Whitepaper

KASPERSKY lab

Was Ihr IT-Schutz wirklich kostet
Total Cost of Protection

Be Ready for What's Next.

Inhaltsverzeichnis

Was Schutz wirklich kostet

Die Komplexität von IT-Umgebungen steigt, und die Bedrohung durch Malware wird immer größer. Dadurch stehen IT-Abteilungen vieler Unternehmen unter Druck, ihre Anti-Malware-Lösungen neu zu überdenken. Die bisherigen Lösungen, die gestern noch wirkungsvoll waren, sind wirkungslos angesichts der heutigen Bedrohungen, bei denen Sicherheitslücken auf mobilen Plattformen, in Open-Source-Systemen und im Internet ausgenutzt werden. Anti-Malware ist kein Massenartikel mehr, sondern Unternehmen müssen erkennen, dass ihre aktuelle Lösung sie mehr kostet, als sie je erwartet hätten. Sie denken darüber nach, Ihre aktuelle Lösung zu erneuern oder zu einem anderen Anbieter zu wechseln? Kaspersky Lab empfiehlt Ihnen eine ganz neue Herangehensweise, um Anti-Malware zu beurteilen – einen Ansatz, den wir Total Cost of Protection nennen.

Moderne IT-Umgebungen

Moderne IT-Umgebungen zeichnen sich dadurch aus, dass sie komplex sind und sich häufig verändern. Der Netzwerkperimeter hat sich aufgelöst. Die Zahl der Verbindungen zu Unternehmensressourcen über öffentliche Netzwerke mittels Smartphones, Laptops und Tablets wird immer größer. Die „Consumerization“ von IT schreitet immer mehr voran und wird zur Normalität in Unternehmen. Diese Strategie wird auch „Bring-your-own-device“-Strategie genannt (was nichts anderes bedeutet, als dass Mitarbeiter ihre privaten mobilen Endgeräte auch geschäftlich nutzen). Daten sind nicht mehr auf den Mainframe begrenzbar oder durch eine Server-Farm geschützt, sondern befinden sich auf einer Vielzahl von geschäftlichen und privaten Geräten. Durch die zunehmende Nutzung von Open Source und anderer Betriebssysteme als Microsoft gestalten sich Umgebungen von Betriebssystemen immer vielfältiger. Virtualisierung und Cloud-Computing verändern die Dynamik der IT-Administration und lassen zusätzliche Sicherheitslücken entstehen. Benutzer arbeiten zusammen und nutzen neue Wege, Inhalte untereinander auszutauschen.

Technologische Neuerungen bieten Unternehmen wie auch der IT eine Reihe aufregender neuer Möglichkeiten. Aber auch Cyberkriminelle lassen sich von diesen Veränderungen inspirieren. Zugleich sinkt aber das Fachwissen auf dem Gebiet der Sicherheit, und Budgets werden hierfür gekürzt.

Laut Frost & Sullivan ist das heutige Niveau der Personalausgaben im Vergleich zu 2008 für den Bereich Informationssicherheit in vielen Ländern gleich geblieben. Das ist bemerkenswert: Innerhalb von drei Jahren ist die Zahl der Angriffsvektoren und Malware-Bedrohungen exponentiell gestiegen. Dennoch ist das Sicherheitspersonal in diesem Zeitraum nicht aufgestockt worden. Während Technologien sich verändern und Malware-Bedrohungen eskalieren, wird selbst das Halten des entsprechend geschulten Personals zu einer Herausforderung. Oftmals bleibt IT-Abteilungen nichts anderes übrig, als zu reagieren und die Risiken einzuschätzen, nachdem Benutzer die Technologie bereits angenommen haben, wie im Fall Sozialer Netzwerke und mobiler Geräte. In anderen Fällen werden Technologien von IT-Abteilungen eingeführt, bevor die Sicherheitsexperten auf dem Wissensstand sind, der notwendig wäre, um geeignete Schutzfunktionen für die Umgebung zu implementieren, wie das Beispiel Cloud-Computing zeigt (1). Mit der schnellen Entwicklung von Unternehmen können die Sicherheitsabteilungen kaum mehr mithalten, und Unternehmen tun nichts, um diese fatale Sicherheitslücke zu schließen (2).

