
BEST PRACTICES
BEI VERSCHLÜSSELUNG.
With Kaspersky, now you can.
kaspersky.de/business-security
Be Ready for What's Next.
KASPERSKY lab

INHALT

VERSCHLÜSSELUNG LEICHT GEMACHT. ES GEHT UM IHRE DATEN.

Proaktiver Schutz von Daten ist eine weltweit zwingende Notwendigkeit. Auf den wichtigen Absatzmärkten der Welt sind Unternehmen aller Größenordnungen mittlerweile verpflichtet, Gesetzesinitiativen zu Datensicherheit und -schutz umzusetzen. Von PCI DSS, HIPAA, SOX, DPP (EU-weit), PIPA (Japan) bis zum Data Protection Act in Großbritannien existiert ein weltweiter Trend, Unternehmen von Behördenseite aus zum Schutz vertraulicher Daten zu verpflichten. Der Informationsbeauftragte der britischen Regierung beispielsweise hat sich dahingehend geäußert, dass Datenverluste „ohne einen Schutz der Daten durch Verschlüsselung“ voraussichtlich behördliche Maßnahmen nach sich ziehen werden. [6]

1. EINLEITUNG

In einer kürzlich durchgeführten Umfrage von Kaspersky Lab gaben 29 % der Teilnehmer an, dass Ihr Unternehmen bereits von Diebstahl oder Verlust mobiler Geräte betroffen war. Laut Kensington wird alle 53 Sekunden ein Laptop gestohlen.[1&2]

Auch wenn Sie angesichts dieser Zahlen zuerst an die Kosten für den Ersatz der Geräte denken, sind die eigentlichen Probleme beim Verlust mobiler Endgeräte ganz andere. Geräteersatzkosten mögen für Ihr Unternehmen ein Problem darstellen, aber im Fall eines Datenverlusts sind dies Ihre geringsten Sorgen. Kommt ein Laptop oder ein Smartphone abhanden, macht die Bereinigung des entstandenen Datenlecks mehr als 80 Prozent der Folgekosten[3] aus – unabhängig von der Größe des Unternehmens.

Rechnen Sie nun noch den ständig anwachsenden Bußgeldkatalog für Datensicherheitsverletzungen, den Imageschaden und die Auswirkung auf die Kundenloyalität hinzu, und es wird schnell klar, dass die Kosten eines Datenschutzverstoßes weit über die Geräteersatzkosten hinausgehen. 85 Prozent der Kunden weltweit haben angegeben, dass sie das Unternehmen wechseln würden, wenn dieses ihre persönlichen Informationen verlieren oder erfolgreich gehackt würde. 47 Prozent würden sogar rechtliche Schritte einleiten.[4]

Es muss Ihnen jedoch nicht unbedingt ein Gerät abhandenkommen, um vertrauliche Daten zu verlieren. Vertrauliche Geschäftsdaten, geistiges Eigentum und Geschäftsgeheimnisse sind mittlerweile die Hauptziele von Malware-Attacken.

