

Schutz vor Datenverlust

IIIIII Sichere Lösung auf Smart Card-Basis verbessert die Endpunktkontrolle und Desktopverschlüsselung



UNTERNEHMEN > LÖSUNG

Datenverlust am virtuellen Arbeitsplatz verhindern

Unternehmen und Behörden sind auf digitale Informationen angewiesen: was ihr operatives Geschäft angeht ebenso wie bei der internen und externen Kommunikation. Gelingt es Unternehmen, die Datenflut effizient zu nutzen, können sie einen Wettbewerbsvorteil und daraus resultierende Produktivitäts- und Wirtschaftlichkeitsgewinne realisieren. Gleichzeitig müssen sich Unternehmen immer häufiger mit Datensicherheitsproblemen und möglichen Haftungsfällen auseinandersetzen, wenn sie den On-Demand-Zugriff auf sensible Daten gewähren, egal ob inner- oder außerhalb der traditionellen Netzwerk Grenzen.

Heute können Mitarbeiter über Desktop-PCs, Macs, Thin Clients, Laptops, PDAs, Smartphones und Internetterminals rund um die Uhr auf Netzwerkdaten und persönliche Dateien zugreifen. Die Datenmobilität nimmt permanent zu; leistungsstarke, mobile Speichermedien können bereits mehrere Gigabytes an Daten speichern. Über FireWire-, Bluetooth- und USB-Protokolle lassen sich innerhalb kürzester Zeit Verbindungen zu den Storage-Systemen von Unternehmen herstellen – sowohl berechtigt als auch unberechtigt.

Der Schutz der Unmengen an privaten und vertraulichen Daten, die in Unternehmen und Behörden anfallen, ist inzwischen zu einer wichtigen Aufgabe im Bereich IT und Datensicherheit geworden. Die finanziellen Auswirkungen infolge von Datenverlusten in Unternehmen können enorm sein, so dass es nicht weniger als eine wirtschaftliche Notwendigkeit ist, dieses Risiko weitestgehend zu verringern. Eine im Jahr 2009 vom Ponemon Institute durchgeführte Untersuchung ergab, dass sich die durchschnittlichen Kosten eines einzelnen Falls von Datendiebstahl im Jahr 2008 auf 6,65 Millionen US-Dollar beliefen. Hierin sind die Kosten, die durch Kundenabwanderung aufgrund eines solchen Vorfalles entstehen, noch nicht einmal inbegriffen. Der Datenschutz im gesamten Unternehmensnetz ist zudem notwendig, um gesetzliche Vorschriften und branchenspezifische Bestimmungen zum Schutz der Kundendaten zu erfüllen.

Die Kontrolle des Netzwerkzugriffs allein reicht als Schutzmechanismus für sensible Daten allerdings nicht mehr aus. Aufgrund der weiten Verbreitung von Laptops, tragbaren Speichermedien und elektronischem Dokumentenaustausch müssen Unternehmensdaten unabhängig von ihrem Speicherort geschützt sein – egal, ob sie auf Festplatten gespeichert sind, auf mobile Speichermedien heruntergeladen oder über E-Mail- bzw. FTP-Verbindungen übertragen werden.

Schutz von Daten unabhängig vom Speicherort

Lösungen zum Schutz vor Datenverlust wie zum Beispiel Endpunktkontrolle und Desktopverschlüsselung tragen dazu bei, die Gefahr des Verlusts bzw. Diebstahls sensibler Daten zu minimieren. Systeme zur Endpunktkontrolle verwalten nicht nur Netzwerkclients, also Laptops, Desktop-PCs und Peripheriegeräte, sondern kontrollieren auch die lokale bzw. netzwerkgestützte Verarbeitung der Daten. Diese Systeme sind zudem in der Lage, den Datenzugriff über Wechselmedien, wie zum Beispiel USB-Geräte, zu überprüfen und Rechte für jedes einzelne Gerät festzulegen.

Die Desktopverschlüsselung schützt sensible Daten, gespeichert und auch bei der Übertragung, sodass nur vorher festgelegte Benutzer mit den angeforderten Zugangsdaten auf sie zugreifen können. Abhängig von den Sicherheitsanforderungen eines Unternehmens kann die Desktopverschlüsselung in verschiedenen Stufen der Datenspeicherung zum Einsatz kommen. Zu den am weitesten verbreiteten Anwendungen zur Desktopverschlüsselung gehören Datei-, Festplatten- und E-Mail-Verschlüsselungen. Auch Laptops und mobile Speichermedien können zum Schutz vor Datenverlust verschlüsselt werden.

Schutz vor Datenverlust

IIIIII Sichere Lösung auf Smart Card-Basis verbessert die Endpunktkontrolle und Desktopverschlüsselung

Leistungsstärkere Lösungen zum Schutz vor Datenverlust

Was die Datensicherheit angeht, zählen USB-Sticks mit Speicherkapazitäten von 32 GB und mehr zu den Hauptgefahrenquellen. Viele Arbeitnehmer verwenden sie zum Speichern vertraulicher Daten, doch aufgrund ihrer geringen Größe gehen sie leicht verloren oder werden gestohlen. Anwendungen zur Verschlüsselung und Endpunktkontrolle, die in verschlüsselte USB-Laufwerke integriert sind, sowie personalisierte und auf mehrere Faktoren beruhende Sicherheitssysteme steigern die Effizienz von unternehmensweiten Lösungen zum Schutz vor Datenverlust. Mit ihrer erhöhten Sicherheit für mobile Daten und das personalisierte Verschlüsselungstool bieten diese Lösungen viele Vorteile, darunter:

- **Umsetzung von Sicherheitsrichtlinien für Wechselmedien.** Selbst bei Verlust oder Diebstahl eines Laufwerks ist der unberechtigte Zugriff auf Daten unmöglich.
- **Erhöhte Sicherheit für die Desktopverschlüsselung.**

Verschlüsselungsschlüssel sind besser geschützt, wenn sie auf einer sicheren Plattform, wie zum Beispiel einer in den USB-Token integrierten Smart Card, generiert und gespeichert werden. Dies ermöglicht auch die Zwei-Faktoren-Authentifizierung, die auf den Komponenten Besitz und Wissen basiert: Der Zugriff ist nur mit USB-Token und PIN-Code möglich.

