KASPERSKY lab

GLOBAL
SECURITY
INTELLIGENCE

IHRE DATEN SIND IN GEFAHR: SCHÜTZEN SIE SIE DURCH VERSCHLÜSSELUNG

#EnterpriseSec
kaspersky.com/enterprise

INHALTSVERZEICHNIS

IHRE DATEN SIND IN GEFAHR: SCHÜTZEN SIE SIE DURCH VERSCHLÜSSELUNG

Mit den geschäftlichen Anforderungen des Unternehmens Schritt zu halten, kann sich für IT-Manager als echte Herausforderung erweisen. Da Sie unter dem ständigen Druck stehen, mit weniger mehr zu erreichen, sehen Sie sich gezwungen, neue Technologien zum Einsatz zu bringen, um Produktivität und Effizienz zu steigern und die Kosten unter Kontrolle zu halten – und das alles vor dem Hintergrund einer ständig steigenden Bedrohung durch Cyberkriminalität. Zu allem Überfluss wird die Mitarbeiterschaft in Ihrem Unternehmen immer mobiler – und verlässt dabei die sicheren Grenzen des Unternehmens. Bei einer ausreichend mobilen Mitarbeiterschaft entsteht in einer IT-Abteilung leicht der Eindruck eines Belagerungszustands.

Laut einer Studie des Ponemon Institute sind bereits jetzt 62 % der Mitarbeiter in Unternehmen mobil, und dieser Wert soll bis 2015 auf 85 % ansteigen. Mit der wachsenden Mobilität seiner Mitarbeiter wird auch der Aktionsradius der Daten in einem Unternehmen erhöht – und mit ihm das Risiko von Datenverlust oder -diebstahl. Der robuste Verteidigungswall, den Sie zum Schutz der Unternehmenssysteme errichtet haben, hat an Effektivität verloren, weil die Daten, die er sichern soll, auf der ganzen Welt unterwegs sind. Es verwundert also nicht, dass 80% der IT-Profis in Unternehmen der Meinung sind, dass Laptops und andere mobile Geräte, auf denen Daten gespeichert werden, ein beträchtliches Risiko für Unternehmensnetzwerke und -systeme darstellen.[1]

Laut einer Studie von Intel werden 5 bis 10 % aller Laptops während ihrer Lebensdauer gestohlen bzw. kommen abhanden. Denken Sie einmal daran, wie viele Mitarbeiter in Ihrem Unternehmen bereits mobil arbeiten, und lassen Sie sich dann folgende Werte durch den Kopf gehen: Durchschnittlich 63 % von ihnen nutzen mobile Geräte, um auf Unternehmensdaten zuzugreifen und mit ihnen zu arbeiten.

- 50 % nutzen mobile Geräte für den Zugriff auf Daten, für die besondere Auflagen gelten.
- Auf 63 % der mobilen Geräte, die gestohlen werden oder anderweitig abhandenkommen, befinden sich vertrauliche Informationen.
- Alle 53 Sekunden wird ein Laptop gestohlen.
- 63 % aller Sicherheitslücken sind die Folge der Nutzung mobiler Geräte, wobei Diebstahl und unbefugte Nutzung am Arbeitsplatz zu den Hauptursachen zählen.[2]

Der rasante Anstieg der Mobilität in Unternehmen bedeutet, dass unternehmenseigene Daten einem erheblichen Risiko ausgesetzt sind.

Auch wenn Sie angesichts Geräteverlusten oder -diebstählen zuerst an die Kosten für den Ersatz der Geräte denken, liegen die eigentlichen Risiken doch woanders. Das Ponemon Institute schätzt den finanziellen Verlust, der durch einen abhanden gekommenen Laptop entsteht, auf 49.246 US-Dollar, wobei die Ersatzkosten für das Gerät lediglich zwei Prozent ausmachen. Die Bereinigung des entstandenen Datenlecks macht mehr als 80 Prozent der Folgekosten aus – unabhängig von der Größe des betroffenen Unternehmens.