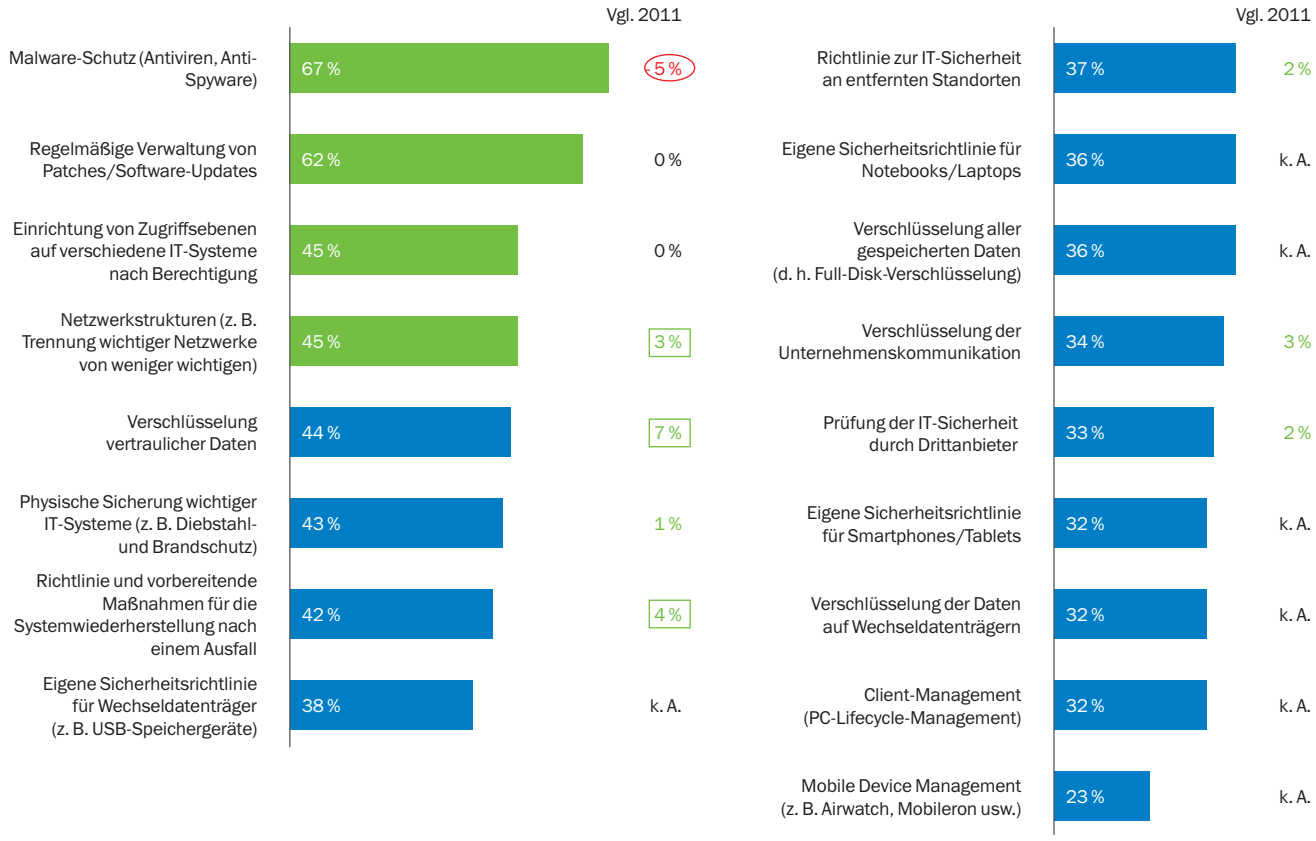
Das Ponemon Institute schätzt den finanziellen Schaden, der durch den Verlust eines Laptops entsteht, auf 49.246 US-Dollar, wobei die Ersatzkosten für das Gerät lediglich zwei Prozent ausmachen. Eine Verschlüsselung kann die Kosten, die durch den Verlust eines Laptops entstehen, um durchschnittlich 20.000 US-Dollar senken.[5] Egal ob Ihr Problem ein gestohlener Laptop, ein verlorenes Speichermedium oder Datendiebstahl durch Malware ist, durch Verschlüsselung werden vertrauliche Daten für Kriminelle oder andere nicht befugte Nutzer unbrauchbar gemacht.

1 Quelle: Bericht von Kaspersky Lab zu globalen IT-Risiken, 2012
2 Quelle: Kensington: The Cost of Stolen or Lost Laptops, Tablets and Phones, 2012
3 Quelle: Ponemon: The Billion Dollar Lost Laptop Problem, 2012
4 Quelle: Unisys Security IndexTM: GLOBAL SUMMARY, 18. Oktober 2011 (Wave 2H’11)
5 Quelle: Ponemon: The Cost of a Lost Laptop, 2009
6 Quelle: Information Commissioner’s Office, http://www.ico.gov.uk, 2012

2. BEST PRACTICES

Früher waren Verschlüsselungstechnologien ausschließlich Regierungsbehörden oder Großkonzernen mit hohem Kapital vorbehalten. Die Technologie hat sich jedoch weiterentwickelt. Heutzutage können sich Unternehmen aller Größenordnungen ressourcenschonende und einfach zu handhabende Verschlüsselungslösungen leisten.

