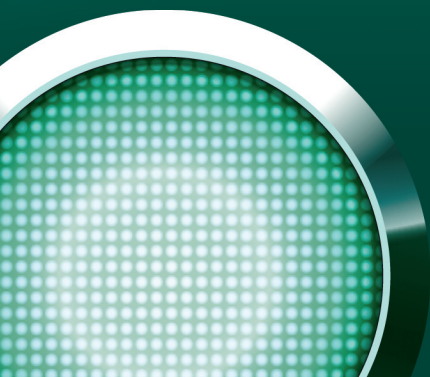


**KASPERSKY**

W H I T E P A P E R

# Sicherheitsstrategien in KMUs



Während in großen Unternehmen, dem Enterprise-Segment, in der Regel komplette Teile der IT-Abteilung mit dem Aufbau und der Pflege der Sicherheitsinfrastruktur beschäftigt sind, ist in den kleinen und mittleren Unternehmen (KMUs) eine solche personelle Ausstattung nicht möglich. Welchen Gefahren sind diese Firmen ausgesetzt, und wie lassen sie sich möglichst ohne Last für das Personalbudget abwenden?

Was das Thema „IT-Security“ in den kleinen und mittleren Unternehmen angeht, so sieht die Realität üblicherweise eher düster aus. Kein Systemadministrator oder IT-Mitarbeiter hat die zeitliche Ressource, sich ausgiebig mit sicherheitsrelevanten Meldungen und Entwicklungen auseinander zu setzen. Es ist weit weniger die Frage des Wollens als der schlichte Umstand, dass für Sicherheit oft keine Zeit bleibt. Der Grund dafür liegt auf der Hand – solange alles ohne Probleme läuft, merkt niemand, dass sich hier und da bereits eklatante Sicherheitsrisiken auftun. Sicherheit ist unbequem, verbraucht Zeit und Geld und wird nicht einmal mit „Ruhm und Ehre“ bedacht. Sollte zu später Stunde die IT-Mannschaft noch einige Sicherheitspatches einspielen, so ist eher der Kommentar über die anfallenden Überstunden wahrscheinlich, denn der Dank dafür, dass außerhalb der regulären Arbeitszeit ein solcher Einsatz überhaupt zustande kommt.

Die Sensibilisierung rund um das Thema „Sicherheit“ in Richtung der Chefetage, der Unternehmensleitung oder dem Vorstand ist und bleibt die Sache des IT-Beraters oder des eigenen EDV-Leiters. Auch wenn die Zeit dafür fehlt, jedes einzelne böartige Programm beim Vornamen zu kennen, so ist doch die Kenntnis über die Gestalt des potentiellen Gegners von entscheidender Wichtigkeit.

Der Begriff „Computervirus“ wird seit einigen Jahren stellvertretend für verschiedene Schadprogramme benutzt. Da die Übergänge zwischen den einzelnen Schädlingen zunehmend fließend werden, ist diese Verallgemeinerung nachvollziehbar. Ein besser geeigneter Begriff für die allgemeine Benennung wäre jedoch „Malware“.

**Viren** sind die älteste Gattung von Malware und etwa seit Mitte der 1980er Jahre bekannt. Ein Computervirus verbreitet sich, indem er sich einen neuen Wirt (zum Beispiel eine Programmdatei, früher auch häufig einen Bereich im Bootsektor) sucht und

seinen Code dorthin kopiert. Dies geschieht allerdings nur lokal auf dem infizierten PC, entweder beim Start eines Virus, oder auch noch danach, indem sich der Virus resident im Speicher einnistet. Eine Verbreitung über Rechnergrenzen hinweg ist nur durch die Weitergabe von befallenen Datenträgern oder den Versand infizierter Dateien möglich. Zusätzlich zu diesem Verbreitungsmechanismus können Computerviren auch eine Schadroutine beinhalten, die bis zum kompletten Datenverlust führen kann.

**Trojaner** beschränken sich auf die Schadroutine und vermehren sich nicht selbst. Um für eine große Verbreitung zu sorgen, geben sie vor, eine nützliche Anwendung zu sein.