Kaspersky Lab schätzt die durchschnittlichen Kosten, die einem Unternehmen bei einer einzigen schwerwiegenden Datenschutzverletzung entstehen, auf 649.000 US-Dollar.[3]

1 & 2. Ponemon Institute, 2013 State of the Endpoint, Dezember 2012
3. Kaspersky Lab, Global Corporate IT Security Risks: 2013, Mai 2013

DIE VERSCHLÜSSELUNG GEHÖRT ZU DEN VIELVERSPRECHENDSTEN TECHNOLOGIEN, UM DAS RISIKO KRITISCHER DATENLECKS ZU VERRINGERN. SIE IST ABER ERST DANN MAXIMAL EFFEKTIV, WENN SIE IN EIN UMFASSENDES SICHERHEITSSYSTEM ZUM SCHUTZ DER IT-UNTERNEHMENSINFRASTRUKTUR INTEGRIERT WIRD

NIKOLAY GREBENNIKOV, CTO VON KASPERSKY LAB

Rechnen Sie nun noch den ständig anwachsenden Bußgeldkatalog für Datensicherheitsverletzungen, den Imageschaden und die Auswirkung auf die Kundeloyalität hinzu, und es wird schnell klar, dass die Kosten für einen verlorenen Laptop weit über die Geräteersatzkosten hinausgehen.

In einer Welt, die immer mobiler wird, kann der Schutz von geistigem Eigentum, vertraulichen Daten, Netzwerken und Systemen nicht mehr allein durch Perimetersicherheit gewährleistet werden. Kommt ein Gerät abhanden oder wird es gestohlen, sind auch die darauf gespeicherten Daten in Gefahr, wodurch das Gerät zu einer beliebten Beute für Kriminelle wird. Wie aber schützen Sie mobile Daten vor Diebstahl, wenn das Gerät selbst gestohlen wurde?

DIE ANTWORT IST GANZ EINFACH: DURCH VERSCHLÜSSELUNG!

Verschlüsselung ist ein Verfahren, mit dem Informationen so codiert werden, dass nur befugte Benutzer etwas mit ihnen anfangen können. In einem Verschlüsselungsmodell werden beispielsweise Informationen im Nur-Text-Format mithilfe eines Algorithmus verschlüsselt und auf diese Weise in unleserlichen Chiffretext umgewandelt. Hierzu wird in der Regel ein Verschlüsselungscode (Schlüssel) verwendet, der angibt, wie die Daten zu kodieren sind.

Unbefugte Benutzer können zwar den Chiffretext lesen, dieser lässt aber nichts von den ursprünglichen Daten erkennen. Befugte Benutzer können den Chiffretext jedoch mithilfe eines speziellen Algorithmus entschlüsseln, für den ein Entschlüsselungscode erforderlich ist, auf den nur sie Zugriff haben. Für ein Verschlüsselungsmodell ist in der Regel ein Algorithmus erforderlich, mit dem die Ver- und Entschlüsselungscodes generiert werden.

Gartner schätzt, dass die Kosten eines Datenlecks durch einen abhanden gekommenen oder gestohlenen Laptop die Kosten für eine unternehmensweite Verschlüsselungslösung um das bis zu Siebzigfache übersteigen können[4]. Eine Studie von Kaspersky Lab ergab jedoch, dass 35 % der Unternehmen ihre Daten dem Risiko unbefugten Zugriffs aussetzen, weil sie auf den Einsatz von Verschlüsselungstechnologien verzichten.[5]

Welche Motivation sie auch haben mögen, für Unternehmen ist es zwingend erforderlich, ihre Daten, ihr geistiges Eigentum und ihren guten Ruf zu schützen. Unternehmen aus allen Bereichen und Sektoren interessieren sich zunehmend für die Verschlüsselung, sowohl als vorbeugende Maßnahme der Informationssicherheit als auch als Strategie zur Erreichung von Compliance.