In der Zwischenzeit breitet sich die Macht der Malware weiter aus. Viren, Würmer, Spyware und Phishing-Angriffe tauchen immer wieder neu auf, und die Risiken werden immer größer. Die Bedrohung ist weit größer als jene der Angriffe von „Script-Kiddies“. Heutige Malware-Autoren verfolgen finanzielle Ziele. Sie interessieren sich für sensible Daten, wobei der Verlust solcher Daten ein Unternehmen wegen entstehender Rechtskosten und Offenlegungsgebühren durch den Imageschaden und die Schwächung der Kundentreue in die Knie zwingen kann. Nach Jahren technischer Entwicklung und auch Fortschritten in Sachen Sicherheit kämpfen wir noch immer mit Malware. Die Welt der Cyberkriminellen kennt keine Probleme wie Fachkräftemangel, Ressourcenknappheit und fehlendes Know-how. Sie feilen ständig an ihren Strategien und Methoden, um Schwachstellen in Anwendungen Sozialer Netzwerke, mobilen Geräten, virtuellen Umgebungen und Clouds ausfindig zu machen. Sicherheitsprofis belegen dies, wenn sie benennen, was ihnen alles Kopfschmerzen bereitet. Laut einer Studie von Frost & Sullivan gehören dazu Schwachstellen in Anwendungen (73 Prozent), mobile Geräte (66 Prozent) und Angriffe durch Viren und Würmer (65 Prozent). Angriffe von Viren und Würmern stehen zwar nur an dritter Stelle, spielen aber dennoch eine zentrale Rolle, wenn es um Schwachstellen in Anwendungen oder um die Bedrohung für mobile Geräte geht.

Anti-Malware heute

Antiviren-Lösungen von gestern sind in heutigen IT-Umgebungen wirkungslos. Signaturbasierte Antiviren-Lösungen bieten am E-Mail-Gateway keinen ausreichenden Schutz vor Zero-Day-Angriffen, Rootkits, Botnets, Drive-by-Downloads, Spyware und so weiter. Heutige IT-Infrastrukturen benötigen raffinierte Anti-Malware-Lösungen von einem verlässlichen Partner, sodass für einen umfassenden Schutz der sich ständig verändernden IT-Umgebungen gesorgt ist. Firmen, die sich für eine Anti-Malware-Lösung entscheiden, investieren in ein Unternehmen – nicht einfach nur in ein Produkt.

„Wie gut eine Anti-Malware-Software ist, misst sich an der Qualität der Forschungs- und Support-Abteilungen des Anbieters. Diese bilden die Grundlage für ausgezeichnete Reaktionszeiten auf neue Bedrohungen und erstklassige Kundenbetreuung. In Unternehmensnetzwerken findet ein Wandel statt: Desktop-Lösungen werden durch mobile Lösungen, Clouds und virtuelle Ressourcen ersetzt. Diese Entwicklung muss von der Sicherheitssoftware nachvollzogen werden, damit die neuen Umgebungen geschützt werden können“, schreibt Lysa Myers, Director of Research bei West Coast Labs, in ihrem Bericht Changing Malware Threats in Corporate Networks.

Eine zukunftsfähige Lösung zu finden ist kein frommer Wunsch. Es erfordert aber eine genaue Analyse der Anbieter. Ein Anti-Malware-Anbieter sollte vorausschauend sein und die Bedrohungen im Blick haben, die durch die Entwicklung neuer Technologien entstehen. Verfügt der Anbieter über eine Forschungsabteilung, die am Puls der Zeit ist und zukünftige Bedrohungen erkennt? Setzt der Anbieter genügend Ressourcen ein, um den Cyberkriminellen immer einen Schritt voraus zu sein? „Wenn es um die Produktperformance in einer Netzwerkumgebung eines Unternehmens geht, muss Schutz mehr umfassen als nur aktuelle Malware-Erkennungsfunktionen. Ebenso wichtig sind eine zukunftsorientierte Produktforschung und eine Entwicklungsstrategie, die Bedrohungen und Trends voraussieht und dadurch einen proaktiven Netzwerkschutz gewährleistet“, meint Myers.