**Würmer** verbreiten sich aktiv auf neue Systeme, indem sie Sicherheitslücken in den Netzwerk-Diensten nutzen oder Standardpasswörter verwenden. Auch Computerwürmer können eine Schadfunktion beinhalten, die unter bestimmten Umständen aktiviert wird.

**Bot-Netze** (englisch „botnets“) sind eine weiterentwickelte Kombination aus Würmern und Trojanern. Hierbei handelt es sich um einen Netzwerkverbund von infizierten PCs, die über das Internet ferngesteuert werden können. Typischerweise werden diese Bots für die Verbreitung von Spam oder Denial-of-Service-Attacken eingesetzt, ohne dass die PC-Nutzer davon etwas merken. Bekannteste Vertreter von Botnet-Programmen sind Agobot, R(x)Bot oder Phabot.

Eine Infektion von Unternehmens-Computern durch Malware kann nicht nur den üblichen Arbeitsablauf unterbrechen oder stören, sondern auch Firmenheimlichkeiten in Gefahr bringen. Programme, die Daten aus dem Unternehmensnetz ausspionieren und an einen externen Server schicken, heißen **Spyware**. Eine weitere Gefahr stellen kriminelle **Hacker** dar, die sensible Daten ausspähen, aber auch über Denial-of-Service-Attacken die Firmenserver lahmlegen können.

Ebenso lästig sind unerwünschte **Spam- und Phishing-Mails**. Auch Sie schaden einer Firma, denn das manuelle Aussortieren von Spam kostet täglich viel Arbeitszeit. Ebenso wie Malware sollten daher auch solche Nachrichten automatisiert ausgefiltert werden.

**Tipp:** Eine ausführliche Geschichte der Schadprogramme finden Sie auf der Homepage von Kaspersky Lab unter [www.kaspersky.de](http://www.kaspersky.de).

Die Gestalt und das Auftreten von Malware sind permanenten Veränderungen unterworfen. Einer EDV-Abteilung kann kaum zugemutet werden, dass jede aktuelle Gefährdung im Detail bekannt ist. Glücklicherweise ist dies auch nicht notwendig, sofern etablierte Sicherheitsfunktionen laufend auf dem neuesten Stand gehalten werden. Der regelmäßige Blick auf News-Bulletins oder das Abonnement von RSS-Feeds mit der Übersicht der aktuellen Bedrohungen ist in jedem Fall ein einfacher und gleichzeitig nützlicher Schritt, um die Aktivitäten der Malware-Autoren im Auge zu behalten.

### Dreistufiges Sicherheitskonzept

Im Allgemeinen kommt ein dreistufiges Sicherheitskonzept beim Schutz eines Unternehmens vor Hackern und Malware zum Einsatz:

- **Stufe 1 – Firewall / IDS**
- **Stufe 2 – Aktualisierung der Betriebssysteme**
- **Stufe 3 – Antiviren- / Anti-Malware-Lösungen**

Auch wenn die drei Stufen für sich betrachtet voneinander unabhängig sind, so sind sie doch für die Sicherheit im Unternehmen gleichbedeutend. Beispielsweise dringt ohne eine aktivierte und richtig konfigurierte Firewall eine sehr große Anzahl von Attacken bis zu den Anwender-PCs durch und muss von dort aktiven Schutzfunktionen abgewehrt werden.

#### Stufe 1 – Firewall / IDS

Die Firewall ist die erste und entscheidende Grenze zwischen dem Internet und dem lokalen Netzwerk. Bereits kleine DSL-Router verfügen über Funktionen, um eine Vielzahl von Attacken abzuwehren. Als ergänzende Sicherheitsstrategie kommen „Intrusion Detection Systeme“ (IDS) zum Einsatz. Bei dieser Hard- oder Software handelt es sich um Systeme, die in der Lage sind, den Netzwerkverkehr auf bekannte Angriffsversuche hin zu überwachen oder Veränderungen in der Gestalt des Datenstroms zu erkennen und gegebenenfalls Alarm zu schlagen. Verwirft das IDS automatisch die betroffenen Datenpakete, so handelt es sich bereits um ein „Intrusion Prevention System“ (IPS).