Es gibt zwei unterschiedliche Verschlüsselungstypen, die entweder getrennt voneinander oder zusammen eingesetzt werden können: die Full-Disk-Verschlüsselung (Full Disk Encryption, FDE) und die File-Level-Verschlüsselung (File Level Encryption, FLE). Eine Studie von Kaspersky Lab hat ergeben, dass in 40 % der befragten Unternehmen FLE zum Einsatz kommt, 39 % sich für FDE entschieden haben und 33 % ein Verschlüsselungsverfahren für Wechseldatenträger nutzen.

4. Gartner-Analyst John Girard, Interview mit Fierce Mobile IT, 25. Oktober 2012. http://www.fiercemobileit.com/story/laptop-data-breach-can-cost-70-times-more-firm-wide-encryption/2012-10-25, 25. Oktober 2012
5. Kaspersky Lab und B2B International, Global IT Risk Report: 2013, Mai 2013

MASSNAHMEN ZUR RISIKOMINDERUNG

Studien von Kaspersky Lab belegen, dass die Privatwirtschaft sich zunehmend für die Verschlüsselung als Teil einer vorbeugenden Strategie zur Vermeidung von Datenverlusten interessiert.

Schutz vor Malware (Viren, Spyware)	71 %	4 %
Regelmäßige Verwaltung von Patches/Software-Updates	54 %	-9 %
Einrichtung von Zugriffsebenen auf verschiedene IT-Systeme nach Berechtigung	52 %	4 %
Netzwerkstrukturen (z. B. Trennung wichtiger Netzwerke von weniger wichtigen)	50 %	3 %
Programmkontrolle (d. h. es können nur genehmigte Programme auf einem Gerät ausgeführt werden)	45 %	k. A.
Richtlinie zur IT-Sicherheit an entfernten Standorten/Niederlassungen	44 %	4 %
Gerätekontrolle (d. h. Kontrolle darüber, welche Peripheriegeräte mit einem Gerät verbunden werden dürfen)	41 %	k. A.
Anti-Malware-Agent für mobile Geräte	40 %	k. A.
File/Folder-Level-Verschlüsselung	**40 %**	**k. A.**
Verschlüsselung aller gespeicherten Daten (z. B. Full-Disk-Verschlüsselung)	**39 %**	**2 %**
Eigene Sicherheitsrichtlinie für Notebooks	38 %	3 %
Eigene Sicherheitsrichtlinie für abnehmbare/tragbare Geräte (z. B. USB-Geräte)	37 %	0 %
Verschlüsselung der Unternehmenskommunikation	**37 %**	**-1 %**
Prüfung der IT-Sicherheit von Drittanbietern	36 %	0 %
Client-Management (PC-Lifecycle-Management)	34 %	-1 %
Verschlüsselung der Daten auf mobilen Geräten	**33 %**	**2 %**
Eigene Sicherheitsrichtlinie für Smartphones/Tablet-Computer	32 %	0 %
Mobile Device Management (MDM)	31 %	-2 %

k. A.: Probleme sind in **2013 erstmals aufgetreten**

Die Abbildung zeigt den Prozentsatz der Unternehmen, die verschiedene Sicherheitsmaßnahmen **vollständig** umgesetzt haben.

