KASPERSKY lab

BEST PRACTICES

Verschlüsselung

www.kaspersky.de

LEITFADEN ZU BEST PRACTICES BEI DER VERSCHLÜSSELUNG

Datenschutz. Handeln Sie jetzt.

Der schnelle Schutz von Daten ist eine weltweit zwingende geschäftliche Notwendigkeit. Kaspersky Lab kann Sie bei der Implementierung vieler Best Practices in den Bereichen Datenverschlüsselung und Datenschutz unterstützen.

Business Case für Verschlüsselung

Seit 2005 wurden mehr als **816** Millionen Datensätze kompromittiert.[1] Allein in den ersten vier Monaten des Jahres 2015 wurden **101** Millionen Datensätze unangemessen offengelegt.[2]

Es vergeht kaum eine Woche ohne Schlagzeilen zu einem weiteren großen Verstoß gegen die Datensicherheit. Das Identity Theft Resource Center hat 2014 das „Jahr der Datenverletzung" getauft und gab als zwei der Hauptgründe für Datenverlust bzw. Datenlecks die auf mobilen Geräten oder Wechseldatenträgern gespeicherten Daten sowie interne Verstöße durch den Zugriff nicht autorisierter Mitarbeiter auf vertrauliche Daten an.[3] In fast 20 % der von Kaspersky Lab befragten Unternehmen sind infolge eines Gerätediebstahls Datenverluste aufgetreten.[4]

Die Forschungsarbeiten von Kaspersky Lab haben ergeben, dass sich die Kosten für ein Datenverlust-Ereignis 2014 in Großunternehmen auf **636.000 $** und in kleinen und mittleren Unternehmen auf **33.000 $** beliefen.[5] Und Ihnen muss kein Gerät abhanden kommen, um sensible Daten zu verlieren. Sensible geschäftliche Informationen, geistiges Eigentum und Geschäftsgeheimnisse sind mittlerweile die Hauptziele von Malware-Attacken.

Dabei geht es nicht lediglich um die direkten Kosten einer Datenverletzung, den Verlust treuer Kunden oder eine Rufschädigung für Ihr Unternehmen (72 Prozent aller Unternehmen mussten sich öffentlich zu einem Vorfall bekennen[6]). In den meisten wichtigen Märkten gibt es inzwischen gesetzliche Vorschriften für die Bereiche Datensicherheit und Datenschutz, wobei Unternehmen oft gezwungen sind, vertrauliche Daten zu verschlüsseln.

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.

Egal ob Ihr Problem ein gestohlener Laptop, ein verlorenes Speichermedium oder Datendiebstahl durch Malware heißt, durch Verschlüsselung werden sensible Daten für Kriminelle oder andere nicht befugte Nutzer unbrauchbar gemacht.

Aber wie geht man hierzu am besten vor?

---

1 Privacy Rights Clearing House: http://www.privacyrights.org/data-breach
2 Identity Theft Resource Center 2015: http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2015.pdf
3 Identity Theft Resource Center 2015: http://www.idtheftcenter.org/Press-Releases/2014breachstatistics.ht
4 Kaspersky Lab: Bericht zu IT-Sicherheitsrisiken, 2014
5 Kaspersky Lab: Bericht zu IT-Sicherheitsrisiken, 2014
6 Kaspersky Lab: Bericht zu IT-Sicherheitsrisiken, 2014

Best Practice-Ansätze bei der Verschlüsselung

Die Verschlüsselungstechnologie von Kaspersky Lab schützt wertvolle Daten vor ungewolltem Verlust, bei Diebstahl oder gezielten Malware-Attacken.

1. ZUERST DIE RICHTLINIE, DANN DIE TECHNOLOGIE

Wie bei vielen Sicherheitsstrategien liegen die Best Practices bei der Verschlüsselung zunächst darin, starke Richtlinien zu erstellen: Sollen gesamte 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 doch? Und wie wäre es mit einem bisschen von allem?

