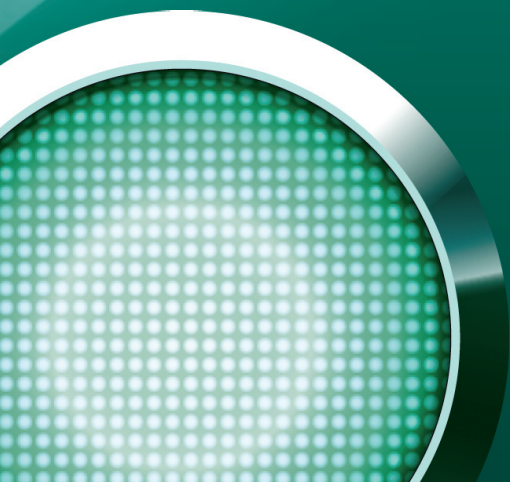




## WHITEPAPER

# Für mehr IT-Sicherheit im Mittelstand

Kaspersky Hosted Security Services



<b>1</b>	<b>IT-SICHERHEIT UND DER MITTELSTAND</b>	<b>3</b>
<b>2</b>	<b>HOSTED SECURITY SERVICES: SICHERHEIT AM PERIMETER</b>	<b>3</b>
<b>3</b>	<b>VIELFÄLTIGE VORTEILE GEGENÜBER APPLIANCES</b>	<b>4</b>
3.1	DEUTLICHE ENTLASTUNG DER IT	4
3.2	HOHES SICHERHEITSNIVEAU	5
3.3	AUSFALLSICHERHEIT UND VERFÜGBARKEIT	5
3.4	GARANTIERTE SICHERHEIT DURCH SERVICE LEVEL AGREEMENTS	5
3.5	FLEXIBLE ABBILDUNG DER EIGENEN IT-SECURITY-POLICY	5
3.6	GERINGE KOSTEN OHNE INVESTITION	6
3.7	RECHTSSICHERHEIT	7
<b>4</b>	<b>KASPERSKY HOSTED SECURITY SERVICES IM DETAIL</b>	<b>7</b>
4.1	SICHERE E-MAIL MIT MAILDEFEND	7
4.2	WEBDEFEND SCHÜTZT DEN ZUGANG ZUM INTERNET	8
4.3	WEBCONTROL FÜR DEN SCHUTZ VOR UNERWÜNSCHTEN INHALTEN	8
4.4	IMDEFEND FÜR SICHERES INSTANT MESSAGING	9
<b>5</b>	<b>ALLES UNTER KONTROLLE</b>	<b>9</b>
	<b>KASPERSKY LAB</b>	<b>9</b>

## 1 IT-Sicherheit und der Mittelstand

Anders als große Firmen haben mittelständische Unternehmen oft nicht das notwendige Know-how und die erforderlichen Ressourcen, um sich effektiv gegen die immer ausgereifteren Bedrohungen aus dem Internet abzusichern. Die Materie ist zu komplex, Security-Spezialisten sind rar und teuer, und außerdem gehört IT-Security einfach nicht zum Kerngeschäft – wodurch sie oft vernachlässigt wird. Dabei sind Mittelständler nicht nur von Viren, Würmern und trojanischen Pferden bedroht – eine im August 2007 veröffentlichte Untersuchung der Universität Siegen hat gezeigt, dass ausländische Nachrichtendienste ganz gezielt versuchen, über das Internet kleine und mittlere deutsche Unternehmen auszuspionieren. Diese Form der Wirtschaftsspionage, so ein Ergebnis der Studie, führe zu katastrophalen Schäden, da sie in den meisten Fällen die Insolvenz des betroffenen Unternehmens zur Folge habe. Die Ergebnisse der Untersuchung decken sich nach Angaben der Universität in weiten Teilen mit den Einschätzungen des Bundesamtes für Verfassungsschutz in Köln, das im Rahmen der Untersuchung kontaktiert wurde.

