next business-IT WHITEPAPER
Wissen & Services für Unternehmen

ADVANCED

Powered by:
KASPERSKY lab

DYNAMIC INFRASTRUCTURE WWW.NEXTBUSINESS-IT.DE

IT-Security in kleinen und mittelständischen Unternehmen
Mit passgenauer Sicherheitslösung gegen aktuelle und künftige Bedrohungen

Aus dem Entwickeln und Verbreiten von Schadsoftware ist längst ein eigenständiger Wirtschaftszweig geworden. Hier wird mit krimineller Energie agiert, denn heute geht es nicht mehr hauptsächlich darum, Endgeräte mehr oder weniger zweckfrei lahmzulegen oder Netzwerke nur zu blockieren. Im Gegenteil: Je intelligenter und nutzenorientierter Programme wie Trojaner, Spionagesoftware und Viren sind, desto größer ist der wirtschaftliche Nutzen – sowohl für den „Erfinder“ als auch für den „Wiederverkäufer“.

Bei den Angriffen muss man zwischen Rundumschlägen, bei denen ein großer Pool von Adressaten mit Schadsoftware „beschossen“ wird, und zielgerichteten Angriffen auf einzelne Unternehmen unterscheiden. Dabei werden nicht nur Arbeitsplatz-Computer und Unternehmensnetzwerke ins Visier genommen, auch die Angriffe auf mobile Endgeräte nehmen immer mehr zu.

Das Ziel ist aber immer dasselbe:

- wirtschaftlich nutzbare Informationen abgreifen, um sie anschließend zu verkaufen;
- Daten manipulieren, um in den Unternehmen Schaden hervorzurufen;
- Kommunikation abhören, um an Geschäftsgeheimnisse heranzukommen.

Es geht also schlichtweg darum, Geld zu verdienen.

Videozitat

Christian Funk, Senior Virus Analyst, Global Research & Analysis Team Kaspersky Lab Deutschland, erläutert die derzeitige IT-Bedrohungslage und nennt die Hauptziele von Angriffen.

Kleine und mittlere Unternehmen (KMU) sind hierfür mittlerweile bevorzugte Ziele. Die Gründe dafür sind leicht nachvollziehbar: KMU sind in ihren Branchen innovativ, verfügen daher oft über wirtschaftlich sehr interessante Informationen und Geschäftsgeheimnisse. KMU aus Industrie und Dienstleistung arbeiten oft mit Großunternehmen zusammen und sind mit diesen nicht nur im eigentlichen Geschäft, sondern auch über die IT vernetzt. IT-Verantwortliche dieser Unternehmen können aber aufgrund ihrer personellen Ressourcen die IT-Security in der Regel nicht zu einem eigenständigen Thema mit höchster Priorität machen.

Hinzu kommt, dass die technologische Komplexität der IT auch in KMU durch Virtualisierung, Mobility und Cloud Computing weiter ansteigt. Auch die finanziellen Ressourcen von KMU sind begrenzt und müssen im Kerngeschäft verfügbar sein. Die Anfälligkeit der IT von KMU gegenüber kriminellen Übergriffen ist aufgrund dieser Faktoren wesentlich stärker gegeben, als dies bei Großunternehmen der Fall ist. Deren IT-Abteilung verfügt in der Regel sowohl über eigene Spezialisten in Sachen Sicherheit als auch über höhere finanzielle Mittel. Hinzu kommt die Tatsache, dass es gerade in mittelständischen Unternehmen mitunter auch am Bewusstsein für die Notwendigkeit einer verlässlichen IT-Security über den bloßen AV-Schutz hinaus fehlt.

Der Ansatz der Kaspersky Endpoint Security for Business mit dem flexiblen Lizenzmodell, der komplett eigenen Entwicklung aller Lösungsbestandteile und dem Ziel der umfassenden IT-Transparenz mithilfe eines zentralen Dashboards bietet KMU

- passgenaue Sicherheit,
- Integrität der eingesetzten Lösung,
- zentrale, einheitliche und einfache Verwaltung.