Für die meisten Unternehmen ist es von entscheidender Bedeutung, Informationen für die richtigen Leute 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 Beteiligten in die Entscheidung mit ein** – IT-Manager, operative Abteilungen, Finanzen, Personalabteilung usw. Auf diese Weise können Sie ermitteln, welche Informationen besonders 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 Zugriff auf welche Art von Informationen benötigt. Und wann. 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 –** Erfassen Sie Ihre Richtlinien schriftlich, 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. So sind zumindest Ihre Daten 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.

- **Halten Sie alles möglichst einfach** – Durch Implementierung einer Technologie, die eine einmalige Anmeldung unterstützt, machen Sie es dem Endbenutzer so einfach wie möglich und minimieren Eingriffe in den Arbeitsalltag.

2. VOLLSTÄNDIGE DATENTRÄGERVERSCHLÜSSELUNG ODER DATEIVERSCHLÜSSELUNG?

Die Antwort ist ganz einfach: Beides.

Verschlüsselungslösungen basieren normalerweise auf zwei unterschiedlichen Methoden, der vollständigen Datenträgerverschlüsselung (FDE) oder der Dateiverschlüsselung (FLE), die jeweils eigene Vorteile aufweisen:

Vorteile der vollständigen Datenträgerverschlüsselung (FDE)

Die FDE-Technologie ist eine der wirksamsten Methoden für Unternehmen, ihre Daten bei Diebstahl oder Verlust zu schützen. Unabhängig davon, was letztendlich mit einem Gerät passiert, kann mit dem FDE-Verfahren sichergestellt werden, dass alle vertraulichen Unternehmensdaten für Kriminelle oder auch nur für neugierige Dritte vollständig unleserlich und unbrauchbar sind.

- 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 verschlüsseln, beispielsweise USB-Laufwerke oder Festplatten in USB-Gehäusen.

- Nützlich ist eine Pre-boot-Authentifizierung (PBA), bei der Benutzer ihre Anmeldedaten eingeben und authentifizieren lassen müssen, noch bevor das Betriebssystem gestartet wird. So entsteht eine weitere Schutzebene. Diebe können nichts direkt von der Oberfläche der Festplatte lesen, und das Betriebssystem lässt sich nicht starten.

  Die Verschlüsselungstechnologie von Kaspersky Lab bietet PBA mit optionaler einmaliger Anmeldung. Für eine bessere Benutzererfahrung funktioniert PBA auch mit anderen als QWERTY-Tastaturen. Bei Verschlüsselungslösungen, die eine Authentifizierung per Smartcard und Tokens unterstützen (Zwei-Faktor-Authentifizierung), erübrigt sich die Verwendung zusätzlicher Kennwörter, was wiederum zu einer verbesserten Benutzererfahrung beiträgt.

- Entscheiden Sie sich für eine Verschlüsselungslösung, bei der die gesamte Hardware im Netzwerk noch **vor** der Implementierung auf Kompatibilität überprüft wird, um spätere Probleme zu vermeiden. Lösungen mit Unterstützung für UEFI-basierte Plattformen, darunter die neuesten Laptops und Workstations ab Windows 8, sorgen dafür, dass Sie auch für die Zukunft gut gerüstet sind.

  Genauso tragen Unterstützung für Intel AES NI – eine neue Verbesserung des Advanced Encryption Standard (AES), durch den die Verschlüsselung bei den Xeon- und Core-Prozessorreihen von Intel beschleunigt wird (sowie einige AMD) – und die neuesten GPT-Festplattenstandards zu einer abgerundeten Verschlüsselungsstrategie bei.

- Ermöglichen Sie eine sichere Datenfreigabe im Unternehmen durch FDE-Verschlüsselung auf Wechseldatenträgern.