Betrachtet man die IT-Sicherheit aus der Sicht eines mittelständischen Unternehmens, so sind zwei völlig unterschiedliche, aber gleich wichtige Szenarien zu unterscheiden. Zum einen geht es um die Absicherung der einzelnen Systeme und Infrastrukturkomponenten innerhalb des eigenen Netzwerkes, zum anderen um den Schutz des gesamten Netzwerkes vor den Bedrohungen von außen. Die interne Sicherheit wird meist durch ausgereifte und einfach zu verwaltende Softwareprodukte wie zum Beispiel Kaspersky Work Space Security oder Kaspersky Business Space Security gewährleistet, die auf den zu schützenden Systemen wie Fileserver und Workstations installiert werden. Für den Schutz des Netzwerks vor externen Bedrohungen dagegen ist eine Gateway-Lösung erforderlich. Hier haben sich in den vergangenen Jahren auf breiter Front Appliances durchgesetzt, auf denen Virens Scanner und Spamfilter bereits vorinstalliert sind, und die ebenfalls einen unkomplizierten und reibungslosen Betrieb versprechen. Dennoch erfordert der Einsatz solcher Appliances neben den hohen Anschaffungskosten ständige Pflege und ein hohes Maß an Expertise in Sachen IT-Sicherheit, die bei vielen Mittelständlern nicht vorhanden ist. Aus diesen und anderen Gründen wird das Out-tasking der Internet Security für immer mehr mittelständische Unternehmen eine attraktive Alternative. Mit den Kaspersky Hosted Security Services bietet Kaspersky Lab eine Lösung an, die nicht nur ein höheres Sicherheitsniveau garantiert, sondern zudem noch deutlich wirtschaftlicher ist als eine Inhouse-Lösung auf Basis von Appliances. Dieses Whitepaper zeigt, wie mittelständische Unternehmen sich mit diesen Services effektiv vor den Be-

drohungen aus dem Internet schützen können, und von welchen Vorteilen sie dabei profitieren.

## 2 Hosted Security Services: Sicherheit am Perimeter

Sowohl die Qualität als auch die Quantität der Angriffe auf Unternehmensnetzwerke ist in den vergangenen Jahren ständig gestiegen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2007“ von einer anhaltend hohen Bedrohungslage der IT-Sicherheit bei Privatanwendern sowie Unternehmen und Verwaltungen. Zudem geht nach Angaben des BSI die zunehmende Virtualisierung von Geschäftsprozessen mit einer Professionalisierung und Kommerzialisierung der IT-Bedrohungen einher. Wo früher Hacker einen mehr oder weniger sportlichen Wettkampf untereinander führten, stehen heute wirtschaftliche Interessen im Vordergrund. Die massenhafte Verbreitung von E-Mail-Spam ist ein lukratives Geschäft, erfolgreiche Phishing-Attacken versprechen Zugriff auf fremde Bankkonten, und gezielte Angriffe auf die IT-Infrastruktur von Unternehmen gewinnen im Bereich der Industrie- und Wirtschaftsspionage immer weiter an Stellenwert.

Die Professionalisierung der Angreifer hat in den vergangenen Jahren auch zu einem erheblichen Wandel der Bedrohungsszenarien geführt. Es geht heute nicht mehr darum, möglichst viele PCs mit Viren oder Würmern zu infizieren, um durch ein entsprechendes Medienecho zu Ruhm und Ehre zu gelangen. Im Gegenteil: Heutige Attacken sind zumeist darauf ausgelegt, den Angriff möglichst lange verborgen zu halten und der Aufmerksamkeit der Hersteller von Antiviren-Programmen zu entgehen. Je später diese mit Signaturen auf einen neuen Schadcode reagieren, umso mehr Zeit bleibt dem Angreifer, diesen Code auf den „richtigen“, sprich lohnenden Zielen zu platzieren. Der Schutz vor Zero-Day- oder Zero-Hour-Attacken – also Angriffen mit Schadcodes, die von Antiviren-Programmen noch nicht erkannt werden – bekommt daher eine dramatisch zunehmende Bedeutung. Zwar verwenden auch Software-Produkte und Appliances heute heuristische Verfahren zur Erkennung neuer Schadcodes, doch analysieren diese naturgemäß nur einen Bruchteil der E-Mails, mit denen es ein Hosted Service zu tun hat. In den Rechenzentren der Hosted Security Services werden täglich Millionen von E-Mails aller Kunden gescannt, wodurch zum Beispiel sehr schnell erkannt wird, wenn eine E-Mail mit Anhang massenhaft über Botnetze verbreitet wird.

