KASPERSKY ENDPOINT SECURITY FOR BUSINESS: TECHNOLOGIE IN AKTION

Schutz vor sichtbaren Gefahren und vor versteckten Bedrohungen

KASPERSKY lab

THE POWER OF PROTECTION

kaspersky.de/business-security
#Securebiz

INHALT

Bei 94 % der Unternehmen ist es zu einer Art von externem Sicherheitsvorfall gekommen.

Quelle: Kaspersky-Umfrage zu globalen IT-Risiken, 2014

SCHÜTZEN SIE IHR UNTERNEHMEN VOR SICHTBAREN GEFAHREN... UND VOR VERSTECKTEN BEDROHUNGEN

Für eine verlässliche IT-Sicherheit zu sorgen, ist so wichtig wie nie zuvor.

UNWISSENHEIT SCHÜTZT VOR SCHADEN NICHT

Mehr als 30 % der Sicherheitsverletzungen passieren in Unternehmen mit 100 oder weniger Mitarbeitern.[1] 44 % der kleinen und mittelständischen Unternehmen (KMUs) wurden schon von Cyberkriminellen angegriffen.[2]

Viele von ihnen sind sich jedoch gar nicht bewusst, welche Gefahr Cyberkriminalität und hochentwickelte Malware für ihr Unternehmen darstellen. Obwohl weniger als ein Fünftel der kleineren Unternehmen angegeben haben, sich gar nicht gegen Online-Verbrechen zu schützen, sind lediglich 60 % von ihnen aktiv bemüht, ihre Malware-Schutzsoftware auf dem neuesten Stand zu halten.[3]

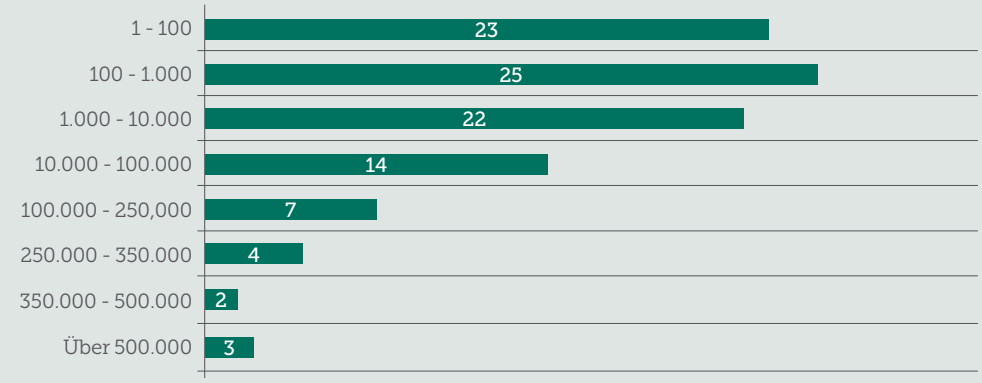
Der Glaube, das eigene Unternehmen wäre zu klein, um von Interesse zu sein, ist genau das, wovon Cyberkriminelle profitieren, wenn sie zunehmend komplexe Malware gegen Ihr Unternehmen einsetzen. Sie wissen, was vielen KMUs nicht bewusst ist: Auch Sie sind ein Angriffsziel.

[1] Untersuchungsbericht von Verizon zu Datenschutzverletzungen 2013
[2] Umfrage der National Small Business Association 2013
[3] Kaspersky Lab, Threatpost, 24. Mai, 2013

VERSTECKTE BEDROHUNGEN

Nehmen wir einmal an, Ihr Unternehmen gehört zu den 80 % der KMUs, die über irgendeine Art von IT-Sicherheitslösung verfügt. Das ist gut, aber kein Grund zur Entspannung: das Volumen an Bedrohungen wird von den meisten Unternehmen deutlich unterschätzt.[4] Lediglich vier Prozent der Befragten lagen bei der Einschätzung der Anzahl von täglich neu entdeckten Bedrohung auch nur ansatzweise richtig.[4]

