te leveren die niet alleen actuele dreigingen onschadelijk maken, maar waarmee u ook voorbereid bent op toekomstige gevaren.

HET KASPERSKY SECURITY NETWORK

- Een complexe, gedistribueerde infrastructuur die speciaal bestemd is om gedepersonaliseerde gegevensstromen met betrekking tot cyberbeveiliging van miljoenen vrijwillige deelnemers overal ter wereld te verwerken
- Ongeveer 60 miljoen vrijwillige deelnemers
- 600.000 gegevensaanvragen per seconde
- Gemiddelde reactietijd bij een aanvraag: 0,02 seconde

FRAUDEPREVENTIE

Online en mobiel bankieren – alle risico's zijn gedekt

Elk jaar worden er honderden miljoenen dollars van online financiële serviceproviders gestolen en deze dreiging neemt nog steeds toe. Goed georganiseerde cybercriminelen richten zich nu twee keer vaker op banken dan op andere soorten instellingen[1].

Maar het aantal aanvallen vormt nog maar de helft van het probleem, omdat veranderingen in het gedrag van klanten banken kwetsbaarder maken dan ooit.

98% van de consumenten gebruikt regelmatig online bankservices of winkelt online[2]

Tegenwoordig bankiert of winkelt het overgrote deel van de internetgebruikers regelmatig online[2], maar men is zich vaak niet bewust van het risico dat ze nemen als ze hun account vanaf niet-beveiligde apparaten gebruiken. Vooral mobiele telefoons zijn kwetsbaar. En aangezien steeds meer consumenten hun mobiel gebruiken om te internetbankieren, zijn criminelen volop bezig specifieke methoden te ontwikkelen om deze waardevolle doelen te exploiteren.

De dreigingen waarmee klanten zich geconfronteerd zien, zijn echt, en als klanten niet goed beveiligd zijn, is ook de bank niet goed beveiligd.

Financiële instellingen kunnen met het Kaspersky Fraud Prevention-platform uitgebreide beveiliging voor hun kernactiviteiten en hun klanten leveren. Kaspersky Fraud Prevention kan banken zelfs helpen de mobiele applicaties van hun klanten veiliger te maken om te strijden tegen het groeiende aantal cyberdreigingen dat zich op mobiele apparaten richt. En onze intelligentie verzekert klanten van optimale effectiviteit van de beveiliging, doordat zelfs bij een veranderend landschap de reacties effectief en relevant blijven.

[1] Global Economic Crime Survey 2014, PricewaterhouseCoopers
[2] Consumer Security Risk Survey 2013, B2B International in samenwerking met Kaspersky Lab

[1] Cyberthreats to ICS systems: you don't have to be a target to become a victim. Industrial Security 2014, Kaspersky Lab

35% van de incidenten in industriële netwerken wordt veroorzaakt door malwareaanvallen[1]

Er was een tijd dat industriële beheersystemen standalone waren en dat operators dachten dat ze hun infrastructuur veilig konden houden. In werkelijkheid is isolatie nooit voldoende geweest om veiligheid te garanderen. Zoals recente belangrijke cases hebben aangetoond, kunnen aanvallen overal vandaan komen en kan zelfs de controle over een nucleaire faciliteit worden overgenomen door malware die via een USB-poort is binnengekomen.

Tegenwoordig worden deze systemen door de behoefte aan internet aan veel nieuwe vulnerability's blootgesteld – en als een netwerk door malware is besmet, kunnen de gevolgen catastrofaal zijn.

Hoewel de meest geavanceerde cyberwapens voor specifieke doelen zijn ontwikkeld, kunnen ze bij gebruik in handen vallen van anderen met vijandelijke bedoelingen en kunnen ze voor nieuwe doelen worden ingezet. Dit betekent dat voor alle kritieke infrastructuur het hoogste beveiligingsniveau nodig is.