Viel niedriger (Vorjahresvergleich)

Viel höher (Vorjahresvergleich)

FULL-DISK-VERSCHLÜSSELUNG (FDE)

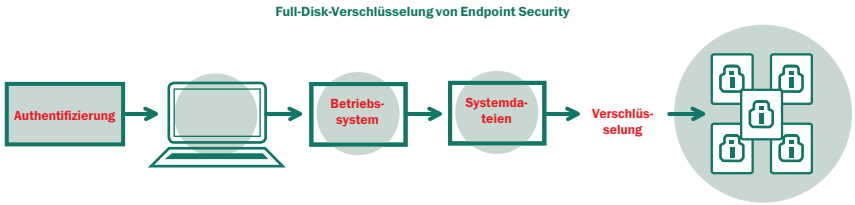
Die FDE-Technologie ist eine der wirksamsten Methoden für Unternehmen, ihre Daten bei Diebstahl oder Verlust zu schützen. Unabhängig davon, was letztendlich mit einem Gerät passiert, kann mit dem FDE-Verfahren sichergestellt werden, dass alle vertraulichen Unternehmensdaten für Kriminelle oder auch nur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

FDE verschlüsselt alle Daten (d. h. sämtliche Daten auf der Festplatte) von der Betriebssystempartition bis hin zu den zusätzlichen Festplatten. Im Grunde wird jede einzelne Datei (einschließlich der temporären Dateien) auf jedem einzelnen Sektor des Datenträgers verschlüsselt. Nur authentifizierte Benutzer haben Zugriff auf das System, entweder über ein Kennwort, ein Token oder eine Kombination aus beiden. Die Technologie lässt sich auch auf Wechseldatenträger, z. B. USB-Laufwerke, anwenden. FDE unterstützt unterschiedliche Setups und kann vom Systemadministrator verwaltet und überwacht werden.

Die FDE-Funktionalität basiert auf einem Pre-Boot-Mechanismus. Dies bedeutet, dass sämtliche Daten auf einem Gerät ab dem Zeitpunkt geschützt werden, ab dem der Benutzer das Gerät einschaltet. Die Software verschlüsselt alle ausgewählten Laufwerke und installiert ein Autorisierungsmodul in der Systemstartumgebung. Beim Systemstart eines Computers wird das Betriebssystem automatisch in eine verschlüsselte Umgebung geladen. Die Verschlüsselung wird also standardmäßig aktiviert, ohne eine nennenswerte Auswirkung auf die Systemleistung des Computers zu haben.

Sämtliche Ver- und Entschlüsselungsvorgänge laufen unabhängig von der verwendeten Software routinemäßig und transparent für den Benutzer ab. Auch die Lese-/Schreibvorgänge laufen in dieser vollständig geschützten Umgebung ab. Alles auf der Festplatte wird verschlüsselt, von den Auslagerungs- über die System-, Seiten-, Ruhezustand- bis zu den temporären Dateien, die oft auch wichtige vertrauliche Informationen enthalten. Ist ein Kennwort verloren gegangen, können die Informationen dennoch mit privaten Schlüsseln entschlüsselt werden, die nur dem Systemadministrator bekannt sind. Mit mobilen Geräten, die mit FDE arbeiten, lässt sich das Risiko von Datenlecks durch Verlust oder Diebstahl erheblich reduzieren.

Die FDE-Funktion ist standardmäßig in Kaspersky Endpoint Security for Business enthalten. Sie kann von der zentralen Verwaltungskonsole im Kaspersky Security Center aus verwaltet werden.



DIE FULL-DISK-VERSCHLÜSSELUNG BRINGT EINE REIHE VON VORTEILEN FÜR DIE IT-SICHERHEIT:

- **Obligatorische Verschlüsselung von vertraulichen Daten**: FDE nimmt dem Endbenutzer die Entscheidung ab, ob verschlüsselt wird oder nicht. Sämtliche Dateien auf der Festplatte werden automatisch verschlüsselt und per Kennwort geschützt, einschließlich temporärer Dateien, die oft vertrauliche Daten enthalten. Der Endbenutzer hat keine Möglichkeit, die Funktion außer Kraft zu setzen.

- **Sicherheit**: FDE verhindert mithilfe einer Benutzername/Kennwort-Funktion den unbefugten Zugriff auf Daten. Wird die korrekte Kombination aus Benutzername und Kennwort eingegeben, ruft das System den erforderlichen Schlüssel ab, um die Dateien auf der Festplatte zu entschlüsseln. Dies sorgt für zusätzliche Sicherheit, da die Daten unmittelbar nach Zerstörung des Kryptographieschlüssels unbrauchbar werden.