GESCHÄTZTE ANZAHL DER TÄGLICH NEU ENTDECKTEN MALWARE-OBJEKTE (%)



Quelle: Kaspersky-Umfrage zu globalen IT-Risiken, 2014

Angesichts solcher Zahlen überrascht es kaum, dass IT-Sicherheitslösungen nicht selten als eine Art Massenprodukt angesehen werden, bei dem es nur geringfügige Unterschiede zwischen den verfügbaren Optionen gibt. Dies ist ein gefährlicher Aberglaube, denn selbst eine Abweichung von nur einem Prozent bei den Erkennungsraten kann in der Folge Hunderttausende von Malware-Objekten bedeuten, die innerhalb eines Jahres durch die Maschen schlüpfen. Woher wir das so genau wissen?

- Kaspersky Lab entdeckt jeden Tag 325.000 neue Malware-Objekte.
- Im zweiten Quartal des Jahres 2014 entdeckten unsere Anti-Malware-Lösungen 528.799.591 Virenangriffe auf Endbenutzersysteme und identifizierten dabei insgesamt 114.984.065 individuelle Schadobjekte.[5]

Dabei sind die gefährlichsten Bedrohungen jene, die Sie nicht kennen – die Bedrohungen, die unsere Experten bei Kaspersky Lab tagtäglich überwachen, analysieren und eliminieren. Wir handeln uns nämlich gerne und gezielt „Ärger" ein. Und wenn wir fündig werden, setzen wir mehr als ein Jahrzehnt Expertise und Erfahrung im Umgang mit Online-Bedrohungen ein, um Sie noch effektiver vor den Gefahren zu schützen, die Ihr Unternehmen auf jeden Fall vermeiden sollte – insbesondere wenn es sich dabei um so genannte APTs, also hochentwickelte, hartnäckige Bedrohungen, handelt.

Die Kluft zwischen dem Bild, das sich Unternehmen von der Bedrohungslage machen, und der tatsächlich vorhandenen Situation, geht immer weiter auseinander. Wir bezeichnen dies als „Wahrnehmungslücke". Unternehmen, egal welcher Größenordnung, scheinen das Ausmaß und die Schwere der Bedrohung, mit der sie sich auseinandersetzen müssen, grob zu unterschätzen.

Costin Raiu, Global Research & Analysis Team, Kaspersky Lab

[4] Kaspersky-Umfrage zu globalen IT-Risiken, 2014
[5] Kaspersky-Bericht zur Bedrohungsentwicklung im 2. Quartal 2014

SCHNELL, REAKTIV, INTELLIGENT

Kaspersky Lab kann bei der Entdeckung von hochkarätigen und bedeutsamen Bedrohungen auf eine lange Erfolgsgeschichte zurückblicken. So ist es uns beispielsweise gelungen, Carbanak (den weltweit größten Online-Bankraub), Dark Hotel, The Mask, Icefog und Red October aufzudecken. Mehr als ein Drittel unserer Mitarbeiter sind im Bereich Forschung und Entwicklung tätig. Sie konzentrieren sich vollständig auf die Entwicklung von Technologien, mit denen die sich ständig weiterentwickelnden Bedrohungen, die tagtäglich von unseren speziellen Analyseteams untersucht werden, vorhergesehen und abgewehrt werden können.

Unser Einblick in das Innenleben einiger der weltweit raffiniertesten Cyberbedrohungen bildet die Grundlage für die Entwicklung einer mehrstufigen Plattform aus Sicherheitstechnologien, die Sie vor bekannten, unbekannten und hochentwickelten Bedrohungen schützt. Unsere Technologien bieten Schutz vor Bedrohungen, die Sie erkennen können – aber auch vor denen, die im Verborgenen bleiben.