Kaspersky Lab heeft als leider in de strijd tegen cybercriminaliteit ongeëvenaard inzicht in de dreigingen waarmee de wereld zich geconfronteerd ziet, evenals de deskundigheid om deze dreigingen onschadelijk te maken.
Samen met overheidsinstellingen en de private sector helpen wij de meerlaagse beveiliging te creëren die nodig is om kritieke infrastructuren en de mensen die hiervan afhankelijk zijn te beschermen. We beseffen dat er voor kritieke infrastructuren een ander beveiligingsniveau nodig is: beveiliging die in hoge mate configureerbaar is en speciaal voor een bepaald doel is ontworpen.

Aangezien in industriële netwerken procesintegriteit een hogere prioriteit heeft dan gegevensintegriteit, biedt Kaspersky Lab een speciale maatwerkversie van het beveiligingspakket voor bedrijven. Ook vervult Kaspersky Lab een leidende rol in de branche bij het ontwikkelen van technologieën voor beveiligde infrastructuren, betere bescherming voor PLC's en beter geïntegreerde SCADA-beschermingslagen.

Gartner voorspelt voor 2014 een groei van 12,14% op de internationale bedrijfsmarkt voor virtualisatie-infrastructuursoftware[1]

Virtualisatie heeft grote, complexe IT-omgevingen compleet veranderd en bedrijven en hun werknemers grote voordelen opgeleverd.

Maar omdat organisaties wereldwijd steeds meer met cyberdreigingen worden geconfronteerd, is het van groot belang dat hun virtuele omgevingen net zo compleet en effectief worden beveiligd als hun fysieke IT-infrastructuur. En nu veel organisaties hun kritieke systemen en gegevens virtualiseren, staat er nog veel meer op het spel.

Door beveiligingsfunctionaliteit aan een IT-systeem – fysiek of virtueel – toe te voegen wordt er in een bepaalde mate gebruikgemaakt van systeembronnen. Wij streven er dus altijd naar de beveiliging te optimaliseren en tegelijkertijd de impact op systeembronnen tot een minimum terug te brengen.

Dit is vooral belangrijk bij virtuele infrastructuren, aangezien efficiënt gebruik van systeembronnen de voornaamste reden is om de technologie te implementeren. Tenzij er een goede balans tussen beveiliging en efficiëntie van de systemen wordt gevonden, kunnen de voordelen van virtualisatie geheel teniet worden gedaan.

De ideale beveiligingsoplossing moet de eigenschappen van virtualisatie zelf weerspiegelen. De oplossing moet flexibel en aanpasbaar zijn en moet een aanzienlijk continu investeringsrendement kunnen leveren door de ideale balans van beveiliging en prestaties – dit is precies wat Kaspersky Security for Virtualization biedt. Bedrijven worden tegenwoordig niet meer gedwongen tot een compromis tussen efficiëntie van systeembronnen en beveiligingsniveau. Bij Kaspersky krijgt u beide in gelijke mate.

[1] Forecast: Enterprise Software Markets, Worldwide, 2010 – 2017, Q413 Update – Gartner

MOBIEL
Een mobiele infrastructuur beheren

Met de opkomst van flexibel werken en het BYOD-beleid (Bring Your Own Device) heeft elke onderneming beveiliging tegen cyberdreigingen nodig, ongeacht waar werknemers naartoe gaan en welke hardware ze gebruiken. Dit betekent dat traditionele beveiligingsmaatregelen gewoon niet voldoende zijn om bedrijfsgegevens onderweg te beschermen.

De hoeveelheid malware die zich specifiek op mobiele apparaten richt, groeit exponentieel. Zelfs een eenmalige inbreuk op één telefoon, tablet of laptop kan de beveiliging van een geheel bedrijfsnetwerk in gevaar brengen. Ongeacht of dit het gevolg is van een drive-by-aanval van een besmette webpagina die door een gebruiker is bezocht, een schadelijke app die is gedownload of gewoon diefstal van het apparaat, de schade kan enorm zijn.

Beveiliging wordt niet alleen een uitdaging door de mobiliteit maar ook door de wildgroei aan soorten apparaten en de draagbaarheid van hardware, waardoor de zichtbaarheid en het beheer van bedrijfsinformatie een hele opgave worden.