Spätestens seit Microsoft das Desktop-Betriebssystem Windows XP mit einer integrierten Firewall anbietet, ist der Einsatz der so genannten „Personal Firewalls“ zunehmend üblicher geworden. Auch innerhalb des lokalen Netzwerks ist die Aktivierung der „Personal Firewall“ eine zusätzliche Schutzfunktion, die vor unerlaubten Zugriffen aus dem eigenen Netzwerk schützt. In vielen Unternehmen kommt die Windows-Firewall jedoch kaum zum Einsatz, was zum einen auf die mangelnde zentrale Administrierbarkeit zurückzuführen ist. Zum anderen haben viele Anwender Zweifel daran, ob die Firewall des Betriebssystem-Herstellers selbst die Lücken des Systems zuverlässig stopfen kann. Umfassende Schutzlösungen wie die von Kaspersky Lab beinhalten eine zentral administrierbare, ausgereifte Personal Firewall mit IDS/IPS, um einen möglichst hohen Schutz der Anwender-PCs zu gewährleisten.

#### Stufe 2 – Aktualisierung der Betriebssysteme

Hacker, Viren, Trojaner & Co. nutzen Sicherheitslücken in Betriebssystemen und Programmen aus, um sich zu reproduzieren und Schaden auszuüben. Microsoft Windows ist sowohl als Desktop- und Server-Betriebssystem stark verbreitet und darum als potentiell Opfer für Programmierer von Malware von hohem Interesse. Jahrelang hat es Microsoft zudem versäumt, die eigene Software von Haus aus sicher zu gestalten. Während Windows NT 4.0 noch alle Funktionen des Betriebssystems grundsätzlich nach der Installation aktivierte, so ist dies bei Windows XP/2003 glücklicherweise anders. So kann ein für Angriffe anfälliger Systemdienst, beispielsweise der Webserver „Internet Information Server“ (IIS), in deaktiviertem Zustand nicht als Sicherheitslücke genutzt werden.

Das aktuelle Desktop-Betriebssystem Windows Vista geht hier noch einen großen Schritt weiter und warnt beziehungsweise fragt den Anwender explizit, ehe eine Systemeinstellung geändert werden kann. An sich eine sehr gute Sache – jedoch schalten viele Anwender ob der vielen Meldungsfenster dieses Feature bereits nach kurzer Zeit ab.

Das regelmäßige Aktualisieren des Betriebssystems, aber auch der vom Anwender benutzten Applikationen, ist für die Gesamtsicherheit der IT-Infrastruktur ein Muss. Diese administrative Aufgabe übernimmt Patchmanagement-Software unterschiedlicher Hersteller. Da ständige Aktualisierungen der Signa-

turen und Erkennungsalgorithmen bei Antiviren-Software eine zentrale Rolle spielen, gehören automatische Updates bei professionellen Anbietern zum Standard.

### Stufe 3 – Antiviren- / Anti-Malware-Lösungen

Auch wenn die Schutzmechanismen der Firewall und des Betriebssystems einwandfrei funktionieren, bleibt stets ein Restrisiko für Server und Computer, durch Schadprogramme attackiert zu werden. Die letzte Verteidigungslinie stellt somit die Antivirensoftware dar. Es gibt verschiedene Kriterien, denen eine moderne Antimalware-Lösung gerecht werden muss. Das wichtigste Kriterium in diesem Zusammenhang überhaupt ist die **Erkennungsrate**, als Maß für die Fähigkeit, überhaupt einen Schädling als solchen identifizieren zu können. Da sich ein neuer Computerwurm binnen kürzester Zeit über die ganze Welt verbreiten kann, muss der Anbieter die Updates der Antiviren-Pattern – also die für die Erkennung nötigen Informationen – möglichst schnell bereitstellen. Natürlich nimmt jedes Antivirenprogramm für sich in Anspruch, mit einer besonders hohen Erkennungsrate zu glänzen. Eine objektive Einschätzung können jedoch einzig und allein unabhängige Labore geben. Bei solchen Tests belegen Kaspersky-Produkte regelmäßig einen Spitzenplatz.