Aber nicht nur die Bedrohungen sind einem Wandel unterworfen – auch die Verbreitungswege und-mechanismen ändern sich. Da praktisch jedes Unternehmen Antiviren-Software einsetzt und mit

einmal bekannt gewordenen Viren verseuchte E-Mails daher sehr leicht zu filtern sind, entwickeln die Angreifer kontinuierlich neue Methoden. Zunehmende Verbreitung finden dabei Social-Engineering-Methoden, bei denen eine E-Mail ohne Schadcode verschickt wird, mit der die Empfänger auf eine Website gelockt werden sollen. Erst auf dieser Website befindet sich der schädliche Code und wird mitsamt den sichtbaren Inhalten der Seite heruntergeladen. Dabei machen sich die Angreifer die Tatsache zunutze, dass viele Unternehmen zwar ihre E-Mail-Systeme mit Antiviren-Software am Gateway oder am E-Mail-Server schützen, nicht aber ihre Web-Zugänge, die oft über ungesicherte Proxy-Server realisiert werden. In jüngerer Zeit werden zudem die immer weiter verbreiteten Instant-Messaging-Systeme zur Distribution von Malware genutzt.

Während große Organisationen und Konzerne meist eine Vielzahl von Sicherheits-Spezialisten in ihren IT-Abteilungen beschäftigen, um sich gegen diese und andere Bedrohungen zu wehren, stehen kleinere und mittelständische Unternehmen vor einem Dilemma. Einerseits ist auch ihre IT-Umgebung mittlerweile unternehmenskritisch und muss entsprechend geschützt werden, andererseits ist es unter wirtschaftlichen Gesichtspunkten nicht vertretbar, das entsprechende Know-how im Hause vorzuhalten. Security-Experten und Marktforscher gehen deswegen davon aus, dass in den kommenden Jahren immer mehr dieser Unternehmen sich externer Dienste wie der Kaspersky Hosted Security Services bedienen werden, um ihre IT effektiv gegen die Vielzahl von Bedrohungen aus dem Internet zu schützen.

### 3 Vielfältige Vorteile gegenüber Appliances

Das Prinzip der Kaspersky Hosted Security Services ist bestechend einfach: Sämtliche E-Mails, Web-Zugriffe und Instant Messages aller Mitarbeiter im Unternehmen werden über die eigens dafür aufgebauten Rechenzentren von Kaspersky Lab geleitet und bereits hier auf schädliche und unerwünschte Inhalte überprüft. Auf diese Weise werden Spam, Viren, Trojaner und andere Schadcodes bereits im Internet aus dem Datenstrom herausgefiltert und erreichen das Unternehmensnetzwerk gar nicht erst. Die Experten von Kaspersky Lab sorgen dabei rund um die Uhr dafür, dass die Sicherheitslösung immer auf dem aktuellsten Stand ist und auch neuer Bedrohungen Herr wird. Gegenüber einer Appliance-basierten Lösung, die vom Unternehmen selbst geplant, installiert und betrieben werden muss, bieten die Hosted Security Services eine Vielzahl von Vorteilen:

- (3.1) Deutliche Entlastung der IT: Betrieb und Wartung des Gesamtsystems einschließlich ständiger Aktualisierungen durch Spezialisten von Kaspersky Lab
- (3.2) Hohes Sicherheitsniveau: IT-Security-Infrastruktur eines Großunternehmens für erfolgreiche Abwehr von Spam- und Malware-Attacken
- (3.3) Ausfallsicherheit und Verfügbarkeit: Betriebsicherheit durch hochverfügbare, ausfallsicher angelegte Rechenzentren von Kaspersky
- (3.4) Garantierte Sicherheit durch Service Level Agreements: Vertraglich über SLAs abgesicherte Serviceleistungen
- (3.5) Flexible Abbildung der eigenen IT-Security-Policy: Umsetzung vorhandener Sicherheitsrichtlinien durch den Kunden selbst über einfach zu bedienendes Web-Portal
- (3.6) Geringe Kosten ohne Anfangsinvestition: Kostenreduzierung und kalkulierbare Fixkosten ohne Investitionen in zusätzliche Hardware
- (3.7) Rechtssicherheit: Strikte Einhaltung deutscher Gesetze wie Datenschutz oder Fernmeldegeheimnis

#### 3.1 Deutliche Entlastung der IT

Der augenfälligste Vorteil beim Einsatz von Hosted Security Services ist die sehr deutliche Entlastung der eigenen IT-Mitarbeiter. Die Planung, Implementierung und vor allem die Wartung einer Inhouse-Lösung auf Basis von Appliances stellt diese Mitarbeiter vor immense Herausforderungen. Nur wenige Hersteller bieten Komplettlösungen an, die alle Bedrohungsszenarien abdecken und für den Einsatz mit E-Mail, Web und Instant Messaging geeignet sind. Setzt man deshalb spezialisierte Produkte unterschiedlicher Hersteller ein, so wird im Allgemeinen ein höheres Schutzniveau erreicht, das allerdings mit einem erheblichen Integrations- und Wartungsaufwand erkaufte werden muss. Hinzu kommt die Verwaltung mehrerer Wartungs- und Update-Verträge mit verschiedenen Herstellern.