Doch was bedeutet das? Regel Nr. 1: Anti-Malware-Lösungen sind höchst unterschiedlich – sie sind keine Massenartikel. Sie werden von einem kostenlosen Produkt keinen kontinuierlich zuverlässigen Schutz erwarten können. Selbst kommerzielle Anbieter investieren unterschiedlich viel in ihre Forschungs- und Supportabteilungen. Auch die teuersten Lösungen garantieren nicht unbedingt kontinuierlich einen zuverlässigen Schutz. Somit wird klar, dass die Suche nach der richtigen Anti-Malware-Lösung einen ganz neuen Ansatz erfordert.

Total Cost of Protection

Bei der Wahl einer Anti-Malware-Lösung spielt nicht mehr allein der Preis eine Rolle. Wenn das so wäre, würde es überall Unternehmen geben, die geschützt wären – und zwar gut geschützt – durch kostenlose Anti-Malware-Software. Auch geht es nicht darum, einfach den marktführenden Anbieter auszuwählen. Die Tatsache, dass ein Anbieter heute marktführend ist, ist kein Garant dafür, dass seine Lösungen, die heute guten Schutz bieten, auch auf die Veränderungen von morgen eingestellt sind. Nichtsdestotrotz entscheiden sich zu viele IT-Abteilungen heute einfach für den preiswertesten Anbieter oder – schlimmer noch – aktualisieren ihre aktuellen Lösungen, ohne dabei Kosten oder Effektivität zu überprüfen. Es ist ein neuer Ansatz der Beurteilung von Anti-Malware-Lösungen nötig. Bei Kaspersky Lab nennen wir das „Total Cost of Protection“.

Die Kostenfalle meiden

Die Total Cost of Protection ist die Summe aller Kosten, die mit einer Anti-Malware-Bereitstellung in Zusammenhang stehen. Diese Kosten umfassen sämtliche Aspekte, die in Betracht gezogen werden müssen. Nur so können Sie abschätzen, was der Schutz Ihres Netzwerks und Ihrer Benutzer Sie tatsächlich kostet. Die Total Cost of Protection setzt sich aus folgenden Aspekten zusammen:

- Schutz
- Performance
- Verwaltung
- Support
- Preis

Wenn eines dieser Elemente aus der Reihe tanzt, werden sich Ihre Gesamtkosten erhöhen. Im Endeffekt würde Sie der Einsatz der Anti-Malware-Lösung mehr kosten als ihr Erwerb.

Schauen wir uns die fünf Elemente genauer an, welche die Total Cost of Protection ausmachen:

Schutz
Wie effektiv schützt diese Lösung Sie vor Malware? Hat das Unternehmen auch Lösungen im Blick, die künftige neue Technologien schützen können (wie Clouds, virtuelle Maschinen und so weiter)?
Das primäre Ziel jeder Anti-Malware-Lösung sollte sein, Ihre IT-Umgebung vor Viren, Würmern, Trojanern, Spyware und so weiter zu schützen. Die erste Frage, die Sie sich also bei der Beurteilung einer Anti-Malware-Lösung stellen sollten, ist: Bietet sie ausreichend Schutz? Leistet sie, was sie sollte?

Mangelnder oder nicht ausreichender Schutz kann folgende Gründe haben:

- Unregelmäßige Aktualisierungen, sodass Systeme neuen Bedrohungen ausgesetzt werden
- Fehlalarme, die wertvolle IT-Ressourcen in Anspruch nehmen
- Fehlerhafte Aktualisierungen, die Systeme lahmlegen
- Malware wird nicht erkannt und infiziert Systeme
- Unzureichende Entfernung von Viren aus infizierten Systemen (erfordert manuelle Bearbeitung)
- Kein Schutz für heterogene und/oder neue Technologien, was Mehrpunktlösungen notwendig macht

Eine Anti-Malware-Lösung, die keinen ausreichenden Schutz aus einem der oben genannten Gründe bietet, kann die Kosten in die Höhe treiben, die sich aus Datenverlust, verminderter Produktivität der Mitarbeiter und der Belastung der IT-Abteilung beim Neuaufsetzen des Systems ergeben. Dies sind finanzielle Verluste durch Cyber-Diebstahl, der auch dem Ruf Ihres Unternehmens schadet.

Performance

Geht bei Ihnen Schutz vor Performance?