Unabhängige Tests werden unter anderem von den folgenden renommierten Einrichtungen durchgeführt: das britische Fachblatt für Computerviren „Virus Bulletin“, das unabhängige deutsche Labor AV-Test.org und das unabhängige österreichische Labor Av-Comparatives.org. Die Antiviren-Datenbank von Kaspersky Lab wird stündlich aktualisiert, was im Monatsdurchschnitt rund 700 Aktualisierungen bedeutet. Im Fall einer Epidemie ist die Datenbank innerhalb kürzester Zeit auf dem neuesten Stand und schützt Computersysteme weltweit. Antivirenlösungen sollten stets so konfiguriert sein, dass Aktualisierungen automatisch heruntergeladen und verteilt werden. Nur so ist eine schnelle Identifikation von neuen Schadprogrammen gesichert.

Wie beim Schutz vor Spam, so gibt es auch bei Antivirenlösungen das Risiko eines Fehlalarms (False Positive). Wird eine an sich unverseuchte Datei irrtümlich als infiziert eingestuft, so kann dies fatale Auswirkungen auf ein Computersystem haben. Mögliche Folgen sind Datenverlust durch das Löschen von Dateien oder das Blockieren bestimmter

Programme. Unabhängige Tests haben Kaspersky Lab mehrfach bescheinigt, dass das **Risiko eines Fehlalarms** bei Kaspersky Anti-Virus praktisch Null ist. Obwohl es eine sehr große Anzahl von Viren gibt, ähneln sie sich oft in der Funktionsweise. Es handelt sich entweder um Varianten bekannter Schadprogramme oder aber um ähnlich programmierte Neuentwicklungen. Um neue, noch unbekannte Varianten zu erkennen, verlässt sich die heuristische Analyse nicht auf feststehende Signaturen, sondern berücksichtigt allgemeinere, typische Merkmale von Malware. So schützt ein gutes Antivirenprogramm bereits dann, wenn noch keine Signatur für einen neuen Schädling vorliegt. Die Antivirus-Engine von Kaspersky Lab ist heute in der Lage, praktisch jede Art von Malware in ausführbaren Dateien, im Arbeitsspeicher oder in Sektoren der Datenträger aufzuspüren.

Virenschreiber versuchen mit verschiedenen Techniken, die Erkennung ihrer Kreationen zu verhindern. Weit verbreitet ist die **Komprimierung** des Schadprogramms mit verschiedenen Utilities. Durch die Kompression werden einige Dateiparameter so verändert, dass eine Erkennung erschwert wird. Die Anzahl unterschiedlicher Kompressionsalgorithmen geht in die Hunderte, oft werden sie auch noch kombiniert. Statt für jede mögliche Kompressionsform eines Virus eine eigene Signatur anzulegen, ist es sinnvoller, komprimierte Dateien für die eigentliche Analyse komplett auszupacken. Nur so ist sichergestellt, dass ein bereits bekannter Virentyp auch dann identifiziert wird, wenn er neu gepackt wurde. Kaspersky Anti-Virus beispielsweise unterstützt mehr als 450 verschiedene Utilities zur Datenkomprimierung, zur Installation und zur Archivierung.

Die Bedrohungsszenarien verändern sich sehr schnell, ständig kommen neue Typen von Malware in den Umlauf. Für eine sichere Erkennung ist daher neben der **Aktualisierung der Signaturen** auch die **Aktualisierung der Antivirus-Engine** selbst erforderlich. Kaspersky Anti-Virus aktualisiert automatisch sowohl die Antiviren-Datenbank als auch die Antiviren-Engine.

### Gefährdet ist nicht der Windows-PC allein!

Da auf vielen Computersystemen Microsoft Windows als Betriebssystem eingesetzt wird, ist es wenig verwunderlich, dass für dieses Betriebssystem die größte Anzahl an Malware existiert. Linux, Unix und MacOS

sind jedoch grundsätzlich nicht vor Malware gefeit. Seit dem Jahr 2002 existiert sogar Schadsoftware, die sowohl Windows- als auch Linux-Anwendungen befallen kann. Handheld-Computer, Smartphones und Mobiltelefone sind ebenfalls zunehmend durch Malware gefährdet. Auch plattformübergreifende Applikationen wie das Office-Paket von Microsoft oder auch OpenOffice werden durch spezielle Makroviren angegriffen.

