

Transparente Multi-Nutzer Verschlüsselungssysteme

Einzigartiger Schutz von vertraulichen Dateien gegen unberechtigten internen und externen Zugriff

Die meisten Schutzmaßnahmen sind auf Bedrohungen von außen ausgerichtet, während die häufigsten internen IT-Risiken vernachlässigt werden. Dabei ist der mögliche Schaden beim Missbrauch von vertraulichen Unternehmensdaten derselbe. In fast jeder Organisation werden wertvolle Informationen wie Berichte, Personalunterlagen, Kundendaten oder Forschungsergebnisse ungeschützt elektronisch gespeichert. Als Folge der heutigen zentralen Datenspeicherung auf Servern, standortübergreifende Vernetzung von Arbeitsplätzen und die Nutzung mobiler Datenträger werden die Sicherheitsrisiken stetig größer. Immer mehr Organisationen nutzen zudem IT-Outsourcing zur Kostensenkung, äußern aber gleichzeitig Bedenken bezüglich der Datenvertraulichkeit.

Gefragt ist eine Sicherheitslösung, die organisationsweit nur autorisierten Benutzergruppen Zugriff auf sensible Daten gewährt. Mit entsprechenden Security Policies haben unternehmensinterne Serveradministratoren oder das Personal des Outsourcers keine Möglichkeit, vertrauliche Daten einzusehen.

SafeGuard LAN Crypt benutzt vollautomatische Dateiverschlüsselung um vertrauliche Dokumente effektiv zu schützen. Die Dateiverschlüsselung erfordert keine Änderungen des Benutzerverhaltens: Die Verschlüsselung läuft transparent und somit unsichtbar im Hintergrund. Jeder Anwender erhält aufgrund seines Profils einen einzigartigen „Schlüsselbund“ mit dem er – wie gewohnt – die freigegebenen Dateien im Klartext lesen kann. Unberechtigte Personen sehen stattdessen nur einen chiffrierten, unleserlichen Zeichensatz.

SafeGuard LAN Crypt trennt die Aufgabenbereiche von Serveradministratoren und Sicherheitsadministratoren. Während Serveradministratoren auch ohne Besitz der Dokumentenschlüssel die Systemverwaltung wie gewohnt durchführen können, implementieren Sicherheitsadministratoren über eine skalierbare Schlüsselverwaltung individuelle Zugriffsrechte für Benutzergruppen und erreichen somit eine Gewaltentrennung in der Administration.

SafeGuard LAN Crypt schützt umfassend die Daten von Behörden und Unternehmen: Skalierbar von kleinen temporären Teams über Abteilungen und Projektgruppen bis hin zum organisationsweiten Einsatz.

Die Vorteile

Verbesserte Sicherheit

- » Transparente Datensicherheit für Benutzergruppen und einzelne Anwender
- » Verschlüsselung auf allen gängigen Medien und in heterogenen Umgebungen
- » Gewaltentrennung in Server- und Sicherheitsadministration
- » Einfache Umsetzung einer unternehmensweiten Sicherheitspolitik
- » Flexibel definierbare Verschlüsselungsregeln für Benutzergruppen
- » Komfortable PKI-Integration und Unterstützung von Zertifikaten, Smartcards und USB-Token

Einfach verteilbar

- » Nahtlose Integration in heterogene IT-Infrastrukturen
- » Zentrale und komfortable Administration über vorhandene Directories bzw. Domänen
- » Kein zusätzlicher Ausbau der IT-Infrastruktur nötig
- » Skalierbar von einzelnen Nutzergruppen bis hin zu einem unternehmensweiten Rollout

Einfach handhabbar

- » Einfache Bedienung durch Einbindung in gewohnte Arbeitsumgebung der Anwender
- » Transparent für den Benutzer, selbsterklärende Funktionalität und somit hohe Benutzerakzeptanz

Sicherheit

- Umfassende Sicherheitslösung gegen unberechtigten Zugriff auf Daten
- Schutz von wertvollen Unternehmensdaten und vertraulichen persönlichen Informationen
- Strikte Gewaltentrennung der Verantwortlichkeiten von Server- und Sicherheitsadministrator
- Optimaler Schutz beim IT-Outsourcing, da Mitarbeiter eines externen Dienstleisters die Dateien verwalten, aber nicht im Klartext lesen können
- Verwendung bewährter und geprüfter Sicherheitsalgorithmen
- Benutzerauthentisierung mit X.509-Zertifikaten
- Unterstützung von Chipkarten und USB-Token

System Administration

- Einfache, zentrale Installation, Konfiguration und Administration durch Einbindung in die existierende IT-Umgebung und Nutzung vorhandener Directory Services bzw. Domänen
- Bequeme Einbindung in existierende PKI-Systeme
- Kosteneffiziente und schnell implementierbare Lösung, die keine zusätzliche Hardware-Infrastruktur benötigt
- Durchdachte Recovery-Strategie, um auf verschlüsselte Daten auch im Notfall zugreifen zu können

Benutzerkomfort

- Berechtigte Anwender können ihre gemeinsam genutzten Informationen geschützt ablegen – ohne Gefahr des unberechtigten Zugriffs Dritter
- Persistente Verschlüsselung
- Keine Änderung der gewohnten Arbeitsumgebung und Arbeitsweise nötig
- Hohe Akzeptanz bei den Anwendern – kein zusätzliches Training notwendig
- Keine Einbußen bei der Server-Performance – Ver- und Entschlüsselung wird auf den Endgeräten automatisch im Hintergrund vorgenommen

Interoperabilität

- Kompatibel mit SafeGuard Data Exchange 5.40 und höher
- Unterstützung von Anti-Malware Produkten (z.B. Sophos)
- Unterstützte Datenbanken: Microsoft SQL Server und Oracle
- Unterstützte Directories: Microsoft Active Directory und Novell eDirectory
- Leistungsfähige Administration API ermöglicht Integration von SafeGuard LAN Crypt in beliebige Provisioning Systeme
- Unterstützung RSA-fähiger Komponenten über Microsoft CryptoAPI7 CSP für die Benutzerauthentisierung (z.B. Chipkarten oder USB-Token)
- Aladdin eToken zertifiziert

Weitere Informationen

Für weitere Informationen über Sophos und die aktuelle Produktlinie von SafeGuard Lösungen besuchen Sie bitte www.sophos.de.

SGLC 3.70

Systemanforderungen

Hardware

- » PC mit Intel Pentium-Prozessor oder kompatibelem Prozessor

Betriebssystem

- » Microsoft Windows Vista Business, Professional, Ultimate
- » Microsoft Windows XP Professional

Unterstützte File Server Betriebssysteme

- » Microsoft Windows (in den Versionen NT, 2000, 2003 und 2008)
- » Novell Netware

Unterstützte Terminal Server

- » Microsoft Windows Server 2003 Terminal Services
- » Citrix MetaFrame

Unterstützte Medien

- » Netzwerklaufwerke, lokale Festplatten, CDs, DVDs, USB-Speichermedien, Speicherkarten

Standards/Protokolle

- » X.509v3-Zertifikate für Benutzerauthentisierung
- » PKCS#12
- » LDAP für Zugriffe auf Microsoft Active Directory und Novell eDirectory
- » Verschlüsselung: 3DES (168 bit), IDEA (128 bit), AES (128 und 256 bit)
- » Hash: MD5, SHA-256
- » Token: Chipkarten und USB-Token via Crypto API

Sprachversionen

- » Deutsch, Englisch, Französisch