Sicherheit sollte nicht auf Kosten der Produktivität von Endbenutzern gehen oder die Effizienz am Arbeitsplatz beeinträchtigen. Denn was nützt eine Lösung, die Endbenutzer daran hindert, ihre Arbeit zu tun? „Bloatware“, wie solche Software häufig genannt wird, nimmt so viele Systemressourcen in Anspruch, dass Mitarbeiter ihr System erst wieder sinnvoll nutzen können, wenn die Software die Überprüfung beendet hat. Stellen Sie sich vor, jeder Endbenutzer genehmigt sich bei jeder Systemüberprüfung oder Aktualisierung der Virensignaturen eine 30-minütige Kaffeepause! Systemüberprüfungen, das Herunterladen aktueller Signaturen und die Aktualisierung neuer Softwareversionen darf nicht die Produktivität und Effizienz Ihrer Mitarbeiter beeinträchtigen. Sollte dies doch der Fall sein, wird die Total Cost of Protection in die Höhe schnellen.

Verwaltung

Wie viele Mitarbeiter werden für die Verwaltung der Lösung benötigt und wie viel Zeit nimmt dies in Anspruch?

Die Verwaltungskonsole ist ein wichtiges Kaufkriterium. Wenn sich das Sicherheitssystem nur mit einer schwerfälligen, nicht einfach zu bedienenden und ressourcenhungrigen Konsole verwalten lässt, wird Ihr Unternehmen durch höhere Kosten belastet werden. Neben den vermehrten Arbeitsstunden für die Verwaltung der Lösung riskieren Sie darüber hinaus auch Sicherheitslücken, die sich aus inkonsistenten Richtlinien oder einfach Fehlern ergeben. Außerdem werden auch die Kosten für Mitarbeiterschulungen höher sein. Die Verwaltung muss simpel, einfach zu bedienen, trotzdem fein abgestuft und leistungsfähig genug sein, um die Risiken in Ihrer Umgebung minimieren zu können. Berichte sollten transparent sein und einen Überblick darüber geben, wie gut Ihre Sicherheitsvorkehrungen funktionieren.

Support

Was Sie der Support wirklich kostet

Über die Kosten für den Support wird im Kontext der Total Cost of Protection kaum gesprochen. Dabei können diese Kosten besonders schmerzhaft sein. Viele Anbieter verlangen zusätzliche Gebühren für den Support, egal, ob für Standard- oder Premiumangebote. Diese Gebühren sollten in die Berechnung der Total Cost of Protection einfließen. Aber das ist längst noch nicht alles. Schlechter Support kann zusätzliche Kosten erzeugen, zum Beispiel durch ewige Warteschleifen, lange Bearbeitungs- beziehungsweise Antwortzeiten und durch Produktivitätseinbußen, die mit allgemeinen Supportproblemen verbunden sind.

Der Support spielt eine zentrale Rolle bei der Bereitstellung der Sicherheitslösung. In einer kürzlich veröffentlichten Studie von Deloitte gaben IT-Manager an, sie würden sich Sorgen um die Sicherheit machen, da sie ihre eigenen Mitarbeiter für nicht ausreichend geschult halten (3). Das bedeutet, dass Ihr Anti-Malware-Anbieter dieses Know-how besitzen muss und es auch bereitstellen sollte.

Preis

Sind die Preise wettbewerbsfähig?

Wettbewerber in der Anti-Malware-Branche sind mittlerweile extrem aggressiv in ihrer Preisgestaltung. Zwar ist der Preis definitiv ein ausschlaggebender Faktor, er sollte aber nicht das alles entscheidende Kriterium sein. Die teuerste Software muss nicht unbedingt die beste sein, und die billigste Lösung kann zur Anhäufung indirekter Kosten führen. Wie bereits erwähnt, kann die Total Cost of Protection für Sie letztendlich höher ausfallen, wenn Sie bei der Beurteilung von Anti-Malware-Lösungen allein den Preis oder diesen an erster Stelle in Betracht ziehen.

Viele Unternehmen zahlen einen viel höheren Preis für Sicherheitslösungen, als sie geplant hatten, und erhalten nicht den Schutz, den sie benötigen.