- Für FDE hat sich auch eine „set and forget"-Praxis für einen unkomplizierten, eingriffsfreien Betrieb bewährt, der Benutzerentscheidungen weitgehend eliminiert. Wenn Sie Zugriff per einmaliger Anmeldung (SSO) ermöglichen, merken Ihre Endbenutzer im Endeffekt überhaupt nichts davon. Dank der Zwei-Faktor-Authentifizierung entsteht eine weitere Schutzebene, und es sind keine zusätzlichen Benutzernamen und Kennwörter erforderlich, was eine einfachere Bedienung erlaubt. Bei Verschlüsselungslösungen, die eine rollenbasierte Zugriffskontrolle (RBAC) ermöglichen, kann die Verschlüsselungsverwaltung zur Vereinfachung auf Rollen-/Funktionsbasis delegiert werden.

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 bewährten Vorgehensweisen halten und eine Lösung gewählt haben, die darüber hinaus eine Verschlüsselung auf Dateiebene vorsieht, stellt dies aber kein Problem dar.

Vorteile der Dateiverschlüsselung (FLE)

FLE arbeitet auf Dateisystemebene und ermöglicht nicht nur einen Schutz von „ruhenden" Daten, sondern auch von Daten, mit denen gearbeitet wird. Mit FLE können Sie bestimmte Dateien und Ordner auf jedem einzelnen Gerät verschlüsseln. Bei hochwertigen Lösungen bleiben die Dateien sogar dann verschlüsselt, wenn sie über das Netzwerk 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-Arbeitsmappen usw.) oder der Anwendung, mit der 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 fein abgestufte 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 außerdem eine effektive Steuerung und Kontrolle von Anwendungsrechten, sodass eindeutige Verschlüsselungsregeln für bestimmte Anwendungen 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 komplett sperren, z. B:
  - Sichere Backups erleichtern, 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.

3. VERSCHLÜSSELUNG VON WECHSELDATENTRÄGERN ERZWINGEN

USB-Flashlaufwerke erreichen mittlerweile Kapazitäten von über 100 GB, externe Festplatten, die kleiner sind als eine Hand, sogar mehrere Terabyte – ein riesige Menge potenziell sensibler Geschäftsdaten, die leicht abhanden kommen könnten, z. B. wenn Sie ein Laufwerk bei Abgabe in der Reinigung in der Jackentasche lassen, es bei der Sicherheitskontrolle am Flughafen vergessen, oder wenn es Ihnen aus der Tasche fällt.

Nachlässigkeiten und Zufälle lassen sich nicht beeinflussen, wohl aber die Konsequenzen, die sich aus ihnen ergeben.

Wirksame Verschlüsselungsstrategien sehen eigentlich auch immer eine Verschlüsselung von Wechseldatenträgern vor. Stellen Sie sicher, dass sensible 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 sensiblen Daten geschützt sind, selbst wenn sie abhanden kommen oder gestohlen werden.

Die effektivsten Verschlüsselungslösungen können mit Funktionen zur erweiterten Gerätekontrolle integriert werden. Auf diese Weise kann die Anwendung von Richtlinien bis hin zu bestimmten Geräteseriennummern abgestuft werden.

Beim Umgang mit sensiblen Daten sollte innerhalb wie außerhalb des Perimeters der so genannte „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.

Entscheiden Sie sich für bewährte und sichere Kryptografie

Ihre Verschlüsselungsstrategie ist nur so gut, wie die ihr zugrunde liegende Technologie. Leicht zu knackende Verschlüsselungsalgorithmen sind wertlos. Wählen Sie eine Verschlüsselungslösung mit Advanced Encryption Standard (AES) mit 256-Bit-Schlüssellänge, vereinfachter Schlüsselverwaltung und sicherer Aufbewahrung. Mit Unterstützung für die Intel® AES-NI-Technologie, UEFI- und GPT-Plattformen ist Ihre Lösung zukunftstauglich.

Der Schlüssel ist von entscheidender Bedeutung – 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.