Für die IT-Unternehmenssicherheit bedeutet dies ein Umdenken. Auf Server und Workstations begrenzte Schutzmaßnahmen reichen nicht mehr aus. Mobiltelefone und Handheld-PCs müssen wie Standard-PCs betrachtet und mit einer Antivirus-Lösung ausgestattet werden – insbesondere, wenn diese zur Synchronisation der Benutzerdaten mit einem stationären Rechner abgeglichen werden. Eine Antivirus-Lösung muss somit neben Windows, Novell NetWare, Unix, Linux und MacOS auch die Betriebssysteme der Mobilgeräte abdecken können.

### Optimierung für Server

Besonders File- und E-Mail-Kommunikationsserver sind neuralgische Punkte für den Schutz gegen Malware. Beinahe alle potentiellen Schädlinge gelangen als E-Mail-Nachricht oder als Datei in das Unternehmen. Alle Anbieter von professionellen Antiviren-Lösungen haben aus diesem Grund spezielle Varianten ihrer Software im Lieferprogramm. Die Unterstützung einer großen Anzahl von Prozessorkernen sowie eines deutlich größeren Arbeitsspeichers hilft bei der schnellen Überprüfung großer Datenmengen.

Klassischerweise werden regelmäßige Sicherungskopien der kompletten Unternehmensdaten, die auf den Servern liegen, vorgenommen. Um sicherzustellen, dass ein Wiedereinspielen der Backups im Schadensfall möglich ist, müssen diese Daten zum Speicherzeitpunkt frei von Schadsoftware sein.

Für die E-Mail-Sicherheit sind darüberhinaus weitere Funktionalitäten der Antiviren-Lösung von Interesse. Neben den Daten, die im E-Mail-Body zu finden sind, sind auch E-Mail-Anhänge und OLE-Objekte während des Scans zu berücksichtigen. Hier kommt erneut die Fähigkeit der Antivirus-Engine bezüglich unterschiedlichster Komprimierungsverfahren zum Vorschein. Mit der Prüfung des ein- und ausgehenden E-Mail-Verkehrs allein ist es bei einer

professionellen Lösung nicht getan. Üblicherweise besitzt ein Unternehmen bereits einen E-Mail-Server und somit auch eine oder mehrere Datenbanken, die nach der Installation der Antiviren-Lösung überprüft werden müssen. Um im Fall einer fehlerhaften Reparatur die originale E-Mail wiederherzustellen, sollte zudem vor dem Entfernen eines infizierten Objekts eine Sicherungskopie erstellt werden.

### Integration in Netzwerksicherheit

Die effektivste Lösung, um die von einem infizierten PC ausgehende Gefahr zu bannen, ist dessen Abtrennung vom restlichen Firmen-Netzwerk. Doch selbst wenn ein Anwender oder Administrator geistesgegenwärtig schnell reagieren würde, ist dies rund um die Uhr und bei einer größeren Anzahl von Computern manuell vollkommen undurchführbar. Die auf professionelle Netzwerksysteme spezialisierte Firma Cisco hat vor einigen Jahren in Gemeinschaft mit anderen Herstellern die Cisco Network Admission Control Initiative (NAC) ins Leben gerufen. Ziel der Initiative ist es, Geräte, die der aktuellen Sicherheitsrichtlinie im Unternehmen nicht entsprechen, erst gar nicht mit dem Netzwerk kommunizieren zu lassen. Technisch gesehen wird die Verbindung zur Netzwerkkarte unterbrochen oder in ein anderes virtuelles Netzwerk (VLAN) umgelenkt. Solche sich selbst schützenden Netzwerke identifizieren Bedrohungen und reagieren entsprechend dem Schweregrad der Attacke selbstständig und ohne Zeitverzögerung. Auch Kaspersky Lab ist Mitglied dieser Initiative und bietet die entsprechenden Informationen für Netzwerkgeräte von Cisco.