Anstieg genutzter Verschlüsselungslösungen in Unternehmen seit 2011



Verschlüsselung wird verstärkt als Mittel im Kampf gegen den Datenverlust eingesetzt.[7]

Im Folgenden möchten wir Ihnen gerne einige Best Practices vorstellen, mit denen auch Ihr Unternehmen eine effektive Verschlüsselungsstrategie umsetzen kann.

7 Quelle: Bericht von Kaspersky Lab zu globalen IT-Risiken, 2012

3. ERST DIE RICHTLINIE, DANN DIE TECHNOLOGIE

Wie bei so vielen Sicherheitsstrategien beginnt auch eine effektive Verschlüsselung mit dem Festlegen überzeugender Richtlinien: Sollen komplette Festplattenlaufwerke verschlüsselt werden? Wechseldatenträger? Oder nur bestimmte Arten von Daten, Dateien und Ordnern? Möglicherweise sollen bestimmte Dokumente für einige Benutzer nicht lesbar sein, für andere aber schon? Oder ein bisschen von beidem?

Für die meisten Unternehmen ist es von entscheidender Bedeutung, Informationen für die richtigen Personen zum richtigen Zeitpunkt zugänglich zu machen. Dank effektiver Richtlinien und der entsprechenden Technologie gelingt dies, ohne die Sicherheit zu beeinträchtigen.

Hier einige nützliche Vorüberlegungen:

- **Beziehen Sie alle relevanten Akteure ein** – das IT-Management, die Geschäftsleitung, die Finanzabteilung. Sie unterstützen Sie dabei, die Arten von Informationen zu bestimmen, die besonders gut geschützt werden müssen.
- **Zugriffskontrolle** – Wenn jeder einen Schlüssel besitzt, macht es keinen Sinn, die Tür abzuschließen. Finden Sie gemeinsam mit den genannten Akteuren heraus, wer zu welchem Zeitpunkt Zugriff auf welche Arten von Informationen benötigt. Als zusätzliche Sicherheitsmaßnahme sollten Zugriffskontrollen regelmäßig auf ihre Aktualität geprüft werden.
- **Machen Sie sich mit den behördlichen Auflagen vertraut** – PCI DSS, HIPAA, SOX, DPP (EU-weit), PIPA (Japan) oder der Data Protection Act in Großbritannien. Sie selbst sind vielleicht nicht mit der wachsenden Anzahl von Datenschutzbestimmungen vertraut, viele Ihrer Kollegen aber schon. Finden Sie heraus, welche Bestimmungen, Gesetze, Auflagen und andere externe Faktoren für die Sicherung und den Austausch von Daten in Ihrem Unternehmen ausschlaggebend sind. Legen Sie Richtlinien fest, wie diese umzusetzen sind, beispielsweise durch automatische Verschlüsselung von Kundenkreditkartendaten oder Sozialversicherungsnummern von Angestellten.
- **Gehen Sie auf Nummer sicher** – Legen Sie Ihre Richtlinien schriftlich nieder, lassen Sie sie von der Unternehmensleitung absegnen, und leiten Sie sie an Ihre Endbenutzer weiter, einschließlich externer Anbieter, die sich möglicherweise um Ihre vertraulichen Daten kümmern. Auch wenn Sie damit nicht auf Begeisterung stoßen – Ihre Daten sind vor unbefugtem Zugriff geschützt.
- **Sichern Sie Ihre Daten** – Eine bewährte Vorgehensweise besteht darin, vor der Installation neuer Software ein Backup der Daten durchzuführen. Bei der Verschlüsselung verhält es sich nicht anders: Sichern Sie immer alle Endbenutzerdaten, bevor Sie mit Ihrem Verschlüsselungsprogramm fortfahren.