Kaspersky Security for Mobile is een product dat al ruim 10 jaar bescherming tegen mobiele malware biedt. Het product kan heel goed worden aangepast om bedrijfsnetwerken te beschermen tegen de dreigingen die inherent zijn aan een mobiele infrastructuur.

Het belangrijkste hierbij is dat ondernemingen met de beheerconsole van Kaspersky hun gegevens op alle endpoints kunnen zien, beheren en beveiligen - vanaf één centrale plaats. De onderneming is dus altijd goed beveiligd, ongeacht hoe mobiel de gegevens zijn.

In 2013 kreeg 18% van de bedrijven te maken met gegevenslekken via mobiele apparaten en werd bij 30% de beveiliging in gevaar gebracht door verlies of diefstal van apparaten[1]

[1] Global Corporate IT Security Risks – Kaspersky Lab
[2] Mobile Malware Evolution: 2013 – Kaspersky Lab, mei 2013

Aangezien aanvallen steeds geavanceerder en ongrijpbaarder worden, voldoen de gewone firewalls en anti-virustechnologie niet meer. Er zijn veel krachtiger tools nodig.

[1] Kaspersky Security Bulletin 2013

IT-afdelingen van grote organisaties hebben te maken met twee gelijk opgaande uitdagingen: toename van complexiteit en dreigingen die steeds geavanceerder worden. Hun werk wordt bovendien complexer doordat het personeel elke dag met een enorme diversiteit aan applicaties en apparaten werkt, en doordat steeds meer werknemers zaken doen via het web en op social media-platformen.

Voor de hedendaagse ondernemingen is uitgebreide en exact beheerde IT-beveiliging meer dan ooit een vereiste. Kaspersky Lab's technologie voor endpointbeheer levert dit en vormt een fundamenteel onderdeel van onze technologiestrategie. Onze beveiligingsoplossingen voor het bedrijfsleven bevatten krachtige beheerfuncties, waaronder dynamische whitelists om applicaties te verifiëren en gegevens en apparaten tegen schadelijke code, applicaties en websites te beveiligen. En we ontvangen continu wereldwijde dreigingsintelligentie om nieuwe en toekomstige dreigingen voor te blijven, terwijl we via het cloudgebaseerde Kaspersky Security Network automatische updates bieden.

Wat heel bijzonder is, is dat deze technologie op één geïntegreerd platform beschikbaar is. Hierdoor kan de IT-beveiliging gemakkelijker, sneller en effectiever worden beheerd. Kaspersky Lab's endpointbeheer levert een essentiële koppeling tussen het opstellen van IT-beveiligingsbeleid en het bruikbaar maken van dit beleid.

SECURITY INTELLIGENCE SERVICES
Opkomende dreigingen: een gewaarschuwd mens telt voor twee