Aber wie erreichen wir dies? Es folgt ein kurzer Überblick darüber, wie die unterschiedlichen Malwareschutz- und Erkennungstechnologien von dem Moment an zusammenarbeiten, in dem eine Datei geladen wird. Es handelt sich dabei um eine einzigartige Kombination aus informationsbasierten Technologien, die eine mehrstufige, umfassende Erkennung und Abwehr von Bedrohungen auf unterschiedlichen Endpoints und anderen IT-Infrastrukturelementen ermöglicht.

ERKENNEN BEKANNTER BEDROHUNGEN

Von dem Moment an, in dem eine Datei heruntergeladen, eine Webseite geöffnet oder eine Anwendung gestartet werden soll, sorgen unsere hochentwickelten Anti-Malware-Engines dafür, dass bekannte, unbekannte und hochentwickelte Viren, Trojaner, Rootkits, Würmer, Spyware, Skripts, Adware und andere bekannte Schadobjekte, die sich in Webseiten und E-Mails verbergen, erkannt und neutralisiert werden. Für den Bereich der bekannten Bedrohungen stehen folgende Engines bereit:

NETWORK ATTACK BLOCKER

Der Network Attack Blocker überwacht den gesamten Netzwerkverkehr auf Grundlage von bekannten Signaturen, um netzwerkbasierte Angriffe, einschließlich Portscanning, Denial-of-Service-Attacken (DoS), Pufferüberläufe und schädliche Remote-Aktivitäten, zu erkennen und abzuwehren.

BLACKLISTS

Spezialteams aus Malware-Analysten aktualisieren die Kaspersky-Datenbanken kontinuierlich mit den allerneuesten Malware-Signaturen und -Daten. Diese dienen zur automatischen Blockierung sämtlicher bekannter Malware-Objekte.

URL-FILTERUNG

Gleicht die URLs im eingehenden/ausgehenden Datenverkehr mit der Kaspersky-Datenbank aus bekannten schädlichen Webseiten oder Phishing-Websites ab, blockiert webbasierte Angriffe, serverseitige polymorphe Malware sowie Command-and-Control-Server (C&C).

FIREWALL

Analysiert sämtliche ein- und ausgehenden Datenpakete und lässt diese durch bzw. sperrt sie je nach bestehendem Sicherheitsrisiko. Nicht autorisierte Verbindungen werden geblockt, um die Angriffsfläche und damit das Infektionsrisiko zu verringern. Die Netzwerkaktivität von infizierten oder anderweitig gefährdeten Systemen wird eingeschränkt. Hierdurch wird die Verbreitung von Malware und der Schaden durch Verstöße gegen Sicherheitsrichtlinien eingedämmt.

Unsere signaturbasierten Technologien basieren auf jahrelanger Erfahrung und profundem Wissen. Alle oben genannten Technologien sind äußerst wirkungsvoll, wenn es darum geht, bekannte Malware abzuwehren (und dank des Kaspersky Security Network bleiben viele Bedrohungen, wie weiter unten beschrieben, auch nur sehr kurze Zeit unbekannt). Aber wie sieht es mit den nur schwer zu fassenden unbekannten bzw. hochentwickelten Bedrohungen aus, von der weiter oben die Rede war? Auch hierfür haben wir eine Lösung...

[6] Dank einer Erkennungsrate von 99,75 % und einer Fehlalarmquote von Null ging die Anti-Spam-Technologie von Kaspersky Lab als Sieger aus dem VB Spam Test im November 2014 hervor.

ERKENNEN UNBEKANNTER BEDROHUNGEN

Werfen wir einen Blick darauf, was passiert, wenn eine Datei die signaturbasierten Kontrollen passiert hat und ausgeführt werden soll. Die mehrstufigen, schnellen Technologien von Kaspersky Lab analysieren die Datei noch während der Ausführung und suchen dabei nach verdächtigen oder schädlichen Verhaltensmustern, die auf eine unbekannte Bedrohung hinweisen könnten.