4. FULL-DISK- ODER FILE-LEVEL-VERSCHLÜSSELUNG?

Die Antwort ist ganz einfach: beides. Verschlüsselungslösungen basieren normalerweise auf zwei unterschiedlichen Methoden, der Full-Disk-Verschlüsselung (FDE) oder der File-Level-Verschlüsselung (FLE), die jeweils eigene Vorteile aufweisen:

4.1 Vorteile der Full-Disk-Verschlüsselung (FDE):

- FDE schützt Ihre „ruhenden Daten“ so nah an der Hardware-Ebene wie möglich, d. h. jeder einzelne Sektor eines Laufwerks wird verschlüsselt. Dies bedeutet, dass alle Daten auf einer Festplatte verschlüsselt werden, also Dateiinhalte, Metadaten, Dateisysteminformationen und Verzeichnisstrukturen. Nur authentifizierte Benutzer haben Zugriff auf die Daten auf einem verschlüsselten Datenträger. Außer Festplatten lassen sich mit FDE auch

Wechselmedien, wie z. B. USB-Laufwerke oder Festplatten in USB-Gehäusen, verschlüsseln.
- Setzen Sie auf Pre-Boot-Authentifizierung – Hierbei muss sich der Benutzer noch vor dem eigentlichen Start des Betriebssystems anmelden. So erhalten Sie zusätzlichen Schutz für den Fall, dass ein Laptop abhandenkommt, denn es können weder Daten direkt von der Festplatte ausgelesen werden, noch lässt sich das Betriebssystem starten.
- Für FDE hat sich auch eine „Set and Forget"-Richtlinie bewährt, die Benutzerentscheidungen weitestgehend eliminiert. Wenn Sie Zugriff per einmaliger Anmeldung (SSO) ermöglichen, merken Ihre Endbenutzer im Endeffekt nichts davon.
- Der größte Vorteil von FDE besteht darin, dass Benutzerfehler als potenzielle Risikoursache ausgeschlossen werden, denn es wird schlicht und einfach alles verschlüsselt. Der Nachteil ist, dass Daten während der Übertragung nicht geschützt werden können, darunter auch Daten, auf die von mehreren Geräten aus zugegriffen wird. Wenn Sie sich an die Best Practices halten und eine Lösung gewählt haben, die darüber hinaus eine File-Level-Verschlüsselung vorsieht, stellt dies jedoch kein Problem dar.

4.2 Vorteile der File-Level-Verschlüsselung (FLE):
FLE greift auf Ebene des Dateisystems und ermöglicht nicht nur den Schutz von „ruhenden" Daten, sondern auch von Daten, mit denen derzeit gearbeitet wird. Mit FLE lassen sich Dateien und Ordner auf beliebigen Geräten gezielt verschlüsseln. Bei hochwertigen Lösungen bleiben die Dateien sogar dann verschlüsselt, wenn sie über das Netzwerk hinweg kopiert werden. Hierdurch können Daten für unbefugte Benutzer gezielt unlesbar gemacht werden, egal wo sie gespeichert sind oder wohin sie kopiert werden. FLE ermöglicht das automatische Verschlüsseln von Dateien auf Grundlage von Eigenschaften wie Speicherort (z. B. alle Dateien im Ordner „Eigene Dokumente"), Dateityp (z. B. alle Textdateien, Excel-Tabellen usw.) oder dem Programm, mit dem eine Datei gespeichert wird. Hochwertige Lösungen ermöglichen es beispielsweise, unabhängig von Ordner oder Laufwerk automatisch alle Daten zu verschlüsseln, die mit Microsoft Word erstellt wurden.