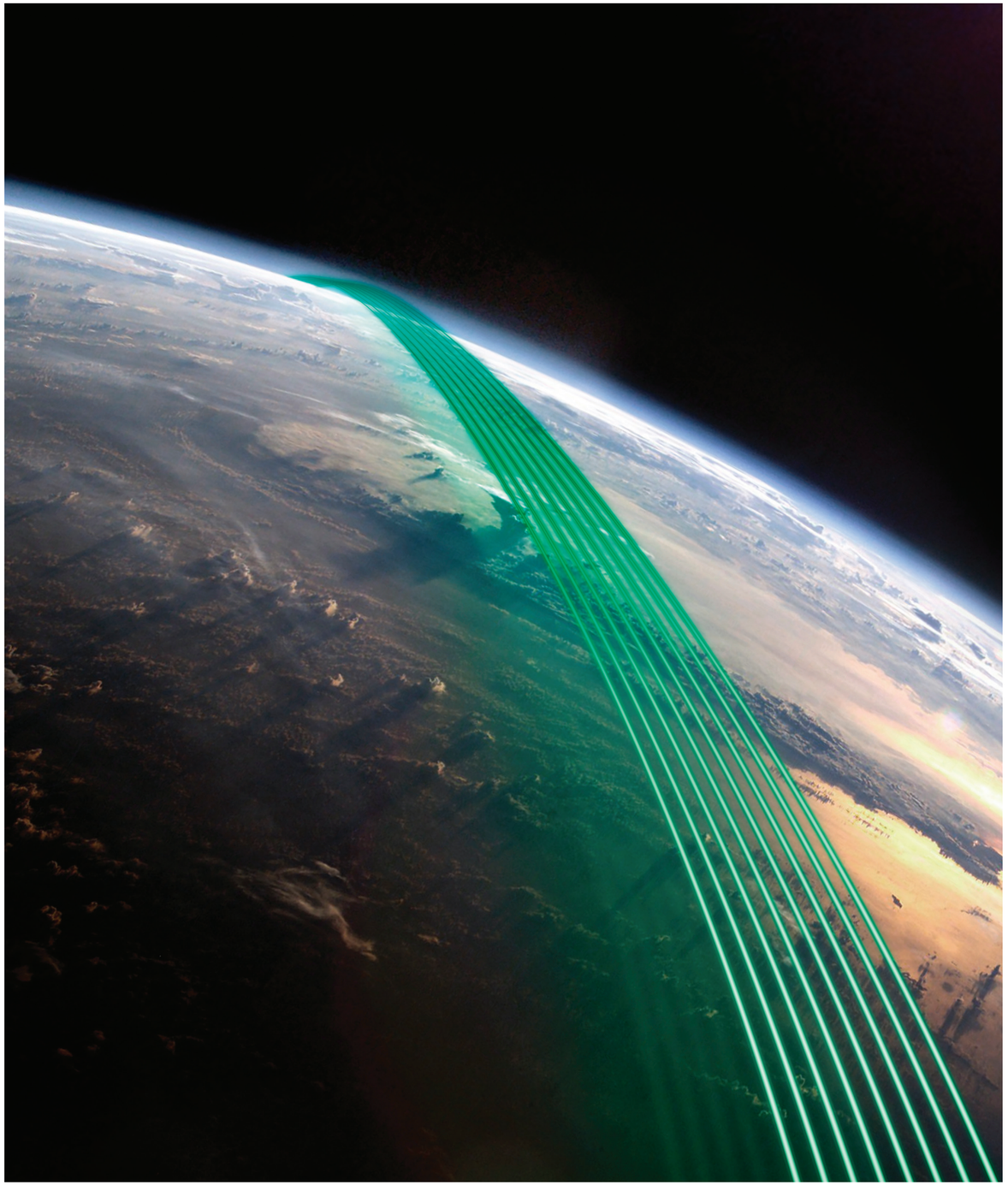
Kaspersky Lab detecteert dagelijks meer dan 315.000 nieuwe malwareprogramma's

Om dreigingen goed te kunnen bestrijden, moeten IT-afdelingen de aard van de dreigingen begrijpen. Nu cyberaanvallen op steeds grotere schaal voorkomen en steeds geavanceerder worden, en de criminelen achter de aanvallen continu iets nieuws bedenken om de beveiliging van hun doelen te ondermijnen, is het niet meer voldoende alleen te reageren als er iets gebeurt.

Ondernemingen moeten weten welk gevaar er op de loer ligt, zodat ze maatregelen kunnen nemen.

Kaspersky Lab's Security Intelligence Services houden het dreigingslandschap continu in de gaten. Ze identificeren opkomend gevaar en ondernemen stappen om systemen te verdedigen en problemen uit de weg te ruimen. Door onze toonaangevende kennis van malware en cybercriminaliteit te combineren met een gedetailleerd inzicht in de bedrijfsvoering van onze klanten, kunnen we rapporten met bruikbare intelligentie genereren die aansluiten op de specifieke behoeften van de onderneming. Wat dus ook de omvang van de dreiging is (van phishing-e-mails die misbruik maken van een bepaalde merknaam tot de laatste wereldwijde trend in cybercriminaliteit), onze klanten blijven dreigingen altijd een paar stappen voor.