Die Vielfalt und die Dynamik der Bedrohungen aus dem Internet erfordern nicht nur den Einsatz unterschiedlichster Technologien zum Schutz der eigenen IT-Umgebung, sondern auch ein umfassendes und jederzeit tagesaktuelles Know-how sowie eine ebenso aktuelle Pflege der Systeme. Ein ansehnlicher Teil der Arbeitszeit der eigenen IT-Mitarbeiter muss daher für Fortbildungsmaßnahmen und die ständige Beobachtung der Sicherheits- und Bedrohungslage sowie für die Installation von Updates und Patches aufgewendet werden. Auf

Grund der Ressourcenknappheit können dies nur wenige mittelständische Unternehmen leisten.

Die Kaspersky Hosted Security Services entlasten die IT-Abteilung von all diesen Tätigkeiten und erlauben es ihr, sich stattdessen wieder auf die strategischen Aspekte der IT und der IT-Security zu konzentrieren. Das Unternehmen eliminiert sämtliche Probleme hinsichtlich der Integration, des Betriebs und der Verwaltung der technischen Infrastruktur, da diese komplett von Kaspersky zur Verfügung gestellt wird.

### 3.2 Hohes Sicherheitsniveau

Als spezialisierter Anbieter von Sicherheitslösungen kann Kaspersky Lab im Rahmen seiner Services alle verfügbaren Technologien zur Absicherung von E-Mail, Web und Instant Messaging einsetzen und integrieren. Über seine Rechenzentren stellt Kaspersky Lab daher auch dem Mittelstand eine IT-Security-Infrastruktur zur Verfügung, die bisher Großunternehmen vorbehalten war. So werden neben den eigenen, vielfach preisgekrönten Lösungen von Kaspersky Lab auch weitere Softwareprodukte eingesetzt, um höchstmögliche Sicherheit zu garantieren. Zudem profitieren alle Services von BitHunt, einer proprietären Heuristik-Engine, die täglich Millionen von E-Mails nach bestimmten Charakteristika und Trends analysiert und klassifiziert. Damit ermöglicht diese Technologie auch die Erkennung von Zero-Day-Attacken, die von einem autonomen Appliance-Programm noch nicht identifiziert werden können. Die proprietäre Natur dieser Technologie hat zudem den Vorteil, dass die Autoren von Malware ihre „Produkte“ nicht gegen BitHunt testen und entsprechend optimieren können.

### 3.3 Ausfallsicherheit und Verfügbarkeit

Was nützt die beste Sicherheitslösung, wenn sie nicht verfügbar ist? Interne Lösungen basieren oft auf einzelnen Appliances am Gateway, die den Datenverkehr filtern und analysieren. Diese Appliances bilden dann einen „Single Point of Failure“, also einen kritischen Punkt, dessen Ausfall die Verfügbarkeit der gesamten Lösung beeinträchtigt. Üblicherweise werden solche Lösungen so konfiguriert, dass bei Ausfall der Appliance der entsprechende Dienst (etwa E-Mail) gar nicht mehr zur Verfügung steht. Dahinter steht der Gedanke, dass ein zeitweiser Verzicht auf den Dienst eher tolerierbar ist als der ungesicherte Betrieb. Dennoch erfordert die Bedeutung der elektronischen Kommunikation im heutigen Geschäftsleben, dass solche Ausfälle auf ein absolutes Minimum reduziert werden.

Im Gegensatz zu Appliance-basierten Lösungen gibt es bei Hosted Security Services keinen Single Point of Failure. Die gesamte IT-Architektur in den Rechenzentren von Kaspersky Lab ist redundant

ausgelegt, und selbst im Falle einer Katastrophe können die verbliebenen Rechenzentren die Arbeit eines ausgefallenen Operations Center unverzüglich übernehmen. Anders als im Unternehmen steht zudem rund um die Uhr qualifiziertes Personal bereit, um eventuell auftretende Probleme unverzüglich zu lösen. So ist Kaspersky Lab in der Lage, für seine Hosted Security Services eine Verfügbarkeit von 99,999 Prozent zu garantieren – entsprechend einer Ausfallzeit von maximal etwa 5 Minuten im Jahr. Eine derart hohe Verfügbarkeit ist im Unternehmen selbst mit redundanter Auslegung von Appliances praktisch nicht zu realisieren.