- FLE bietet Unternehmen, die präzise Zugriffsrichtlinien benötigen, ein hohes Maß an Flexibilität: Wenn anhand von administrativen Richtlinien nur die als vertraulich deklarierten Daten gezielt verschlüsselt werden, lassen sich Szenarien mit einer gemischten Datennutzung realisieren.
- FLE ermöglicht darüber hinaus eine unkomplizierte und sichere Systempflege: Während die Daten in verschlüsselten Dateien geschützt bleiben, sind Software- und Systemdateien zugänglich, um Update- und Wartungsaufgaben zu ermöglichen. Wenn Sie als Leiter der Finanzabteilung vertrauliche Geschäftsinformationen vor Systemadministratoren verbergen wollen, ist dies mit FLE möglich.
- FLE ermöglicht darüber hinaus eine effektive Steuerung und Kontrolle von Programmberechtigungen, sodass eindeutige Verschlüsselungsregeln für bestimmte Programme und Nutzungsszenarien festgelegt werden können. So können Administratoren beispielsweise festlegen, unter welchen Umständen verschlüsselte Daten in ihrer verschlüsselten Form bereitgestellt werden, oder den Zugriff auf verschlüsselte Daten für bestimmte Programme sogar vollständig sperren. So können sie z. B.:
  - Die Durchführung sicherer Backups vereinfachen, da verschlüsselte Dateien bei Übertragung, Archivierung und Wiederherstellung unabhängig von den Richtlinien auf dem Endpoint, auf dem sie wiederhergestellt werden, garantiert verschlüsselt bleiben.
  - Den Austausch verschlüsselter Dateien über IM oder Skype verhindern, ohne den Austausch unbedenklicher Nachrichten einzuschränken.

Mit einem gemischten Verschlüsselungsmodell aus FDE und FLE profitieren Unternehmen von den Vorteilen beider Ansätze. Denkbar wäre beispielsweise, FLE auf Desktop-PCs anzuwenden, während bei Laptops grundsätzlich der gesamte Datenträger verschlüsselt wird (FDE).

5. VERSCHLÜSSELUNG VON WECHSELDATENTRÄGERN

USB-Flashlaufwerke erreichen mittlerweile Kapazitäten von über 100 GB, externe Festplatten, die kleiner sind als eine Hand, sogar mehrere Terabyte – eine riesige Menge potenziell vertraulicher Geschäftsdaten, die leicht abhandenkommen können. Sie können ein Laufwerk beispielsweise in Ihrer Jacke vergessen, die Sie gerade zur Reinigung gebracht haben, es bei der Sicherheitskontrolle am Flughafen liegen lassen, oder es kann Ihnen ganz einfach aus der Tasche fallen.

Nachlässigkeiten und Zufälle lassen sich nicht beeinflussen, wohl aber die Konsequenzen, die sich aus ihnen ergeben. Daher sehen wirksame Verschlüsselungsstrategien immer auch eine Verschlüsselung von Wechseldatenträgern vor. Stellen Sie sicher, dass vertrauliche Daten bei jeder Übertragung von einem Endpoint auf einen Wechseldatenträger verschlüsselt werden. Sie erreichen dies, indem Sie FDE- oder FLE-Richtlinien auf alle Geräte anwenden, und stellen überdies sicher, dass Ihre vertraulichen Daten geschützt sind, selbst wenn sie abhandenkommen oder gestohlen werden.

Beim Umgang mit vertraulichen Daten sollte innerhalb wie außerhalb des Perimeters der sogenannte „portable Modus“ genutzt werden. Sie haben beispielsweise vor, einen Vortrag auf einer Konferenz zu halten, und müssen Ihre Daten über einen USB-Stick auf einem öffentlich zugänglich Computer bereitstellen, auf dem keine Verschlüsselungssoftware installiert ist. Sie müssen die Sicherheit Ihrer Daten auf dem Weg von Ihrem Laptop auf das Präsentationssystem gewährleisten. Führende Verschlüsselungslösungen bieten zu diesem Zweck einen „portablen Modus“. Dieser ermöglicht den Transport von Daten auf verschlüsselten Wechseldatenträgern und die Nutzung auf Computern, selbst wenn auf diesen keine Verschlüsselungssoftware installiert ist.