Die Total Cost of Protection von Kaspersky Lab

Seit seiner Gründung im Jahr 1997 steht für Kaspersky Lab ein Ziel unmittelbar im Mittelpunkt: seine Kunden vor Malware-Bedrohungen zu schützen. Mit der Zeit haben viele unserer Wettbewerber ihr Augenmerk auch auf andere Bereiche gerichtet, was oftmals zu einem Qualitätsverlust ihrer Sicherheitsprodukte führt. Das engagierte Weltklasseteam von Kaspersky Lab mit mehr als 800 Anti-Malware-Forschern und Technikern sowie mehr als 2.000 internationalen Mitarbeitern widmet sich ausschließlich und unermüdlich dem Schutz vor Malware. Unser Ziel ist es, in den fünf einzelnen Bereichen, welche die Total Cost of Protection ausmachen, die branchenweit beste Lösung anzubieten. Unsere Vorteile:

- **Ausgezeichnete Malware-Erkennung**

  Unabhängige Untersuchungen haben ergeben, dass Kaspersky Lab die Liste der wichtigsten Antiviren-Lösungsanbieter (darunter auch Symantec, McAfee und CA) anführt (4). Kaspersky Lab benötigt durchschnittlich nur anderthalb Stunden, um eine Signaturdatei für einen neuen Virus zu schreiben und bereitzustellen. Im Vergleich dazu benötigen andere Anti-Malware-Unternehmen zwei bis vier Stunden. Diese Aktualisierungen werden stündlich an unsere Kunden geliefert und bieten damit den am schnellsten verfügbaren Schutz. Das Zeitfenster, in dem Ihr System Schwachstellen aufweist, wird dadurch möglichst klein gehalten, wodurch sich die Gefahr einer Infektion verringert und somit auch Ihre Total Cost of Protection niedrig gehalten werden.

  Stanley Mierzwa, Director of IT Technology bei The Population Council, beschreibt die großen Vorteile, die Kaspersky Lab bietet:

  „Sobald wir die Kaspersky-Lösung einsetzten, wurde der Unterschied sofort deutlich. Es gab weniger Infektionen, was eine sehr positive Wirkung auf alle Betriebsabläufe hatte. Sie wurden viel effizienter."

- **Hervorragende Performance**

  Kaspersky Lab bietet konsistente Performance auf höchstem Niveau und stellt somit sicher, dass Endbenutzer produktiv und geschützt bleiben. Unsere kleinen, regelmäßigen Aktualisierungen sorgen für bessere Performance und schützen kostspielige Bandbreite, besonders auch im Falle unterbrochener Remoteverbindungen. Ein zusätzliches Plus ist der geringe Speicherbedarf, der ihre Systemressourcen so wenig wie möglich belastet.

  Auch Mike Ciura, Security and Oracle Analyst bei Great Batch Inc., beschreibt die sofortigen Vorteile:

  „Mitarbeiter, die CAD und andere ressourcenintensive Produkte verwenden, haben bisher keine Probleme gemeldet. In vielen Fällen habe ich Komplimente erhalten, dass das System schneller ist und die neue Lösung im Hintergrund läuft, ohne die Arbeitsabläufe zu stören."

- **Vereinfachte Verwaltung**

  Sämtliche Produkte von Kaspersky Lab werden über eine zentrale Konsole verwaltet, wodurch der Zeitaufwand und die für die Verwaltung notwendigen Ressourcen selbst in hochkomplexen und sehr großen IT-Umgebungen von Großunternehmen sehr gering bleiben. Mit dieser einfach zu bedienenden Konsole lassen sich unternehmensweit Risiken erkennen und verwalten – auch für entfernte und mobile Geräte. Ihre Total Cost of Protection kann dadurch erheblich gesenkt werden.

  George Thornton, Network Operations Manager im Montgomery Independent School District, beschreibt, wie sich indirekte Kosten durch den Einsatz einer Kaspersky-Lösung sparen lassen:

  „Bei unserem früheren Anbieter mussten wir mehrere Konsolen verwenden. Mit Kaspersky Lab erfolgt die gesamte Verwaltung über eine zentrale Konsole. Vieles läuft automatisiert ab. Früher haben wir ein bis zwei Tage in der Woche mit der Verwaltung unserer Antiviren-Lösung verbracht. Jetzt sind es nur noch wenige Minuten pro Woche."

- **Erstklassiger Support**

  Der Standardsupport von Kaspersky Lab ist kostenlos und bietet die kürzesten Wartezeiten der Branche (weniger als fünf Minuten). Unsere First-Call-Resolution-Raten (das heißt die Rate der direkten Beantwortung von Anfragen beim ersten Kontakt) liegen bei 90 Prozent. So werden Ihre Probleme schneller gelöst, und die Zeit, in der IT-Mitarbeiter sich mit dem Problem beschäftigen müssen, wird auf ein Minimum verkürzt. Durch unseren lokalen, schnellen, effektiven und dazu kostenlosen Standardsupport verringert sich Ihre Total Cost of Protection.