HEURISTIK

Heuristische Analyseverfahren sorgen für schnellen Schutz vor Bedrohungen, die mit herkömmlichen Antiviren-Datenbanken nicht aufgespürt werden können. Unsere heuristischen Verfahren versetzen uns in die Lage, neue Malware oder noch nicht bekannte Modifikationen bekannter Malware zu erkennen. Mit statischen Analyseverfahren wird der Code auf Anzeichen verdächtiger Befehle untersucht, während mit der dynamischen Analyse der Maschinencode überprüft wird, der möglicherweise von einer Datei ausgeführt werden soll. Dabei wird auf die emulierten Aufrufe mit voraussichtlichen Antworten reagiert, um festzustellen, ob der Code sicher ist oder nicht.

HEURISTISCHE VERFAHREN ZUR PHISHING-ABWEHR

Bei extrem neuartigen Attacken, von denen nur eine kleine Anzahl von Benutzern betroffen sind, sucht unsere Technologie nach zusätzlichen Anzeichen verdächtiger Aktivität, z. B. nach Vokabular, Eingabeformularen oder unleserlichen Symbolfolgen. Dies geschieht zusätzlich zu dem herkömmlichen datenbankorientierten Ansatz, der weiter oben beschrieben wurde.

Phishing-Maschen waren in letzter Zeit der Ausgangspunkt für viele hochgefährliche ATPs.

HOST INTRUSION PREVENTION SYSTEM (HIPS)

Dank unseres HIPS steht eine weitere Schutzschicht zur Verfügung, die verdächtige Anwendungen und Aktivitäten erkennt und verarbeitet und somit verhindert, dass Malware-Bedrohungen ausgeführt werden können. Durch das Festlegen von auf eine anfängliche Analyse folgenden Vertrauensstufen können Sie mit dem HIPS das Verhalten von Programmen kontrollieren. Über die Vertrauensstufe wird festgelegt, welche Ressourcen Anwendungen nutzen können, auf welche Daten sie zugreifen, und welche sie modifizieren dürfen etc. Vertrauensstufen schränken die Ausführung potentiell gefährlicher Programme ein, ohne das Leistungsverhalten von genehmigten, sicheren Anwendungen zu beeinträchtigen. Ein nicht vertrauenswürdiges Programm darf überhaupt keine Aktivitäten entfalten – es kann nicht einmal ausgeführt werden.

PROGRAMMKONTROLLE UND WHITELISTING

Die Programmkontrolle lässt die Ausführungen von Programmen zu, die vom Administrator festgelegt werden, oder blockiert diese. Unser Ansatz basiert auf dem dynamischen Whitelisting – eine fortlaufend aktualisierte Liste vertrauenswürdiger Programme und Softwarekategorien, die nur auf Grundlage bestimmter Regeln und Richtlinien ausgeführt werden können. Kaspersky Lab betreibt ein eigenes, spezielles Whitelisting-Labor mit einer zugehörigen Datenbank aus Milliarden von Dateien, die um ca. eine Million Dateien täglich anwächst.

Programmkontrolle und Whitelisting reduzieren das Risiko durch Bedrohungen, die uns bislang unbekannt sind, da Malware in der Regel in Form einer Programmdatei auftaucht, die noch nicht in einer Whitelist verzeichnet ist. Unternehmen, die mit diesem Ansatz (und den dafür erforderlichen Technologien) arbeiten, können also die Ausführung von Schaddateien verhindern, ohne diese zu kennen oder wissen zu müssen, wie sie genau aussehen.

KASPERSKY SECURITY NETWORK

Das Kaspersky Security Network ist ein weltweites, cloud-basiertes Forschungslabor für Cyberbedrohungen. Das Kaspersky Security Network erkennt, analysiert und verarbeitet bekannte, unbekannte und neuartige Bedrohungen und den Ursprung von Online-Attacken innerhalb von Sekunden und überträgt die gewonnenen Erkenntnisse unmittelbar an die Systeme unserer Kunden.