Selbst einen Ausfall des Mailservers beim Kunden können die Kaspersky Hosted Security Services kompensieren. Können Mails nicht mehr an diesen Mailserver weitergeleitet werden, werden sie bis zu sieben Tage im Operations Center gespeichert und nach Wiederherstellung des Mailservers weitergeleitet

### 3.4 Garantierte Sicherheit durch Service Level Agreements

Trotz hoher Investitionen in Mensch und Technik kann die IT-Abteilung im mittelständischen Unternehmen nur schwerlich Garantien für die Sicherheit übernehmen – zu komplex sind die Bedrohungen, zu vielfältig die Aufgaben und zu knapp die Ressourcen. Auch die Hersteller von Appliances werden solche Garantien nicht geben, zumal sie ja keine Kontrolle über ihre Produkte beim Kunden haben. Kaspersky Lab dagegen bietet für die Hosted Security Services solche Garantien an. Diese werden in Service Level Agreements mit den Kunden festgeschrieben, wobei ein Unterschreiten der vereinbarten Service Level auch sanktioniert wird.

Im Einzelnen garantiert Kaspersky Lab für seine Hosted Security Services:

- Verfügbarkeit von 99,999 Prozent; entsprechend maximal etwa 5 Minuten Ausfallzeit pro Jahr
- 100-prozentige Freiheit von Viren, für die Kaspersky Lab seit mindestens 30 Minuten über eine Signatur verfügt
- Eine Spam-Erkennungsrate von mindestens 95 Prozent

### 3.5 Flexible Abbildung der eigenen IT-Security-Policy

Kein Unternehmen gleicht dem anderen, und auch die Vorstellungen von IT-Sicherheit variieren deutlich. Deswegen bietet Kaspersky Lab für die Hosted Security Services ein einfach zu benutzendes Web-Portal an, über das jeder Kunde seine Services selbst konfigurieren und seine vorhandenen Sicherheitsrichtlinien umsetzen kann. So kann beispielsweise

se jeder Kunde selbst entscheiden, wie er Spam behandeln möchte, ob er virenverseuchte Attachments löschen oder in Quarantäne stellen will oder welche Art von Websites für den Zugriff gesperrt werden sollen. Auf diese Weise ist sichergestellt, dass trotz der standardisierten Infrastruktur der Kunde jederzeit Herr seiner individuellen Lösung ist.

Anders als bei vielen Appliances steht die gesamte Management-Oberfläche der Kaspersky Hosted Security Services in deutscher Sprache zur Verfügung.

### 3.6 Geringe Kosten ohne Investition

Bei der Entscheidung, ob man mit einer oder mehreren Appliances eine eigene Sicherheitslösung aufbauen oder einen Hosted Service nutzen möchte, spielen natürlich auch betriebswirtschaftliche Aspekte eine wesentliche Rolle. Bei der Implementierung einer Inhouse-Lösung sind im Voraus erhebliche Investitionen in die Hardware und in die Softwarelizenzen erforderlich. Hinzu kommen Kosten für die Einstellung bzw. Schulung von Mitarbeitern und anschließend für die Implementierung, Integration und Wartung.

Um sicherzustellen, dass der Schutz auf Dauer so effektiv wie am Tag der Implementierung bleibt, müssen Unternehmen bei einer Inhouse-Lösung jährliche Softwarelizenzgebühren entrichten, die Kompetenzen ihrer Mitarbeiter pflegen und weiterhin in Zusatzprodukte investieren. Für die Kaspersky Hosted Security Services fällt hingegen eine von der Anzahl der abgesicherten Arbeitsplätze abhängige Jahresgebühr an, die komplett als Betriebsausgabe behandelt werden kann. Zusätzliche laufende Kosten etwa für Wartung, Reparaturen oder Ersatzinvestiti-

onen fallen nicht an, so dass auch ein hohes Maß an Planungssicherheit entsteht. Zudem skalieren die Services wesentlich besser als Appliances. Müssen zusätzliche Arbeitsplätze abgesichert werden, erfordert dies lediglich eine Anpassung der Lizenz. Bei Hardware-Lösungen hingegen ist unter Umständen die Anschaffung einer weiteren Appliance erforderlich, die dann auch noch in die Gesamtlösung integriert werden muss.