» IT-Sicherheit – Wo liegen die Risiken?

Wenn man über die IT-Sicherheit und den Daten- bzw. Know-how-Schutz spricht, muss man nicht sehr weit schauen, um den ersten „Risikofaktor“ zu entdecken: Das sind in erster Linie die Mitarbeiter, die mithilfe von IT ihr Tagesgeschäft erledigen.

Dabei sind in der Regel nicht einmal böse Absichten zu unterstellen. Es ist die Komplexität der IT, der Anwendungen und – nicht zuletzt – der möglichen „Angriffswerkzeuge“, die das Erkennen und Ausschalten von Bedrohungen so schwierig macht. Der Angreifer versteckt sich hinter falschen Identitäten beim Versenden von E-Mails, hinter gefälschten Websites, um Zugangsdaten abzugreifen, und hinter scheinbar seriösen digitalen Angeboten, die einen in Fallen locken, in die man schon mit einem Mausklick geraten kann, ohne es überhaupt zu bemerken. Auch die Mobilität der Menschen und Daten im Zeitalter von Smartphone, Tablet und Co. nimmt weiter zu und mit ihr natürlich die Chance, dass Daten in falsche Hände geraten können – sei es durch Verlust oder durch Diebstahl des entsprechenden Geräts.

Das Bewusstsein für die möglichen Gefahren und das Wissen darum, was man tut und was nicht, hat also schon eine große Bedeutung für den Bestand der Sicherheit im IT-Umfeld. Nur wer um die Gefahren weiß, kann bewusst Maßnahmen gegen sie ergreifen. Das ist nichts anderes als das Tragen eines Helms, das Anlegen eines Sicherheitsgurts oder das professionelle Sichern des Hauses gegen Einbruch und Diebstahl.

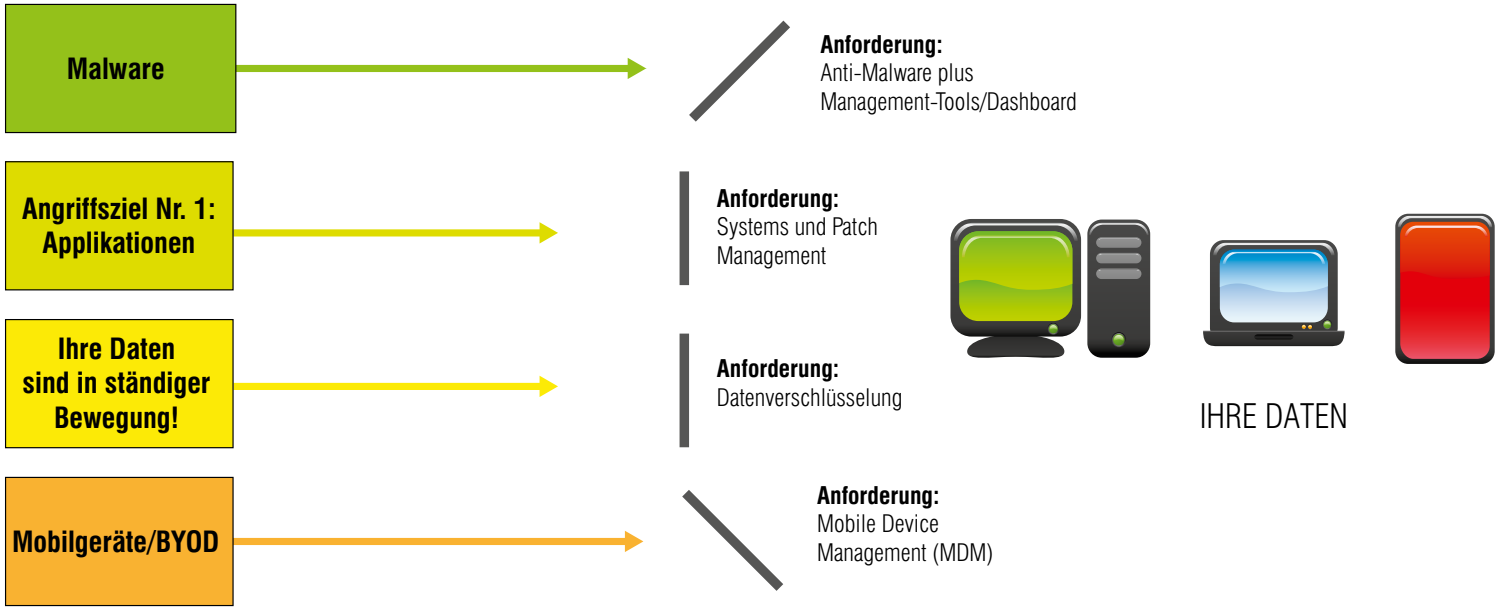
Bewusst Maßnahmen ergreifen heißt unter anderem:

- Mailanhänge unbekannter Herkunft nicht öffnen
- Links in Mails und auf Websites nicht ungeprüft anklicken
- USB-Sticks, mobile Festplatten oder andere Datenträger nicht ungeprüft mit der Unternehmens-IT verbinden
- mobile und stationäre Endgeräte durch komplexe Zugangsdaten schützen

Neben dem technischen und weitestgehend automatisierten Schutz der IT gegen Angriffe von außen ist deshalb die Schulung der Mitarbeiter hinsichtlich der Verhaltensweisen bereits ein wichtiger Faktor, mit dem man Schäden vorbeugen kann.

Niemandem ist es möglich, alle Gefahren selbst zu erkennen und zu bannen, wie aufmerksam und wachsam er auch sein mag. Die Komplexität der heutigen IT bietet nicht nur seriösen Unternehmen wirksame Unterstützung im Wertschöpfungsprozess. Im Rahmen dieser Komplexität und der allumfassenden Nutzung von IT werden deshalb durchaus auch raffinierte Methoden eingesetzt, um

Herausforderungen an die IT-Sicherheit



Durch den immer umfassenderen orts- und zeitunabhängigen IT-Einsatz und den Datenzugriff über das Internet wird auch die Abwehr von Risiken komplexer. Einzellösungen hinterlassen Lücken im Schirm.

trotz Wachsamkeit und Vorsicht illegal an Daten, Identitäten und Know-how zu kommen.

» Angreifer wollen Geld verdienen

Die größte Gefahr geht dabei von sogenannter Malware aus, die auf den oben beschriebenen Wegen, oft in Form eines Trojaners, auf das mobile Endgerät, den Arbeitsplatz-Computer oder gar in den zentralen Speicher des Unternehmensnetzwerks gelangt. Trojaner verstecken sich meist in vermeintlich nützlicher, in der Regel kostenlos angebotener Software, in per Mail zugesandten Dokumenten oder auf Websites, deren alleiniger Besuch je nach Systemkonfiguration schon für eine Infektion ausreichen kann.

Die Aufgabe des Trojaners ist das unbemerkte Herunterladen und Installieren weiterer für den Angreifer „nützlicher“ Programme. Mit diesen kann er beispielsweise unbemerkt Tastatureingaben überwachen, auf den Desktop zugreifen, Dateien direkt kopieren oder an die IT angebundene Geräte wie Kameras, Produktionsanlagen oder Kommunikationssystem manipulieren beziehungsweise steuern. Auch der Einsatz der befallenen IT für eigene Zwecke wie Spamversand über „mitgebrachte“ E-Mail-Systeme und somit die weitere Verbreitung der Schadsoftware sind typische Ziele der Angreifer. Für diesen Zweck können über das Internet auch befallene Geräte bei „Bedarf“ zu weltweiten Netzen (Bot-Netzen) zusammengeschaltet und zentral gesteuert werden.