- **Zentrale Schlüsselverwaltung**: Die Verschlüsselungscodes werden in einem zentralen Repository gespeichert, zu dem nur der Sicherheitsadministrator Zugriff hat.

- **Zentrale Verwaltung der Verschlüsselung**: Sämtliche Funktionen für FDE-Systeme können innerhalb des Unternehmens zentral verwaltet werden. Hierzu gehören die Verwaltung der Entschlüsselungscodes, die Zugangskontrolle für mobile Geräte, ggf. Sperrungen, Reporting und die Wiederherstellung verlorener Kennwörter.

- **Einfachheit und Flexibilität**: FDE-Systeme arbeiten mit vollständig automatisierten, für den Endbenutzer transparenten Abläufen. Nach erfolgter Authentifizierung verläuft der Ver-/Entschlüsselungsvorgang vollständig transparent und ohne Beeinträchtigung der Anwenderfreundlichkeit.

- **Zentrale Datenwiederherstellung**: Bei Verlust von Kennwörtern oder Beschädigung des Datenträgers lassen sich die Daten mithilfe eines speziellen, zentral verwalteten Notfallwiederherstellungsverfahren trotzdem wiederherstellen und entschlüsseln.

Obwohl FDE für Daten auf verloren gegangenen oder gestohlenen Geräten ausreichenden Schutz bietet, werden Daten während der Übertragung nicht geschützt, d. h. Daten, die elektronisch von einem Gerät an ein anderes übermittelt werden, z. B. per E-Mail. Aus diesem Grund wird in vielen Unternehmen die File-Level-Verschlüsselung genutzt.

FILE-LEVEL-VERSCHLÜSSELUNG (FLE)

BEI FLE WERDEN EINZELNE DATEIEN ODER VERZEICHNISSE DURCH DAS DATEISYSTEM SELBST VERSCHLÜSSELT. DIES STEHT IM GEGENSATZ ZUR FULL-DISK-VERSCHLÜSSELUNG, BEI DER DIE PARTITION ODER DER DATENTRÄGER, AUF DEM SICH DAS DATEISYSTEM BEFINDET, KOMPLETT VERSCHLÜSSELT WIRD. FLE VERSCHLÜSSELT NICHT ALLE DATEN AUF EINER FESTPLATTE ODER EINEM WECHSELDATENTRÄGER, WIE ES BEI FDE DER FALL IST.

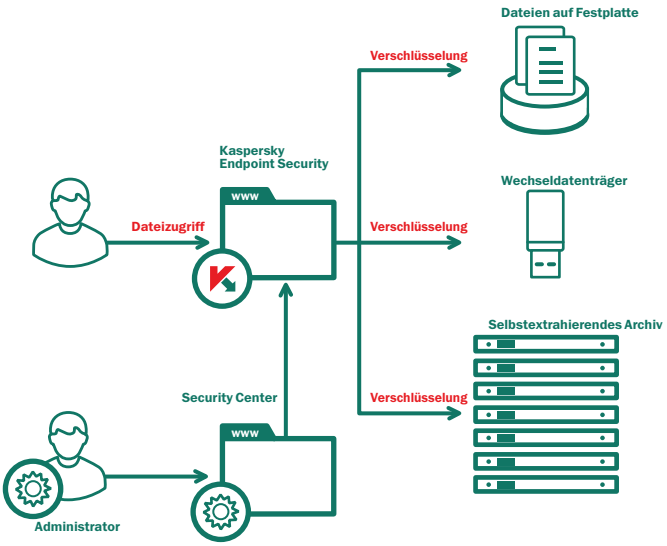
Die File-Level-Verschlüsselung (FLE) ermöglicht die Verschlüsselung von Daten in ausgewählten Dateien und Ordnern auf einem bestimmten Gerät. Hierdurch können Daten für unbefugte Benutzer gezielt unlesbar gemacht werden, egal wo sie gespeichert werden. Mit FLE können Systemadministratoren Dateien automatisch auf der Grundlage von Speicherort und Dateityp verschlüsseln lassen.