Neben diesen direkten Ausgaben gibt es noch zahlreiche weniger offensichtliche Kosten, die mit dem Betrieb einer Internet-Sicherheitslösung verbunden sind. So bedeutet die Nutzung einer Inhouse-Lösung etwa, dass Spam-Nachrichten und Viren erst innerhalb des Unternehmensnetzes herausgefiltert werden können. Da Spam alleine in den meisten Unternehmen über 70 Prozent aller E-Mails ausmacht, kann dies Zusatzkosten für höhere Bandbreiten, zusätzliche Verarbeitungsleistung und Speicherplatz nach sich ziehen. Werden unerwünschte Nachrichten herausgefiltert, bevor sie das Unternehmensnetzwerk erreichen, ermöglicht dies ein erhebliches Einsparungspotenzial. Durch das höhere Sicherheitsniveau sinkt zudem die Zahl sicherheitsrelevanter Zwischenfälle, die üblicherweise ein zeit- und damit kostenintensives Eingreifen der IT-Abteilung und des Benutzer-Supports erfordern.

Beispielrechnungen ergeben, dass ein Unternehmen mit 200 Anwendern allein durch die Absicherung des E-Mail-Verkehrs über den Service mailDefend von Kaspersky Lab etwa 8.000 bis 10.000 Euro pro Jahr einsparen kann.

### Vergleich der Kaspersky Hosted Security Services mit Security-Appliances

	Appliance	Kaspersky Hosted Security Services
Implementierungszeit	mittel bis lang	sehr kurz
Total Cost of Ownership	mittel bis hoch	niedrig
Berichtswesen	schlecht bis gut	sehr gut
24-Stunden-Support	gegen Zusatzkosten	ja
Garantierte Ergebnisse	nein	ja
Kompatibel mit bestehender IT	unsicher	ja
Investition erforderlich	ja	nein; nur laufende Kosten
Sicherheitsniveau	hoch	sehr hoch
Prozessbasierte Sicherheit	meist nein	ja
Kundenspezifische Lösung	nein	nein
Entlastung des Gateways	nein	ja
Schutz vor DoS-Attacken	nein	ja
Skalierbar	schlecht	sehr einfach
Spezialisten erforderlich	ja	nein

### 3.7 Rechtssicherheit

Für das Management vieler mittelständischer Unternehmen ist IT-Sicherheit lediglich ein technisches Problem, um das sich die Spezialisten kümmern sollen. Dabei gibt es einen weiteren Aspekt, der unmittelbar vom Management zu adressieren ist: Viele Maßnahmen zur Sicherstellung der IT-Sicherheit tangieren wesentliche rechtliche Fragen. So berührt das Filtern von E-Mails oder Instant Messages grundsätzlich geschützte Rechte der Mitarbeiter (Datenschutz, Fernmeldegeheimnis). Auch die gesetzlichen Regelungen zur Veränderung oder Unterdrückung von Nachrichten sind zu beachten – andernfalls droht der Unternehmensführung sogar eine strafrechtliche Verfolgung. Eine Lösung auf Basis von Appliances so zu planen und zu konfigurieren, dass alle gesetzlichen Bestimmungen eingehalten und die Rechte der Mitarbeiter gewahrt werden, ist nicht trivial und erfordert in jedem Falle die Einbeziehung kompetenter Juristen. Die Kaspersky Hosted Security Services berücksichtigen von Haus aus die deutsche Rechtslage und können daher sehr einfach rechtssicher eingerichtet werden. Trotzdem empfiehlt Kaspersky Lab, vor dem Einsatz seiner Services juristischen Rat einzuholen.

## 4 Kaspersky Hosted Security Services im Detail

Die Kaspersky Hosted Security Services schützen die wichtigsten Kommunikationsdienste im Internet, die in Unternehmen täglich genutzt werden:

- E-Mail
- Web-Zugang
- Instant Messaging

Dabei bieten sie einen umfassenden Schutz gegen alle Bedrohungen, denen diese Dienste ausgesetzt sind, wie:

- Befall durch Viren oder anderen Schadcode
- Ausspähung durch Trojaner
- Spam
- Phishing-Attacken
- Versand vertraulicher Daten durch Mitarbeiter

### 4.1 Sichere E-Mail mit mailDefend

mailDefend ist der Kaspersky-Service für die Absicherung des gesamten E-Mail-Verkehrs eines Unternehmens. Der Dienst basiert auf der populären