Man muss sich dabei vor Augen halten, dass es immer um ein Ziel geht: Geld verdienen. Entweder geschieht das beispielsweise mithilfe des erbeuteten Know-hows und dessen Verkauf oder über die Erledigung von Aufträgen Dritter mithilfe der fremd beherrschten IT beziehungsweise durch Nutzung derer Kapazitäten wie Rechenpower und Internetbandbreite.

» Kleine und mittlere Unternehmen im Fadenkreuz?

KMU, zum Beispiel aus den Bereichen Industrie, Forschung, Entwicklung und Dienstleistung, sind für diese Zwecke attraktive Ziele. Diese Unternehmen sind gut in der gesamten Wirtschaft vernetzt. Einerseits in Richtung auftraggebender Großindustrie, die international tätig ist, IT durchgängig einsetzt, diese aber in der Regel mit viel Aufwand schützt. Andererseits beispielsweise in Richtung lokaler Handwerksunternehmen, die oft mit an

Videozitat

Dipl.-Oec. Patrick Grüttner, Channel Account Manager bei Kaspersky Lab, erläutert den Bedarf an integrierten Sicherheitslösungen speziell in KMU.

Bord geholt werden, wenn es um die Anfertigung von Modellen, Prototypen oder Kleinserien in der Vorproduktionsphase etc. geht.

Oft finden sich gerade hier Schwachstellen im Schutz der IT vor Viren, Spionageprogrammen und unsachgemäßem oder gar unbefugtem direktem Zugriff über Schnittstellen. Und natürlich spielt auch hier bereits die Komplexität der IT selbst bereits eine Rolle, denn viele kleine Unternehmen setzen auf serverbasierte Netzwerke, teilweise bereits auch auf Virtualisierung und Cloud Computing. Da wird die Security zur Herausforderung, die sich mit einem Virenscanner allein nicht mehr professionell bewältigen lässt.

IT-Leistung versus IT-Sicherheit?

Ein wesentlicher Faktor ist hier auch die Belastung des IT-Verantwortlichen durch sein Tagesgeschäft. Seine Aufgabe besteht darin, mithilfe der Unternehmens-IT die Wertschöpfungsprozesse zu unterstützen. Innovation ist gefragt. Themen wie Virtualisierung und Cloud Computing stehen im Rahmen der Modernisierung der IT auch in kleinen Unternehmen an. Da können sicherheitsrelevante Themen wie Schutz und Management mobiler Endgeräte, Patch Management von Betriebssystemen und Anwendungssoftware aus Zeitmangel schnell ins Hintertreffen geraten.

Die Antwort von Kaspersky Lab

Das Problem der Komplexität in der IT wird noch präsenter, wenn verschiedene IT-Risiken wie

- Angriffsschutz,
- Virenschutz,
- Datenverschlüsselung,
- Endgerätemanagement,
- Diebstahlschutz

mit unterschiedlichen, spezialisierten Lösungen adressiert werden. Bestenfalls sind diese Lösungen miteinander verbunden, schlimmstenfalls sind sie nicht miteinander kompatibel. Für IT-Administratoren bedeutet dies, dass sie von einem Dashboard zum nächsten wechseln müssen, um Richtlinien umzusetzen, den Status von Endpunkten zu prüfen und Programme mit Patches zu aktualisieren – sozusagen „Handarbeit“. Dadurch kann es leicht zu Sicherheitslücken kommen.

Kaspersky Endpoint Security for Business ist eine neue Herangehensweise.