Behalve dat we algemene intelligentie en maatwerkrapporten leveren, kunnen we ook aanvallen onderzoeken die op onze klanten gericht zijn, de indringers identificeren, hun methoden analyseren en uitzoeken hoe ze kunnen worden bestreden. Verder verschaffen onze opleidingsdiensten IT-afdelingen de kennis die ze nodig hebben om aanvallen te detecteren en af te slaan voordat ze schade veroorzaken. En met Security Account Management hebt u constant toegang tot een Kaspersky Lab-expert, zodat we snel een oplossing voor mogelijke vulnerability's kunnen zoeken voordat criminelen ze kunnen exploiteren.



In onafhankelijke tests eindigen producten van Kaspersky Lab vaker in de top 3 dan die van andere leveranciers.

Kaspersky Lab is actief in meer dan 200 landen en regio's over de hele wereld en onze technologieën beschermen meer dan 300 miljoen mensen. We hebben meer dan 2800 zeer gekwalificeerde specialisten in dienst onder leiding van voorzitter en CEO Eugene Kaspersky, die veel internationale lofbetuigingen heeft ontvangen, waaronder die van Top Global Thinker door Foreign Policy Magazine in 2012.

Ons Global Research and Analysis Team (GReAT) bestaat uit de beste analisten in de branche. Het team vormt een integraal onderdeel van de grotere R&D-afdeling van Kaspersky Lab en biedt toonaangevende anti-dreigingsintelligentie en onderzoek en innovatie, zowel intern als extern. Onze klanten profiteren ook van het Kaspersky Security Network, dat cyberbeveiligingsgerelateerde gegevens in real-time verwerkt om ons vroeg inzicht in nieuwe dreigingen te geven en ons in staat te stellen maatregelen te ontwikkelen.

Behalve dat Kaspersky Lab individuen en bedrijven over ter wereld helpt zich te beveiligen tegen cyberdreigingen, werken we ook samen met internationale organisaties zoals INTERPOL en Europol, evenals nationale en regionale wethandhavingsdiensten wereldwijd om tegenmaatregelen te implementeren die de werking van malware en cybercriminaliteit tegengaan.

We gebruiken bij ons onderzoek technische expertise om alle elementen van een aanval te analyseren, van de infectiehaarden en schadelijke programma's tot de ondersteunde opdracht- en beheerinfrastructuur en exploitatiemethoden. We verwerken het gekregen inzicht in al onze oplossingen om ons te helpen malwareaanvallen op te sporen en te bestrijden, ongeacht hun oorsprong en doel. We zetten dus al onze ervaring in ten gunste van onze klanten.

Momenteel werken we aan de ontwikkeling van een set oplossingen, waaronder een beveiligd besturingssysteem voor industriële beheersystemen (SCADA-systemen), om beveiliging te bieden tegen de mogelijk verwoestende impact van aanvallen op kritieke infrastructuren. We overdrijven niet als we stellen dat het onze missie is de wereld tegen cybercriminaliteit te beschermen.

- Kaspersky Lab behaalt in onafhankelijke producttests de beste resultaten in de branche. In 2013 hebben de endpointproducten van Kaspersky Lab aan 75 tests en beoordelingen meegedaan. In 42 gevallen behaalden ze een eerste plaats en bij 86% van de tests kwam Kaspersky Lab in de top 3 terecht.
- Meer dan een derde van onze werknemers is werkzaam in R&D, met een toename van 38% in technologiepatenten van 2012 tot 2013.
- We hebben als eerste geavanceerde dreigingen zoals Duqu, Flame, Gauss, Red October, Icefog en The Mask ontdekt.
- Kaspersky Lab heeft meer dan 80 wereldwijde partners en technologie-OEM-overeenkomsten met bedrijven zoals IBM, Cisco, Juniper Networks, HP, Microsoft en Qualcomm.