Durch die Nutzung anonymisierter Echtzeitdaten von 60 Millionen Endpoints weltweit unterliegt jede einzelne Datei, die die von Kaspersky Lab geschützten Systeme durchläuft, einer Analyse, die auf relevanten Bedrohungsinformationen beruht. Dieselben Daten stellen sicher, dass die am besten geeignete Gegenmaßnahme eingeleitet wird. Im Zusammenspiel mit den übrigen Komponenten der Kaspersky-Engine sorgt das Kaspersky Security Network so für Schutz vor unbekannten Bedrohungen, noch bevor Signaturen verfügbar sind. Herkömmliche signaturbasierte Reaktionen können Stunden in Anspruch nehmen; das Kaspersky Security Network benötigt hierfür ca. 40 Sekunden.

ERKENNEN UNBEKANNTER BEDROHUNGEN

Ihre Datei wurde heruntergeladen und ausgeführt. Unsere Technologien haben die Datei geprüft, analysiert, mit aktuellen Informationen verglichen und sie dann auf Grundlage bekannter und unbekannter Bedrohungen entweder blockiert oder zugelassen.

Aber wie sieht es mit hochentwickelten Bedrohungen aus?

Die Technologien zur Erkennung hochentwickelter Bedrohungen nutzen eine Reihe schneller und ausgeklügelter verhaltensbasierter Mechanismen, die das Verhalten von Prozessen überwachen, verdächtige Verhaltensmuster erkennen, schädliche Aktivitäten blockieren und ggf. bereits vorgenommene Änderungen, einschließlich Cryptors, zurücksetzen.

Sehen wir uns dies einmal näher an ...

AKTIVITÄTSMONITOR

Der Aktivitätsmonitor erfasst Daten zu Programmen und anderen wichtigen Systemaktivitäten mithilfe von Tracking-Routinen und unterscheidet dabei Verhaltensmuster. Die Erkenntnisse werden an die anderen weiter oben beschriebenen Schutzkomponenten von Kaspersky Lab weitergegeben. Mit Aktivitäten, die mit Bedrohungsmustern übereinstimmen, wird entweder auf Grundlage der vom Administrator festgelegten Richtlinien verfahren oder es wird die Standardeinstellung angewendet, d. h. der Schadprozess wird beendet und zur späteren Analyse in Quarantäne genommen.

Der Treiber in unserer Anti-Malware-Komponente, der die Dateioperationen abfängt, erfasst ebenfalls Informationen über Änderungen an der Registry, während die Firewall Daten über die Netzwerkaktivitäten der Programme sammelt. Sämtliche Informationen werden in den Aktivitätsmonitor eingespeist, der wiederum über ein eigenes Modul verfügt, das in der Lage ist, auf komplexe Systemereignisse wie die Installation von Treibern zu reagieren.

Schädliche Aktionen und destruktive Verhaltensmuster, die auf Malware hinweisen, werden blockiert.

AUTOMATISCHER EXPLOIT-SCHUTZ (AEP)

Diese Technologie richtet sich speziell gegen Malware, die Schwachstellen in Software ausnutzt. Die auf einer eingehenden Funktionsanalyse der am weitesten verbreiteten Exploits beruhende Technologie ist in der Lage, typische Verhaltensmuster zu erkennen und deren vollständige Ausführung zu verhindern.

AEP funktioniert wie ein Sicherheitsnetz, das unsere anderen Technologien ergänzt. Er arbeitet mit unserem Aktivitätsmonitor zusammen.

ROLLBACK

Die kontinuierliche und detaillierte Überwachung der Systeme ermöglicht es, dass Änderungen mit außergewöhnlich hoher Präzision zurückgesetzt werden können, d. h. die Auswirkungen von Infizierungen lassen sich begrenzen und die Systeme können in einen sicheren Zustand zurückversetzt werden. Rollback-Mechanismen können aktualisiert werden und basieren auf eigens erstellten und modifizierten Programmdateien, MBR-Modifikationen, wichtigen Windows-Dateien und Registrierungsschlüsseln.