Auf einen Blick

Vorteile von Kaspersky Endpoint Security for Business

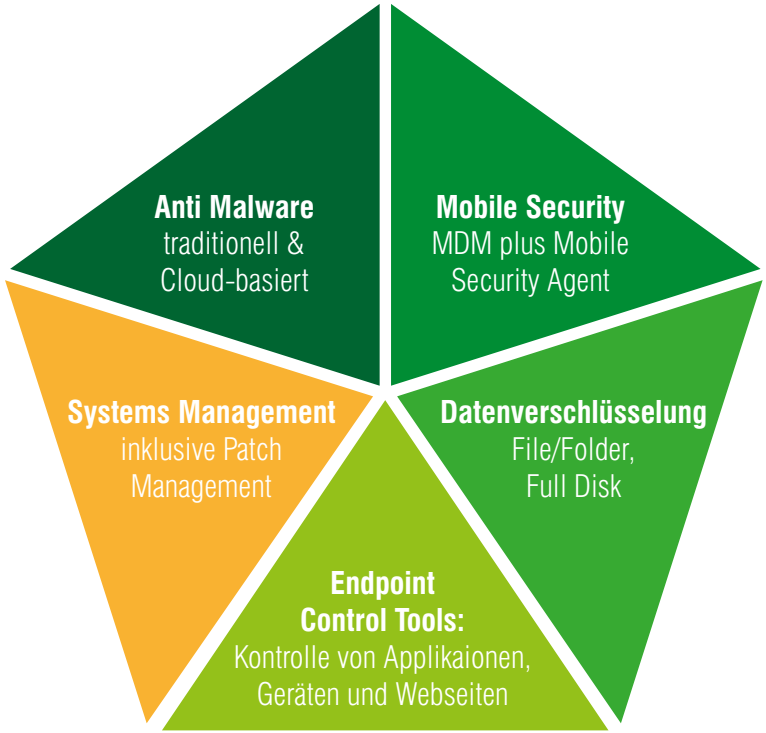
- Anti-Malware
- Datenverschlüsselung
- Sicherheit und Verwaltung mobiler Geräte
- Kontrolle von Programmen, Geräten und Webseiten
- Systems Management und Patch Management
- Alles aus Kaspersky-eigener Entwicklung (keine „Integration von Fremdprodukten“)
- Dynamische Weiterentwicklung
- Vier Lizenzmodelle für den passgenauen Einsatz nach Bedarf

Die Lösung überwindet bestehende Standards und Einschränkungen und gibt auch kleinen Unternehmen, die mit Ressourcenengpässen in der IT zu kämpfen haben, die Möglichkeit, ihre IT-Sicherheit zu automatisieren, auszubauen und gleichzeitig deren Verwaltbarkeit zu gewährleisten.

Kaspersky Endpoint Security for Business wurde grundlegend neu entwickelt. Das heißt, dass anstelle mehrerer miteinander verbundener Softwarelösungen nur eine einzige IT-Sicherheitsplattform verwendet wird. Das Ergebnis ist ein weitaus einfacheres Sicherheitsmanagement, da Richtlinien nur einmal festgelegt und dann per Mausklick auf mehreren Endpunkten und in verschiedenen Umgebungen angewendet werden können.

Kaspersky Endpoint Security for Business beinhaltet eine komplette und vollständig eingebundene Plattform inklusive Malware-Schutz, zuverlässigen Tools zur Programmkontrolle, Systems Management, Datenverschlüsselung und Verwaltung mobiler Geräte von einer einzigen Konsole aus. Von einem zentralen Dashboard lassen sich Programme verwalten, sämtliche Geräte inventarisieren, einsehen, kontrollieren und schützen – ganz gleich, ob es physische, virtuelle oder mobile Geräte, Unternehmens- oder Privatgeräte sind.

Verwaltung über eine zentrale Managementkonsole: **Kaspersky Security Center**



Das zentrale Management von Endgeräten aller Art reduziert die Komplexität der IT-Security, schafft einen nahtlosen Schirm gegen Bedrohungen aller Art und verbessert die Transparenz der IT.

Unternehmen aller Größen können so ohne großen Schulungsaufwand oder spezielles Know-how ein hohes Maß an Sicherheit auch in einer komplexen und sich häufig ändernden IT-Umgebung erreichen.