Bei FLE werden einzelne Dateien oder Verzeichnisse durch das Dateisystem selbst verschlüsselt. Dies steht im Gegensatz zur Full-Disk-Verschlüsselung, bei der die Partition oder der Datenträger, auf dem sich das Dateisystem befindet, komplett verschlüsselt wird. FLE verschlüsselt nicht alle Daten auf einer Festplatte oder einem Wechseldatenträger, wie es bei FDE der Fall ist. Der Administrator hat die Wahl, welche Daten verschlüsselt werden sollen und welche nicht. Hierzu werden Richtlinien genutzt, die über eine benutzerfreundliche Softwareoberfläche umgesetzt werden.

Mit der FLE-Technologie kann der Systemadministrator bis ins Detail hinein anpassen, welche Dateien verschlüsselt werden sollen. Dies kann manuell oder automatisch erledigt werden. Einige Lösungen stellen spezielle, vorkonfigurierte Tools bereit, mit denen Dateien einfach, schnell und zuverlässig verschlüsselt werden können. Die fein abgestuften Richtlinien für den Zugriff auf die Daten sind leicht anzuwenden. So könnten beispielsweise Arbeitsmappen mit Finanzdaten obligatorisch verschlüsselt werden, allgemeinere Informationen jedoch nicht. Verschlüsselungsrichtlinien können individuell angepasst werden, um festzulegen, was zu welchem Zeitpunkt verschlüsselt werden soll. Hier einige Beispiele:

- **Dateien auf lokalen Festplatten**: Administratoren könnten Listen mit zu verschlüsselnden Dateien zusammen mit Name, Erweiterung und Verzeichnis erstellen.
- **Dateien auf Wechseldatenträger**: Erstellen Sie eine Standardverschlüsselungsrichtlinie, um die Verschlüsselung aller Wechseldatenträger zu erzwingen. Wenden Sie dieselben Regeln auf jedes der Geräte an, oder legen Sie für jedes der Geräte unterschiedliche Regeln fest.
- **Auswählen, was verschlüsselt werden soll**: FLE ermöglicht je nach Bedarf die Anwendung unterschiedlicher Verschlüsselungsregeln. Sie können beispielsweise festlegen, alle Dateien auf einem Wechseldatenträger zu verschlüsseln oder nur die neuen. Es gibt außerdem den „portablen Modus“ für verschlüsselte Dateien auf PCs, auf denen Kaspersky Endpoint Security for Business nicht installiert ist.
- **Dateien von Anwendungen**: Lassen Sie automatisch alle Dateien verschlüsseln, die mithilfe einer beliebigen Anwendung erstellt oder geändert wurden.
- **Selbstextrahierende Archive**: Dateien, die zu selbstextrahierenden, verschlüsselten Archiven hinzugefügt werden, können mit einem Kennwort entschlüsselt werden, auch wenn auf dem betreffenden PC Kaspersky Endpoint Security nicht installiert ist.

DIE DATEIVERSCHLÜSSELUNG IST TRANSPARENT, D. H. DASS JEDER MIT ZUGANG ZUM DATEISYSTEM DIE NAMEN (UND MÖGLICHERWEISE AUCH ANDERE METADATEN) DER VERSCHLÜSSELTEN DATEIEN UND ORDNER EINSEHEN KANN, INKLUSIVE DER DATEIEN UND ORDNER INNERHALB DER VERSCHLÜSSELTEN ORDNER, WENN DIESE NICHT DURCH BETRIEBSSYSTEMEIGENE ZUGANGSKONTROLLFUNKTIONEN GESCHÜTZT WERDEN. DIE DATEI-/ORDNERVERSCHLÜSSELUNG WIRD AUF ALLEN ARTEN VON SPEICHERMEDIEN FÜR ENDBENUTZERGERÄTE EINGESETZT.