- **Mobiler Zugriff auf Zugangsdaten.** Wenn die Verschlüsselungsschlüssel und die PKI-Zugangsdaten auf einem tragbaren Gerät gespeichert sind, kann man von jedem beliebigen Desktop-PC auf seine verschlüsselten Dateien zugreifen.
- **Einfache Handhabung.** Zum Verschlüsseln bzw. Entschlüsseln von Dateien wird lediglich ein PIN-Code benötigt.
- **Langfristiger Nutzen der Investition.** Da die PKI-Zertifikate aller führenden Zertifizierungsstellen unterstützt werden, verlängert sich der Lebenszyklus dieser Investition.
- **Verbesserter ROI dank flexibler Plattform für verschiedene Anwendungen.** Ein einziger, personalisierter USB-Token kann für verschiedene Sicherheitsanwendungen eingesetzt werden.



Smart Guardian – Funktionen:

- > Plug & Play ohne lokale Softwareinstallation; für den Einsatz unter verschiedenen Betriebssystemen geeignet
- > Autorisierte Plattform für Lösungen zur Endpunktkontrolle
- > Unterstützt PKCS#11-basierende Smart Card-Funktionalität und Authentifizierung mit Einmal-Passwort
- > Zertifizierung gemäß FIPS 140-2, Level 3
- > Erhältlich mit 2 und 4 GB Speicherkapazität
- > Intuitive und benutzerfreundliche, grafische Benutzeroberfläche

Stellen Sie sich den Herausforderungen mit Protiva™ Smart Guardian

Als weltweit führender Anbieter von digitalen Sicherheitslösungen bietet Gemalto äußerst sichere, Smart Card-basierende USB-Token. Diese bieten als Plattform zum Schutz vor Datenverlust einzigartige Sicherheit und Flexibilität. Protiva Smart Guardian basiert auf führenden Produkten im Bereich der Endpunktkontrolle und Desktopverschlüsselung. Die Speicher dieser Token sind Smart Card-verschlüsselt und mit Kapazitäten von 2 und 4 GB erhältlich.

Die Kombination aus Endpunktkontrolle und sicherer Datenspeicherung macht Smart Guardian zur idealen Lösung, um sensible Daten zu schützen sowie um zu überwachen, wie diese an den virtuellen Arbeitsplatz übertragen werden bzw. in die Unternehmenssysteme zurückfließen. Verglichen mit anderen verschlüsselten USB-Speichergeräten bieten sie ein einzigartiges Sicherheitsniveau, da alle wichtigen Funktionen und Verschlüsselungsschlüssel in der sicheren Umgebung des Smart Card-Moduls verwaltet werden. Zudem trägt auch die Zwei-Faktoren-Authentifizierung dazu bei, bestehende Sicherheitsrichtlinien

umzusetzen, sodass nur berechtigte Anwender auf die verschlüsselten Daten zugreifen können. Dies ist besonders wichtig, wenn ein Gerät verloren geht oder gestohlen wird.

Einfache Implementierung und Handhabung, reibungsloser Support

IT-Administratoren können die Protiva Smart Guardian-Token problemlos implementieren und verwalten; Anwender benötigen für den Einsatz keinerlei Schulungen. Die Token unterstützen eine Vielzahl von Betriebssystemen und erfordern keine Treiber. Die Einbindung in bestehende Infrastrukturen kann somit schnell und effizient erfolgen. Da die Geräte mit vielen Systemen kompatibel sind und das USB-Protokoll unterstützen, können Anwender von jedem Desktop-PC aus auf ihre Daten zugreifen, selbst wenn sie nicht mit dem Netzwerk verbunden sind.

Dazu schließen sie einfach ihren registrierten mobilen Token an die USB-Schnittstelle an und geben ihren PIN-Code ein, um Dateien zu ver- bzw. entschlüsseln. Wird der PIN-Code häufiger als zuvor festgelegt falsch eingegeben, sperrt sich das Gerät und ist somit gegen Brute-Force-Angriffe und unberechtigte Zugriffe auf die Verschlüsselungsschlüssel geschützt. Ein Administrator kann es dann gegebenenfalls lokal oder aus der Ferne über ein PKI-basiertes Challenge-Response-Verfahren wieder entsperren.

Eine Plattform für die Zukunft

Protiva Smart Guardian von Gemalto ist darüber hinaus eine stabile Plattform, mit der Unternehmen ihre IT-Sicherheitsrichtlinien gemäß den steigenden Anforderungen ausweiten können. Da sich die Speicher partitionieren lassen und die Standard-PKI-Zertifikate aller führenden Zertifizierungsstellen wie zum Beispiel Microsoft® Windows® Certificate Services unterstützt werden, können die Geräte über ein sicheres, mobiles VPN auch für künftige Anwendungen, z. B. Authentifizierungen, digitale Signaturen, sicheren Remote-Zugriff und mobile Verwaltungslösungen, genutzt werden.

Entdecken Sie die neue Dimension der Datensicherheit mit den Smart Guardian-USB-Token unter www.gemalto.com/enterprise