6. BEWÄHRTE UND SICHERE VERSCHLÜSSELUNG

Ihre Verschlüsselungsstrategie ist nur so gut wie die ihr zugrunde liegende Technologie. Leicht zu knackende Verschlüsselungsalgorithmen sind wertlos. Der Advanced Encryption Standard (AES) mit einer Schlüssellänge von 256 Bit gilt als der „goldene Standard“ unter den Verschlüsselungsverfahren. Er wird von US- Regierungsbehörden eingesetzt und ist ein international anerkannter Industriestandard. Der Schlüssel ist von entscheidender Bedeutung, denn Verschlüsselungsalgorithmen sind immer nur so gut wie die Schlüssel, mit denen sie entschlüsselt werden. Bei einfach zu knackenden Schlüsseln ist Ihr gesamtes Verschlüsselungsprogramm wertlos. Genauso wichtig für eine wirksame Verschlüsselung ist eine effektive Handhabung der Schlüssel. Das sicherste Türschloss der Welt nützt Ihnen herzlich wenig, wenn Sie den Schlüssel unter die Fußmatte legen.

7. Malware-Schutz NICHT VERNACHLÄSSIGEN

Auch wenn Laptops nicht verloren gehen oder gestohlen werden, besteht das Risiko, dass Daten abhandenkommen. Cyberkriminelle haben es verstärkt auf vertrauliche Daten auf geschäftlich genutzten Geräten abgesehen, beispielsweise durch Malware, mit der Informationen von Laptops entwendet werden können, ohne dass der Benutzer es bemerkt.

Keine Verschlüsselungsstrategie kommt ohne einen integrierten Malware-Schutz aus, der gezielt vor schädlichen Codes schützt, mit denen wertvolle Informationen von Ihrem Laptop gestohlen werden sollen. Als bewährte Vorgehensweise wären hier Anti-Malware-Updates und Scan-Funktionen zu nennen, die automatisch auch ohne ein Eingreifen des Benutzers ausgeführt werden können.

8. VERGESSENE KENNWÖRTER

Der durchschnittliche Benutzer vergisst sein Kennwort beinahe genauso oft, wie er seinen USB-Stick oder sein Smartphone verliert. Und manchmal versagt auch die zuverlässigste Hardware oder das beste Betriebssystem, und Sie stehen ohne Zugriff auf entscheidende Informationen da. Bewahren Sie kryptografische Schlüssel an einem zentralen Ort oder in treuhänderischer Verwahrung auf. Hierdurch wird die Entschlüsselung von Daten in Notsituationen erheblich vereinfacht.

Eine effektive Verschlüsselungslösung stellt Administratoren Tools für eine unkomplizierte Datenwiederherstellung für die folgenden Fälle bereit:

- Bei Anforderung durch den Endbenutzer (vergessenes Kennwort usw.)
- Aus Wartungsgründen oder bei technischen Problemen, z. B. wenn ein Betriebssystem nicht geladen werden kann oder bei einem mechanischen Schaden an einem Laufwerk, der repariert werden muss.

Wenn ein Benutzer sein Kennwort vergisst, kann als alternative Authentifizierungsmethode eine Reihe von Fragen dienen, die der betreffende Benutzer korrekt beantworten muss.

9. EINFACH UND ZENTRAL

In der Vergangenheit wurde von Seite der Unternehmen oft der Einwand geäußert, die Implementierung und Verwaltung einer Verschlüsselungslösung sei zu aufwändig und kompliziert. Viele der älteren Lösungen werden getrennt von Anti-Malware-Programmen bereitgestellt und erhöhen so tatsächlich die Komplexität. Die Handhabung verschiedener Lösungen – Anti-Malware, Endpoint-Kontrolle, Verschlüsselung – ist, selbst wenn diese von einem Anbieter stammen (ganz zu schweigen von mehreren Anbietern), nicht nur teuer, sondern in allen Phasen der Bereitstellung auch sehr zeitaufwändig: Beschaffung, Mitarbeiterschulung, Provisioning, Richtlinienverwaltung, Wartung und Upgrades müssen für jede der Komponenten als getrenntes Projekt angelegt werden. Ein integrierter Ansatz spart nicht nur Zeit und Geld, sondern gestaltet die Softwarebereitstellung auch so einfach und schmerzlos wie möglich.