DEFAULT DENY

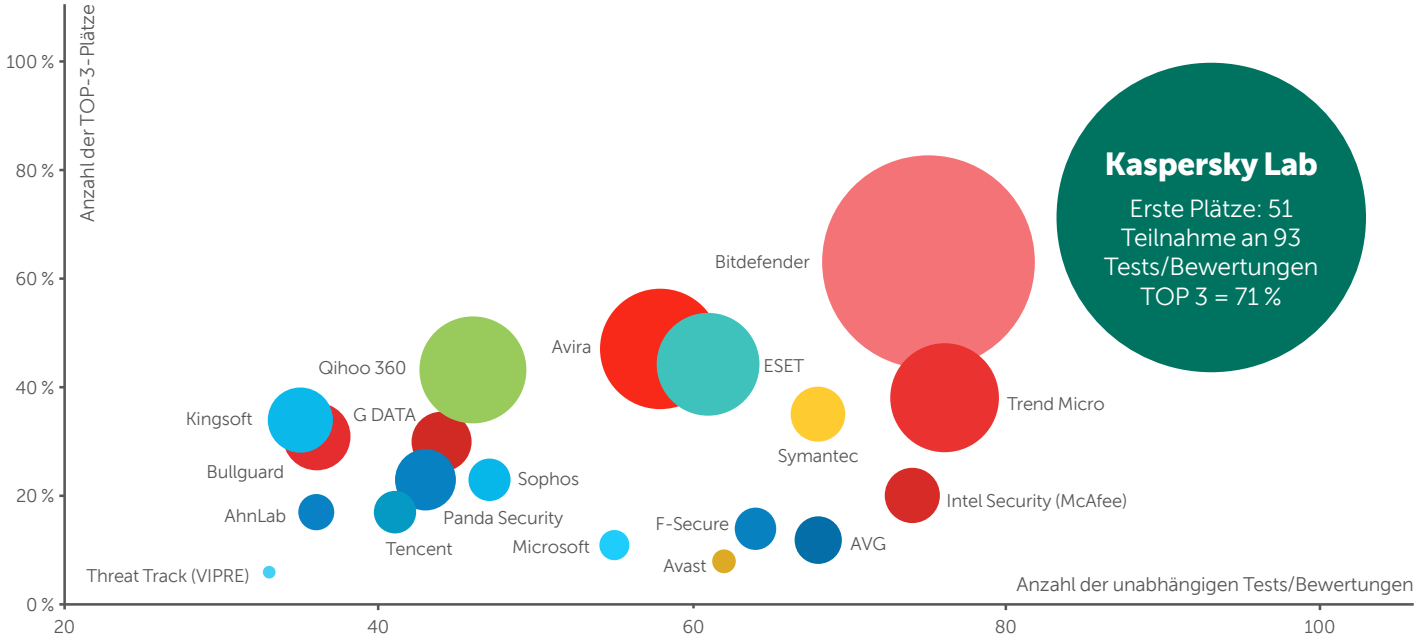
Der Default-Deny-Modus wird zunehmend als die wohl effektivste Sicherheitsstellung im Umgang mit einer sich ständig weiterentwickelnden Bedrohungslage gesehen. Dabei wird die Ausführung aller Programme auf allen Workstations blockiert, und es werden nur die explizit vom Administrator zugelassenen Programme ausgeführt.

„Default Deny" bedeutet, dass sämtliche neuen, dateibasierten Malware-Variationen automatisch blockiert werden, selbst bei gezielten Angriffen.

KLEINE VERÄNDERUNGEN KÖNNEN DEN ENTSCHEIDENDEN UNTERSCHIED AUSMACHEN

Wie wir gesehen haben, kann ein einziger zusätzlicher Prozentpunkt bei der Erkennungsrate zu Hunderttausenden von Malware-Objekten führen, die durch das Sicherheitsnetz schlüpfen. Wir haben außerdem erfahren, wie unsere zusätzlichen Mechanismen für Abwehr, Erkennung und Analyse unbekannte und sogar hochentwickelte Bedrohungen erkennen und ausschalten, bevor sie Schaden anrichten können.