### Zentrale Administration

In kleineren Umgebungen mit weniger als fünf Computern ist es sicherlich ein gangbarer Weg, eine Antiviren-Software direkt vom Installations-Medium auf jeden PC zu installieren und so zu konfigurieren, dass jedes System die regelmäßigen Updates direkt von der Homepage des Herstellers bezieht. Somit unterscheidet sich die Konfiguration dieser PCs nicht von Rechnern, die im privaten Umfeld betrieben werden.

In größeren Umgebungen ist eine solche „Turnschuh-Administration“ weder zeitgemäß noch ressourcenschonend. Bereits die Versorgung der Client-PCs mit einer Antiviren-Lösung muss zentral geschehen. Dazu wird der Client-Agent direkt auf das System „gepusht“. Nach dem ersten Start der Agenten-Soft-

ware beginnt diese in regelmäßigen Abständen, Kontakt mit der Server-Software aufzubauen. Dabei prüft sie, ob neue Signaturdateien vorliegen, und ob ein Update für die Software selbst oder Regeländerungen umgesetzt werden müssen. Der komplette Vorgang ist im Idealfall für den Anwender vollkommen transparent, und es kommt zu keiner Unterbrechung der täglichen Arbeit.

Für den Systemadministrator hat diese Vorgehensweise viele Vorteile. Abgesehen davon, dass er sich Laufwege spart, ist er mit einem Blick in die Management-Oberfläche sicher, dass alle PCs am Standort gegen Malware gesichert sind. Für die Gestaltung der Management-Oberfläche hat sich unter Microsoft Windows in der jüngeren Vergangenheit die „Microsoft Management Console“ (MMC) als Standard-Arbeitsmittel für Administratoren herauskristallisiert. Die MMC erspart dem Administrator das Umlernen in eine andersartige Umgebung und ermöglicht gleichzeitig die Zusammenstellung individueller Oberflächen und Befehle, die der Administrator für die Bewältigung seiner täglichen Aufgaben benötigt. Da die MMC grundsätzlich die Kontaktaufnahme zu anderen Systemen ermöglicht, ist in vielen Fällen ein „Aufschalten“ auf einen Server überhaupt nicht mehr notwendig.

## Kaspersky Lab

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam und Hacker-Abwehr. Unser hoch spezialisiertes Virenlabor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen. Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Produkten anderer Hersteller – unter anderem Juniper, Clearswift, G-Data, Blue Coat, Alcatel und ZyXEL – als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, etwa dem heuristischen Analysator zur Entdeckung und Entschärfung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme. Die Antivirus-Technologien von Kaspersky Lab bieten eine hohe Erkennungsrate verschiedener Schadprogramme bei minimalen Fehlauflösungen und garantieren somit einen effektiven Schutz Ihrer

Computer und vertraulicher Daten. Eine Besonderheit der Programme ist die Virenprüfung archivierter und gepackter Dateien verschiedenster Formate. Der heuristische Analysator, das Intrusion Prevention System (IPS) und der Behaviour Blocker ermöglichen zudem einen proaktiven Schutz vor neuen, noch unbekanntem Viren. Die Antiviren-Datenbank und der Programmkern werden durch stündliche Updates aktuell gehalten. Neben den vielfach ausgezeichneten Programmen bietet Kaspersky Lab allen Kunden ein breites Angebot weiterer Dienstleistungen, wie die Anpassung an die Anforderungen des Unternehmens, so dass Sie ohne Ausfälle arbeiten können. Wir entwickeln maßgeschneiderte Antivirus-Lösungen und schulen die Mitarbeiter. Unsere Kunden haben Zugang zu einer der weltweit größten Antiviren-Datenbanken, die stündlich aktualisiert wird. Darüber hinaus bieten wir unseren Anwendern technische Unterstützung in deutscher, englischer, französischer und russischer Sprache.

### Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crime-ware, Hacker, Phishing-Attacken und Spam.

Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht.

Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen.

### Kontakt

Kaspersky Labs GmbH  
Steinheilstr. 13  
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0  
Telefax: +49 (0)841 981 89 100

info@kaspersky.de  
www.kaspersky.de