Bei der Dateiverschlüsselung werden einzelne Dateien auf beliebigen Speichermedien verschlüsselt; der Zugriff auf die verschlüsselten Daten ist dann nur noch mithilfe der korrekten Authentifizierung möglich. Bei der Ordnerverschlüsselung wird dieses Prinzip nicht auf einzelne Dateien, sondern auf Ordner angewendet.

Die Dateiverschlüsselung ist transparent, d. h. dass jeder mit Zugang zum Dateisystem die Namen (und möglicherweise auch andere Metadaten) der verschlüsselten Dateien und Ordner einsehen kann, inklusive der Dateien und Ordner innerhalb der verschlüsselten Ordner, wenn diese nicht durch betriebssystemeigene Zugangskontrollfunktionen geschützt werden. Die Datei-/Ordnerverschlüsselung wird auf allen Arten von Speichermedien für Endbenutzergeräte eingesetzt.

Die Dateiverschlüsselung wird über eine treiberbasierte Lösung implementiert, die ein spezielles Kryptomodul besitzt, mit dem alle Dateizugriffsvorgänge abgefangen werden. Beim Zugriff auf eine verschlüsselte Datei (bzw. eine Datei in einem verschlüsselten Ordner) überprüft die FLE-Anwendung, ob der Benutzer erfolgreich authentifiziert wurde, oder öffnet im Fall eines selbstextrahierenden Archivs eine Kennwortabfrage. Nach erfolgter Authentifizierung wird die gewünschte Datei automatisch von der Software entschlüsselt.

Da die FLE-Software die Dateien einzeln entschlüsselt, ist die Beeinträchtigung der Systemleistung vernachlässigbar. Die Datei-/Ordnerverschlüsselung wird in der Regel für Benutzerdatendateien eingesetzt, also für Textdokumente oder Tabellenblätter. FLE-Lösungen sind nicht in der Lage, Betriebssystem- oder Ruhezustandsdateien zu verschlüsseln.

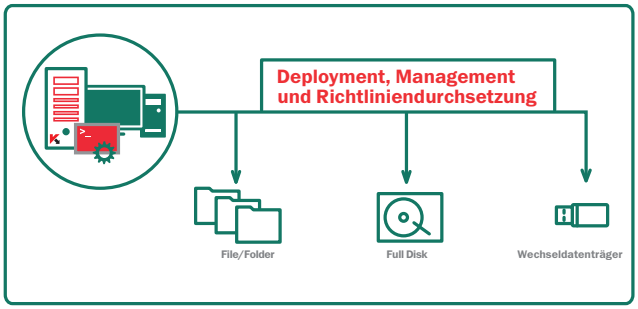
FLE bietet eine Reihe von Vorteilen für die IT-Sicherheit:

- **Flexibilität**: Individuell gestaltbare Richtlinien für Dateityp und Verzeichnis (Dateien, Erweiterungen und Verzeichnisse) lassen sich für unterschiedliche Anwendungsfälle und Anforderungen erstellen.
- **Unterstützung von Wechseldatenträgern**: Spezielle Verschlüsselungsrichtlinien für alle Wechseldatenträger, die an einen PC/Laptop angeschlossen werden. Wenden Sie dieselben Regeln global an, oder wählen Sie je nach Gerät unterschiedliche Optionen aus.
- **Transparente Softwareverschlüsselung**: Verschlüsselung von Daten, die von einer beliebigen Software auf der Festplatte erstellt oder geändert werden. Definieren Sie entweder programmabhängige Zugriffsrechte für verschlüsselte Dateien, oder ermöglichen Sie den Zugriff nur auf den Chiffretext.
- **Zentrale Verwaltung**: Sämtliche Dateiverschlüsselungsfunktionen können zentral verwaltet werden, darunter auch die Richtlinien, Rechte- und Schlüsselverwaltung.