Sicherheitssoftware von Kaspersky Lab, die seit über 10 Jahren konsequent fortentwickelt wird und heute zu den am weitesten verbreiteten Sicherheitsprodukten gehört. Zudem werden auch weitere Softwareprodukte eingesetzt, um das Sicherheitsniveau weiter zu erhöhen. Der Service stützt sich ferner auf die Expertise des multinationalen Viren-Forschungsteams unter der Leitung von Eugene Kaspersky, der weltweit als einer der führenden Spezialisten im Bereich der Virenforschung gilt.

mailDefend besteht aus den Komponenten mailDefend AV (Anti-Virus) zur Erkennung und Filterung schädlicher Codes und mailDefend AS (Anti-Spam), das die Postfächer der Anwender vor der Flut unerwünschter Nachrichten schützt. Beide Komponenten arbeiten in den Datenzentren von Kaspersky Lab eng zusammen und sind für den Anwender völlig transparent. Administratoren können mailDefend über das Kaspersky Hosted Security-Web-Portal einfach konfigurieren und dabei die Sicherheitsrichtlinien des Unternehmens uneingeschränkt umsetzen.

Das Funktionsprinzip von mailDefend ist denkbar einfach. Alle eingehenden und optional auch alle ausgehenden E-Mails werden im Datenzentrum analysiert und klassifiziert. Legitime Mails, also solche, die weder Schadsoftware enthalten noch als Spam eingestuft wurden, werden daraufhin mit minimaler Verzögerung im Sekundenbereich an den vorgesehenen Empfänger weitergeleitet.

Enthält eine Mail dagegen schädlichen Code, so wird sie in der Regel – und abhängig von der Sicherheitsrichtlinie des Kunden – gelöscht oder in einem nur für Administratoren zugänglichen Bereich auf den Systemen im Datenzentrum gespeichert. So werden unerfahrene Endanwender wirksam vor Schadsoftware geschützt. Dabei steht mit BitHunt eine Technologie zur Verfügung, die durch heuristische Verfahren auch Zero-Hour-Viren erkennen und verdächtige Mails solange zurückhalten kann, bis eine Signatur für den neuen Virus existiert.

Während Schadsoftware mit sehr großer Sicherheit als solche erkannt werden kann, ist Spam schwerer zu fassen. Viele Nachrichten wie beispielsweise Newsletter, die für einen Empfänger Spam darstellen, enthalten für den anderen wichtige Informationen. Eine eindeutige Klassifizierung kann daher bei Spam nicht immer vorgenommen werden. Um trotzdem eine möglichst akkurate Einstufung vornehmen zu können, setzt mailDefend auf die Kombination aller heute verfügbaren Verfahren zur Spam-Erkennung. Zudem kann der Administrator eine Black- und eine Whitelist mit Domains anlegen, von denen keine bzw. alle Mails angenommen werden. Nachdem eine E-Mail alle eingesetzten Filtertechniken durchlaufen hat, wird ihr eine Spam-Wahrscheinlichkeit zugeschrieben.

Wird eine eingehende E-Mail als Spam klassifiziert, kann sie markiert und weitergeleitet, gelöscht, oder aber in den persönlichen Quarantäne-Ordner des vorgesehenen Empfängers verschoben werden. Dieser Quarantäne-Ordner liegt auf den Systemen im Datenzentrum und ist ausschließlich für den jeweiligen Mitarbeiter zugänglich, der über konfigurierbare Berichte auch regelmäßig über den Inhalt seines Quarantäne-Ordners informiert wird. So ist sichergestellt, dass Spam-Mails das Unternehmensnetzwerk gar nicht erst erreichen, legitime E-Mails, die fälschlich als Spam klassifiziert wurden (False Positives), aber nicht verloren gehen. Erst nach Ablauf einer vom Administrator vorzugebenden Aufbewahrungszeit, meist 30 bis 60 Tage, werden die Nachrichten automatisch aus dem Quarantäne-Ordner gelöscht.

Die Einrichtung von mailDefend ist völlig problemlos und kann von jedem erfahrenen Administrator innerhalb weniger Minuten durchgeführt werden. Es müssen lediglich die MX-Records der eigenen Domain im DNS so modifiziert werden, dass sie auf die Datenzentren von Kaspersky Lab zeigen.