Besonders für kleine und mittelständische Unternehmen ist diese Lösung mit ihrem geringen Verwaltungsaufwand geeignet, denn sie erfordert keine Systemintegration und kann auch von IT-Mitarbeitern angewendet werden, die keine IT-Sicherheitsexperten sind. Trotzdem ist es mit dieser Lösung möglich, alle Endpunkte, an denen auf Unternehmensdaten zugegriffen wird, nahtlos einzusehen, zu kontrollieren und zu schützen – unabhängig davon, ob es sich um Desktops, virtuelle Computer, Tablet-Computer, Smartphones oder die Privatgeräte von Mitarbeitern handelt. Grundlage von Kaspersky Endpoint Security for Business ist eine einzige und konsistente Managementkonsole. Die Sicherheitstools können so auf einem zentralen Dashboard aufgerufen und gesteuert werden, Konfiguration, Bereitstellung, Richtlinienverwaltung und Sicherheitseinstellungen sind im gesamten Unternehmen einheitlich.

Der Sicherheitsverantwortliche bekommt somit wichtige Tools wie

- Endpoint-Steuerung (Gerätekontrolle, Diebstahlschutz, Webkontrolle, Applikationskontrolle),
- Verschlüsselung,
- Überwachung von Mail, Internet Gateway und SharePoint,
- Cloud-gestützte Signaturdatenbank,
- Reporting-System

aus einer Hand zur Verfügung gestellt.

Videozitat

Armin Recha, Director Corporate Sales, Kaspersky Lab DACH, erläutert die Vorteile einer zentralen Konsole für System- und Security-Management in KMU.

Bedarfsorientiert in vier Stufen

Kaspersky Endpoint Security for Business steht in vier unterschiedlichen Stufen zur Verfügung:

Core

Anti-Malware-Schutz für Workstations inklusive Firewall und Kaspersky Security Center

Select

Workstation- und Datei-Server-Sicherheit, Whitelisting und Programm-, Geräte- und Webkontrolle. Ebenfalls eingeschlossen ist eine mobile Schutzlösung, die aus einem Endpoint-Sicherheitsagenten und Mobile Device Management (MDM) besteht.

Advanced

Auf der Stufe Advanced wird von Kaspersky Lab der Datenschutz in Form einer Verschlüsselung von Dateien oder des gesamten Datenträgers hinzugefügt. Bei Kaspersky Systems Management wird Sicherheit mit IT-Effizienz kombiniert. In diesem breiten Funktionsangebot sind wichtige Tools enthalten, die dem Administrator Folgendes ermöglichen:

- Erstellen und Speichern von Images sowie die Remote-Bereitstellung von Systemen
- Behandlung von Schwachstellen in der Software mit einer leistungsstarken Kombination aus Advanced Vulnerability Scanning und intelligentem Patch Management priorisieren
- Lizenzverwendung und die Einhaltung des Software-Lizenzmanagements sicherstellen
- Updates und neue Software für Benutzer von der zentralen Konsole aus der Ferne bereitstellen und installieren

Total

Im Flaggschiffprodukt Kaspersky Total Security for Business werden alle vorigen Stufen zu einer Komplettversion kombiniert. Zusätzlich wird die Sicherheit mit dem Web-, E-Mail- und Collaboration-Serverschutz auf alle Netzwerkebenen ausgedehnt.