Schützen Sie Ihre Daten einfach und sicher mit der Verschlüsselungstechnologie von Kaspersky Lab

- FULL DISK
- FILE-/FOLDER-LEVEL
- WECHSELDATENTRÄGER/ INTERNE GERÄTE

ÜBER EINE EINZIGE VERWALTUNGSKONSOLE VERWALTET.



ZUSAMMENFASSUNG

Eine mobile Mitarbeiterschaft muss für die Absicherung von Unternehmensdaten nicht zwangsläufig eine neue Herausforderung bedeuten. Für die Absicherung von Daten auf den besonders gefährdeten mobilen Geräten Verschlüsselungstechniken einzusetzen, ist folgerichtig, kann aber erhöhten organisatorischen Aufwand nach sich ziehen. Ein einfacher Weg, dies zu vermeiden, besteht in der Implementierung von Verschlüsselungstechnologien als Teil einer umfassenden Sicherheitsplattform, die vollständig integrierte Technologien und Tools, z. B. zuverlässigen Malware-Schutz, Kontroll-Tools, Systems Management, Mobile Device Management und Verschlüsselung, in einer benutzerfreundlichen Lösung vereint. Dies ermöglicht eine vollständige Transparenz der bestehenden Risiken für alle Geräte in einem Unternehmen – alles durch eine einmalige Investition und von einer zentralen Verwaltungskonsole aus.

Kaspersky Endpoint Security for Business (KESB) ermöglicht eine zuverlässige Datenverschlüsselung für alle Geräte von einer zentralen Konsole aus, wodurch Sie den Aufwand und das Risiko für Ihr Unternehmen verringern. Außerdem ermöglichen uns das Kaspersky Security Network sowie die international anerkannten Threat Research and Global Research and Analysis Teams (GReAT) eine umfassende Sicht auf Millionen von Bedrohungen aus allen Teilen der Welt. Diese Informationen sorgen dafür, dass wir Sicherheitsvorfälle erkennen und häufig vorhersagen können, und dazu beitragen, dass Unternehmen einen besseren Schutz und einen aktiven Sicherheitsansatz realisieren können. Wir konzentrieren unsere Bemühungen auf die Lösung globaler Probleme im IT-Sicherheitsbereich – vom kritischen Infrastrukturschutz, über Enterprise Mobility und sichere Virtualisierung bis hin zu Betrugsprävention und Sicherheitsinformationsdiensten.

Kaspersky Lab hat sich langfristig der Antizipation und Verhinderung von IT-Sicherheitsrisiken verschrieben, um das Risiko für Unternehmen heute und in einer immer komplexer werdenden Zukunft zu reduzieren.

Über Kaspersky Lab

Kaspersky Lab ist der weltweit größte Privatanbieter von Lösungen für den Schutz von Endpoints. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer*. In seiner 16-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Einzelverbrauchern wirksame digitale Lösungen für die Datensicherheit. Der Hauptsitz des Unternehmens ist in Großbritannien registriert. Kaspersky Lab ist zurzeit in nahezu 200 Ländern und Regionen weltweit tätig und sorgt für den Schutz von mehr als 300 Millionen Anwendern weltweit.

Weitere Informationen erhalten Sie unter www.kaspersky.de.

* Das Unternehmen belegte im Rahmen des IDC-Rating „Worldwide Endpoint Security Revenue by Vendor 2012“ den vierten Rang. Die Rangfolge wurde im IDC-Bericht „Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares“ (IDC Nr. 242618, August 2013) veröffentlicht. In dem Bericht wurden Softwarehersteller auf Grundlage ihrer Erlöse aus dem Verkauf von Sicherheitslösungen für Endpoints im Jahr 2012 eingestuft.