KASPERSKY LAB BIETET DEN BESTMÖGLICHEN SCHUTZ*



Unabhängige Testergebnisse beweisen übereinstimmend, dass Kaspersky Lab den bestmöglichen Schutz bietet. Allein 2014 haben wir an 93 unabhängigen Tests und Bewertungen teilgenommen, aus denen wir 51 Mal als Sieger hervorgingen und in 71 % der Fälle eine Top-3-Platzierung erreichten. Dies ist nur einer der Gründe, warum viele OEMs – darunter Microsoft, Cisco Meraki, Juniper Networks und Alcatel Lucent – Kaspersky Lab die internen Sicherheitsfunktionen ihrer eigenen Produkte anvertrauen.

Sämtliche Sicherheitstechnologien von Kaspersky Lab werden hausintern und auf Grundlage ein und derselben Codebasis entwickelt und auf dem neuesten Stand gehalten. Hieraus ergibt sich eine nahtlose Integration, die den Aufbau einer mehrstufigen Plattform ermöglicht, die leistungsfähiger ist als die Summe ihrer Einzelteile. Dieses Maß an Integration führt überdies zu einer verbesserten Performance, schnelleren Updates und einem einheitlichen Look and Feel – damit Sie mehr Zeit haben, sich auf Ihre Kernkompetenzen zu konzentrieren, während Kaspersky Lab sich um Ihre Sicherheit kümmert.

* Anmerkungen:
Laut dem Gesamtergebnis eines im Jahr 2014 durchgeführten unabhängigen Tests von Unternehmens-, Verbraucher- und mobilen Produkten.

Das Gesamtergebnis umfasst Tests, die von den folgenden unabhängigen Testlaboren und Zeitschriften durchgeführt wurden:
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin.
Die Größe des Kreises entspricht der Anzahl erster Plätze.

NOCH HEUTE EINSTEIGEN: KOSTENLOSE 30-TÄGIGE TESTVERSION

Mit unserer kostenlosen Testversion können Sie sich unverbindlich davon überzeugen, wie effektiv unsere hochwertige Sicherheitslösung Ihr Unternehmen vor Malware und Cyberverbrechen schützt.

Besuchen Sie **kaspersky.com/trials**, um sich vollständige Produktversionen herunterzuladen, und sehen Sie selbst, wie zuverlässig Kaspersky Lab Ihre IT-Infrastruktur, Endpoints und vertraulichen geschäftlichen Daten schützt.

DEMOVERSION JETZT KOSTENLOS HERUNTERLADEN

DEM GESPRÄCH BEITRETEN

#Securebiz

Auf YouTube ansehen

Werden Sie unser Fan auf Facebook

Folgen Sie uns auf Twitter

Treten Sie uns auf LinkedIn bei

Auf Slideshare ansehen

Lesen Sie unseren Blog

Treten Sie uns auf Threatpost bei

Schauen Sie sich uns auf Securelist an

ÜBER KASPERSKY LAB

Kaspersky Lab ist der weltweit größte Privatanbieter von Lösungen für den Schutz von Endpoints. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer*. In seiner 17-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Einzelverbrauchern wirksame digitale Lösungen für die Datensicherheit. Der Hauptsitz des Unternehmens ist in Großbritannien registriert. Kaspersky Lab ist zurzeit in nahezu 200 Ländern und Regionen weltweit tätig und sorgt für den Schutz von mehr als 400 Millionen Anwendern weltweit. Weitere Informationen erhalten Sie unter: www.kaspersky.de.

* Das Unternehmen belegte im Rahmen des IDC-Rating „Worldwide Endpoint Security Revenue by Vendor 2013" den vierten Rang. Die Aufstellung stammt aus dem IDC-Bericht „Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares" (ID #250210, August 2014). In dem Bericht wurden Softwarehersteller auf Grundlage ihrer Erlöse aus dem Verkauf von Sicherheitslösungen für Endpoints im Jahr 2013 eingestuft.

kaspersky.de/business-security
#Securebiz