CeBIT pro Studio Mittelstand

CeBIT Studio Mittelstand 2013

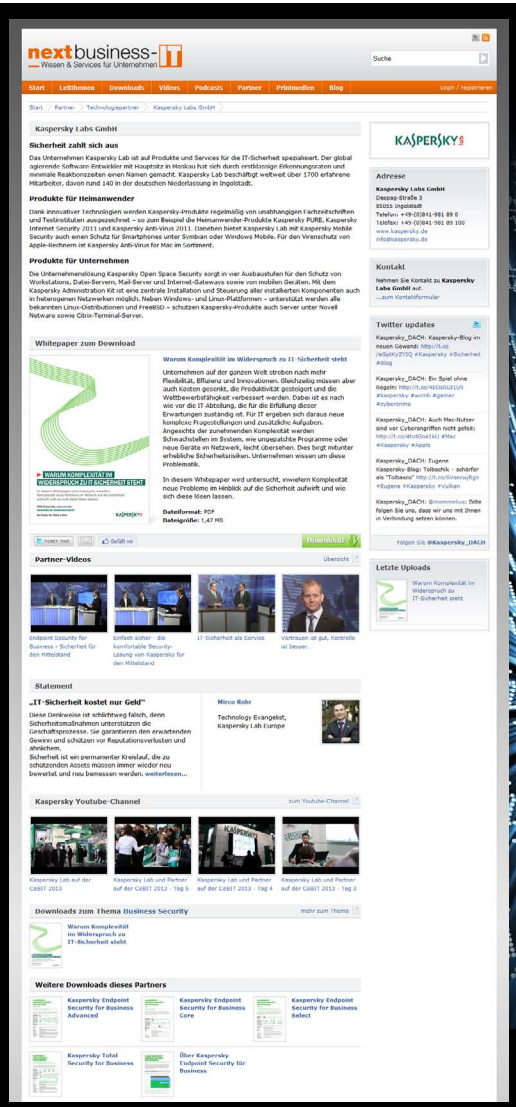
Sicherheit für den Mittelstand

In seiner 15-jährigen Unternehmensgeschichte hat Kaspersky Lab zahlreiche Innovationen im Bereich IT-Sicherheit auf den Weg gebracht und bietet effektive digitale Sicherheitslösungen für Großunternehmen, KMU und Heimanwender. Kaspersky Lab ist derzeit in rund 200 Ländern auf der ganzen Welt vertreten und schützt über 300 Millionen Nutzer weltweit.

Für den bestmöglichsten Schutz forscht Kaspersky Lab ständig an neuen Technologien und ist dabei ein wichtiger Wegbereiter für neue Sicherheitsstandards. So hat Kaspersky Lab nicht nur als erster Hersteller auf einen proaktiven Schutz vor unbekannten Viren gesetzt, sondern auch den ersten Virenschutz für Linux entwickelt sowie die erste Antiviren-Lösung mit Citrix-Zertifikat auf den Markt gebracht.

Im CeBIT Studio Mittelstand 2013 zeigen Experten von Kaspersky Lab auf, wie mittelständische Unternehmen innovative Technologien wie die proaktive Analyse von Bedrohungen schützen Anwender auch vor unbekannten Gefahren aus dem Internet, und das bei minimalem Ressourcenverbrauch. Dieses Studio stellt das derzeit sowohl inhaltlich als auch technisch professionellste Web-TV-Format im und für den Mittelstand dar – sowohl, was die Interaktionsplattform als solche betrifft, als auch die Aufbereitung der Themen sowie die Vielzahl renommierter Experten aus Unternehmertum, Wirtschaft, Organisationen und Politik.
Alle Sendungen mit Kaspersky Lab zum Thema Endpoint Security können Sie **hier** on demand abrufen.

Aktuelle Whitepapers zu den Security-Lösungen von Kaspersky Lab finden Sie auf **www.nextbusiness-IT.de/kaspersky**



nextbusiness-IT Partner bieten mehr!

Downloads und Videos, Social-Media-Updates, Unternehmensprofil sowie Kontaktmöglichkeiten zu **Kaspersky** finden Sie im Internet.

www.kaspersky.com/de/business-security
Kontakt: salesdach@kaspersky.de

www.nextbusiness-it.de/kaspersky

Impressum

Verlagsanschrift: G+F Verlags- und Beratungs- GmbH,
Kapellenstraße 46, 76596 Forbach, Telefon: (07220) 213, Telefax: (07220) 215, info@gf-vb.de, www.gf-vb.de; **Geschäftsführer:** Andreas R. Fischer
Redaktion: Jürgen Bürkel v. i. S. d. P., Guntram Stadelmann
Leitung Key-Account-Management: Steffen Guschmann
Leitung Strategisches Marketing: Heiko Fischer
Produktion: Strattack GmbH

Bildnachweis: Alle Bildrechte liegen bei den jeweiligen Eigentümern