  Terry Meitz, Senior Network Engineer bei Peachtree Financial, bestätigt die hohe Supportqualität von Kaspersky Lab:

  „Der Support von Kaspersky Lab war absolut phänomenal. Die Wartezeiten waren sehr kurz. Das Supportteam war sehr aufmerksam, und es hat Spaß gemacht, mit ihm zu arbeiten. Sie haben nicht nur das Problem gelöst, das Anlass unserer Anfrage war, sondern sie lösten nebenbei auch noch ein weiteres Problem, auf das wir überhaupt erst während unseres Gesprächs aufmerksam wurden."

- **Wettbewerbsfähige Preise**

  Kaspersky Lab bietet im Vergleich zu seiner Anti-Malware-Konkurrenz wettbewerbsfähige Preise und liegt preislich entweder auf demselben Niveau oder sogar darunter. Wir von Kaspersky Lab bieten Ihnen unseren besten Schutz zu einem attraktiven Preis-/Leistungsverhältnis.

  Victor Andreev, Systems Administrator im Centre for Education & Training, fasst die Total Cost of Protection folgendermaßen zusammen: „Das Angebot von Kaspersky Lab lag weit unter dem Angebot unseres damaligen teuren Anbieters. Angesichts der vielen Vorteile und des sehr guten Preises mussten wir nicht lange über einen Wechsel nachdenken."

Zusammenfassung

Unser Hauptziel ist, unseren Kunden die beste Total Cost of Protection zu bieten. Aber nicht nur heute. Unser Kerngeschäft besteht darin, die wichtigen technologischen Trends und Neuerungen und die sich dadurch eröffnenden Chancen und entstehenden Risiken zu erkennen – und schließlich Lösungen für aktuelle und zukünftige Bedrohungen bereitzustellen. Die Zukunftstauglichkeit unserer Lösungen sichern wir durch ständige Verbesserungen der Performance und Funktionalität unserer Produkte. Der Funktionsumfang wird kontinuierlich erweitert, um Daten besser schützen und verwalten zu können. Zudem erweitern wir unser Portfolio und investieren in Technologien, mit denen sich die ständig im Wandel befindlichen IT-Umgebungen unserer Kunden besser schützen lassen. Zugleich möchten wir unseren Kunden auch weiterhin die beste Total Cost of Protection bieten.

Fordern Sie Kaspersky Lab heraus!

Wir laden Sie ein, Kaspersky Lab 30 Tage lang zu testen – auf verschiedenen Plattformen wie Smartphones und anderen mobilen Geräten. Testen Sie unsere Verwaltung, die automatisierten Tools sowie unsere Berichte und Dashboards. Sehen Sie selbst, wie Sie mit Kaspersky Lab die Total Cost of Protection senken können.

Wir möchten Sie motivieren, Ihre Sicherheitsoptionen mit Ihrem Lösungsanbieter zu besprechen. Sie können uns auch gern per E-Mail an salesDACH@kaspersky.de oder telefonisch unter +49841981890 kontaktieren.

Wenn Sie sich für einen kostenlosen 30-Tage-Test interessieren, besuchen Sie bitte unsere Website unter http://www.kaspersky.de.

(1) Laut der Frost & Sullivan-Studie „Global Information Security Workforce“ (2011), gesponsert von (ISC)2, gaben 74 Prozent der weltweit befragten Experten für Informationssicherheit an, dass für Cloud-Computing neues Know-how entwickelt werden muss.

(2) 66 Prozent der Befragten geben in einer Studie von Frost & Sullivan an, dass ihr Budget für Services im Jahr 2011 keinen Anstieg verzeichnet hat. 63 Prozent berichten, dass das Budget für ausgelagerte oder verwaltete Services gleichbleibend ist.

(3) Financial Services Global Security Study (Deloitte, 2010)

(4) www.kaspersky.de/auszeichnungen

Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
Deutschland

www.kaspersky.de
E-Mail: salesdach@kaspersky.de
Telefon +49 (0) 841 98 189 0
Telefax +49 (0) 841 98 189 100

xmla

KASPERSKY lab