### 4.2 webDefend schützt den Zugang zum Internet

Ähnlich wie mailDefend AV das Unternehmen vor E-Mail-Viren schützt, sichert der Service webDefend den oft vernachlässigten Zugang zum Internet ab, der in vielen Unternehmen über ungesicherte Proxy-Server erfolgt. Auch webDefend agiert als Proxy, d.h. alle Seitenaufrufe der Mitarbeiter im Unternehmen werden zunächst an die Systeme im Kaspersky-Datenzentrum geleitet. Hier werden nun stellvertretend die entsprechenden Webseiten abgerufen. Dabei wird der Datenstrom einschließlich sämtlicher heruntergeladener Skripte, Dateien oder Makros auf schädlichen Code und Spyware hin überprüft, bevor er an den Mitarbeiter im Unternehmen weitergeleitet wird. Lediglich Streaming-Media-Inhalte und verschlüsselter Datenverkehr (HTTPS/SSL) können nicht gescannt werden. Für die Anwender ist das gesamte Verfahren völlig transparent, und die Verzögerung durch Umleitung und Scan bewegt sich im Bereich von Millisekunden, ist also praktisch nicht spürbar.

Der Administrator hat die Möglichkeit, User-Messages zu definieren, um den Benutzer darüber zu informieren, wenn ein Virus oder Spyware entdeckt wurde.

### 4.3 webControl für den Schutz vor unerwünschten Inhalten

Der Service webControl bietet dem Unternehmen die Möglichkeit, den Zugang zum Internet einzuschränken und den Zugriff auf unerwünschte Websites und Inhalte zu verhindern. Über das Service-Portal kann

der Administrator Kategorien von Websites sowie Inhaltsarten auswählen, auf die nicht zugegriffen werden darf. Alternativ kann der Webzugang auch auf die in einer Positivliste verzeichneten Websites beschränkt werden. Dabei besteht die Möglichkeit, Benutzergruppen anzulegen, für die jeweils eigene Zugriffsrichtlinien definiert werden können.

Wenn ein Benutzer eine Webseite oder einen Anhang aufruft, für die bzw. den eine Zugangsbeschränkungsrichtlinie gilt, wird der Zugriff auf diese Webseite oder diesen Anhang verweigert, und dem Benutzer wird eine automatische Warn-Webseite angezeigt oder eine Warn-E-Mail zugesendet.

Zusätzlich zur Beschränkung von Kategorien und Inhaltsarten ermöglicht webControl auch die Einführung von Zeitplänen sowie von Quoten für ein- und ausgehenden Verkehr.

### 4.4 imDefend für sicheres Instant Messaging

Ähnlich wie webDefend arbeitet imDefend als Proxy für die im Unternehmen genutzten Instant-Messaging-Dienste. Auch hier wird der gesamte Verkehr über die Operations Center von Kaspersky Lab geleitet, wo Viren und Spyware herausgefiltert werden. Zusätzlich ist es möglich, Wörterbücher oder Wortlisten zu erstellen, um Nachrichten zu blockieren, in denen ein darin enthaltenes Schlagwort vorkommt. Der Administrator hat die Möglichkeit, User-Messages zu definieren, um den Benutzer darüber zu informieren, wenn ein Virus oder Spyware entdeckt wurde.

Möchte ein Unternehmen nur bestimmte IM-Anwendungen zulassen, können unerwünschte Applikationen gesperrt werden. Dies gilt auch für Add-on-Services wie z.B. Video, Spiele oder Sprache sowie für den Internet-Telefoniedienst Skype.

Auch imDefend ermöglicht dem Administrator, unterschiedliche Richtlinien für bestimmte Benutzergruppen einzurichten, um so verschiedene Policies umzusetzen.

## 5 Alles unter Kontrolle

Für alle Kaspersky Hosted Security Services gilt der Grundsatz, dass – trotz Outtasking – der Kunde die Kontrolle über seine Sicherheitsrichtlinien hat. Über das Service-Portal hat der Administrator jederzeit die Möglichkeit, selber neue Richtlinien umzusetzen oder bestehende zu modifizieren. Zu allen Services bietet Kaspersky Lab eine Vielzahl von Berichten mit unterschiedlichen Detaillierungsgraden, die automatisiert erstellt und dem Administrator in der von ihm gewünschten Frequenz per E-Mail zugestellt werden. Dabei kann er zwischen verschiedenen Formaten wählen, darunter Grafik, XML, PDF, CSV oder Tabellenformate.

Die Berichte geben dem Administrator unter anderem Auskunft über geblockte E-Mails, aufgetretene Viren und Spyware, Phishing-Versuche etc. Sie können auf einzelne Domains, Benutzergruppen oder Benutzer heruntergebrochen werden und beliebig einstellbare Zeiträume umfassen. Für den Administrator sind sie damit auch ein ideales Instrument zur Kontrolle, ob die in den SLAs garantierten Service Level eingehalten wurden.

### 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

www.hostedsecurity.de