Einfach zu handhabende Lösungen sind effektiver. Entscheiden Sie sich für eine Lösung, die von Anfang an eine Verwaltung über nur eine Konsole und unter nur einer Richtlinie ermöglicht. Hierdurch sparen Sie Investitionskosten und vermeiden Kompatibilitätsprobleme zwischen unterschiedlichen Komponenten, die alle getrennt voneinander verwaltet werden müssen. Darüber hinaus hat sich die Verwendung ein und derselben Richtlinie sowohl für die Endpoint-Verschlüsselung als auch für den Malware-Schutz, die Gerätekontrolle und alle anderen Sicherheitseinstellungen für Endpoints bewährt. Hierdurch lassen sich integrierte und in sich stimmige Richtlinien durchsetzen. So kann beispielsweise die IT-Abteilung den Anschluss von bestimmten Wechselmedien an einen Laptop zulassen und gleichzeitig Verschlüsselungsrichtlinien für das Gerät erzwingen. Eine eng integrierte Technologieplattform hat zudem den Vorteil einer insgesamt verbesserten Systemleistung.

10. FAZIT

Mit Kaspersky Endpoint Security for Business können Best Practices im Bereich Verschlüsselung in Unternehmen aller Größenordnungen realisiert werden. Durch die Kombination aus leistungsstarken Verschlüsselungsverfahren und branchenweit führendem Malware-Schutz und Endpoint-Kontrolltechnologien schützt unsere integrierte Plattform vertrauliche Daten vor den Risiken, die durch Verlust oder Diebstahl von Geräten bzw. durch Malware entstehen.

Präzise Kontrollmöglichkeiten und eine umfassende Funktionalität lassen sich ganz einfach über eine zentrale Konsole verwalten, die einen vollständigen Überblick über die gesamte Sicherheitslandschaft ermöglicht – egal, ob es sich um virtualisierte Maschinen, physische Systeme, Mobilgeräte oder Wechselmedien handelt.

Im Gegensatz zu vielen anderen Datenschutzlösungen lässt sich mit Kaspersky Endpoint Security for Business ein auf gemeinsamen Richtlinien beruhendes Verwaltungsmodell komplett neu aufbauen: Die Verschlüsselungsrichtlinien werden als Teil derselben Gesamtrichtlinie festgelegt, die auch den Malware-Schutz, die Geräte- und Programmkontrolle und alle Einstellungen der Endpoint-Sicherheit regelt. Die Voraussetzung für einen solchen ganzheitlichen Ansatz ist die vereinheitlichte Codebasis von Kaspersky Lab: Unsere Experten entwickeln Software und Technologien, die eng miteinander verzahnt sind und dem Benutzer anstatt einer unzusammenhängenden Anwendungssammlung eine echte Sicherheitsplattform bieten.

Eine enge Integration entscheidender Sicherheitskomponenten (z. B. Anti-Malware, Verschlüsselung und Programm- und Gerätekontrolle) vereinfacht die Verwaltung und Überwachung und garantiert gleichzeitig Stabilität, integrierte Richtlinien, Reporting und intuitiv zu bedienende Tools.

Ein Hersteller, eine Investition, eine Installation – umfassende Sicherheit.

SEE IT. CONTROL IT. PROTECT IT.

With Kaspersky, now you can.
kaspersky.de/business-security

Be Ready for What's Next

Kaspersky Lab DACH
www.kaspersky.de

92p6a/Stand: März 2013