Entscheiden Sie sich für mehrstufige Sicherheit

Endbenutzer und verlorene Geräte sind nicht die einzigen Gründe für einen Datenverlust. Datendiebe entwickeln zunehmend ausgeklügeltere Malware, die auf Ihren Systemen eingeschleust wird und Ihre Daten unauffällig entwendet. Oft wird solche Malware erst nach Jahren entdeckt. Durch Verschlüsselung lässt sich zwar erreichen, dass eventuell gestohlene Daten nutzlos sind, aber sie ist sehr viel effektiver, wenn sie im Rahmen einer breiteren, integrierten Sicherheitsstrategie eingesetzt wird. Dazu gehören qualitativ hochwertige Anti-Malware-Programme sowie Geräte- und Programmkontrollen, die zusammenarbeiten, um Kriminellen so wenige Chancen wie möglich für den Zugriff auf Systeme und den Diebstahl vertraulicher Daten zu bieten.

Keine Verschlüsselungsstrategie kommt ohne einen integrierten Malware-Schutz und Kontrollen aus, mit denen schädliche Codes ermittelt und außer Kraft gesetzt werden können. Gleichzeitig muss das System auf alle Arten von Schwachstellen gescannt werden, die einen Datenverlust für das Unternehmen bedeuten könnten. Und natürlich muss all dies mit minimalem Benutzereingriff vor sich gehen. Im Idealfall sollte der Benutzer gar nichts davon mitbekommen.

Kennwort vergessen?

Der durchschnittliche Benutzer vergisst sein Kennwort beinahe genauso oft, wie er seinen USB-Stick oder sein Smartphone verliert.

Und manchmal lässt Sie auch die zuverlässigste Hardware oder das beste Betriebssystem im Stich – und ohne Zugriff auf entscheidende Informationen. 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, das repariert werden muss.

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

Zentrale Verwaltung

Der Verschlüsselungstechnologie wird nachgesagt, dass ihre Implementierung und Verwaltung zu komplex sind. Dies ist in hohem Maße darauf zurückzuführen, dass herkömmliche, ältere Lösungen getrennt von Anti-Malware-Programmen und anderen IT-Sicherheitstechnologien bereitgestellt werden, was zu unnötig komplexen Systemen führt. Die Handhabung verschiedener Lösungen – Endpoint-Kontrolle, Anti-Malware und Verschlüsselung – ist, selbst wenn diese von einem Anbieter stammen , nicht nur teuer, sondern in allen Phasen der Bereitstellung auch sehr zeitaufwändig: Anschaffung, Mitarbeiterschulung, Provisioning, Richtlinienverwaltung, Wartung und Upgrades müssen für jede der Komponenten als getrenntes Projekt angelegt werden.

Eine vollständig integrierte, mehrstufige Sicherheitslösung spart nicht nur Zeit und Geld, sondern gestaltet die Softwarebereitstellung auch so einfach und problemlos 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 den Anti-Malware-Schutz, die Gerätesteuerung 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.

ZU GUTER LETZT ...

Mit Kaspersky Endpoint Security for Business werden bewährte Verschlüsselungspraktiken in Unternehmen aller Größenordnungen zur Realität.

Lückenlose Integration mit unserem vielfach ausgezeichneten Malware-Schutz und unseren Technologien für Endpoint-Kontrolle und -Verwaltung bietet echte mehrstufige Sicherheit, die auf einer gemeinsamen Codebasis aufbaut. Dies ermöglicht die Anwendung von Verschlüsselungseinstellungen im Rahmen derselben Richtlinie, die auch für den Malware-Schutz, die Gerätekontrolle und andere Aspekte der Endpoint-Sicherheit eingesetzt wird. Keine Notwendigkeit, verschiedene Lösungen bereitzustellen und zu verwalten. Die Kompatibilität der Netzwerkhardware wird automatisch überprüft, bevor die Verschlüsselung eingesetzt wird; Unterstützung für UEFI- und GPT-Plattformen ist Standard.

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 integrierte Sicherheitsplattform bietet.

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


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Lab ZAO, Moskau,
Russland
www.kaspersky.de

Informationen zur
Internetsicherheit:
www.viruslist.de

Informationen zu Partnern in Ihrer Nähe finden
Sie hier:
http://www.kaspersky.com/de/partner_finden

KASPERSKY lab