

Um sich vor finanziellen Verlusten zu schützen, müssen Unternehmen lückenlose Informationssicherheits-Systeme einrichten, die auf der Basis von festgelegten Standards und Regularien alle möglichen Lücken, über die Daten absichtlich oder unabsichtlich an Dritte gelangen können, schließen. Diese Systeme sollten vertrauliche Daten sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks schützen. Datenschutz wird auf Grund der weiten Verbreitung von Laptops, Netbooks und anderen tragbaren Datenträgern in Unternehmen, besonders beim Top-Management, zunehmend wichtig. Diese Datenträger werden oft auch außerhalb des Unternehmensnetzwerks verwendet und benötigen zusätzlichen Schutz.

Passwortschutz basierend auf Tools der Standard-Betriebssysteme ist nachweislich nicht ausreichend, da Daten trotz Benutzung von Passwörtern leicht von der Festplatte eines beispielsweise verlorenen oder gestohlenen Laptops gelesen werden können.

InfoWatch CryptoStorage Enterprise bietet Verschlüsselung von Informationen, um dem Schutz vertraulicher Daten vollständig gerecht zu werden. Das Produkt sorgt für

- den Schutz vertraulicher Daten, die am Arbeitsplatz und auf Unternehmensservern sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks gespeichert sind
- eine Minimierung von finanziellen, rechtlichen und anderen Risiken, die im Zusammenhang mit einem Datenverlust auftreten können
- die Einhaltung von Vorschriften für die persönliche Datensicherung

Funktionalität des Produkts

Sicherung verschiedener Objektarten

InfoWatch CryptoStorage bietet

- Verschlüsselung separater Dateien und Verzeichnisse
- Verschlüsselung logischer Laufwerke, inklusive der Verschlüsselung der System- und Boot-Sektoren
- Verschlüsselung entfernbarer Laufwerke und Massenspeicher (USB, Flash, Memory Cards für mobile Datenträger u.a.)
- Erstellung besonderer geschützter Bereiche - Container-Dateien

Die Verschlüsselung findet im transparenten Modus statt: Wenn Daten gelesen werden, werden sie automatisch im Speicher des Computers dechiffriert, während des Speicherns werden die Daten wiederum automatisch chiffriert.

InfoWatch CryptoStorage unterstützt auch die Verschlüsselung und den Schutz des RAM-Speichers, beispielsweise auch der Datei, die erstellt wird, wenn der Computer in den Ruhezustand gefahren wird, oder Windows-Dump Files, die im Fall eines Systemfehlers erzeugt werden.

Demarkationen für einen sicheren Zugang

Um mit geschützten Dateien arbeiten zu können, müssen User sich autorisieren. Zugang zu chiffrierten Objekten wird mit Hilfe von Passwörtern oder geheimen Keys gewährt, die auf einem beliebigen Speichergerät liegen können. Ist die Boot- oder System-Partition geschützt, findet die Autorisierung im Pre-Boot-Modus statt. InfoWatch CryptoStorage Enterprise unterstützt mit USB eToken/USB ruToken eine Zwei-Wege- Authentifizierung.

"Datenverluste haben für Organisationen ernsthafte finanzielle Konsequenzen. Die Gesamtkosten der Datenverluste steigen dabei von Jahr zu Jahr stetig an."

Ponemon Institute

Features:

- Verlässlicher Datenschutz dank modernem und starkem Verschlüsselungs-Algorithmus
- Preis-Effektivität ohne versteckte Kosten: Alle Features sind in einem einzigen Modul verfügbar
- Einfache Installation und Wartung: Integration mit Active Directory für eine leichte Anwendung der Security-Policies
- Skalierbarkeit: InfoWatch CryptoStorage Enterprise kann auch in Unternehmen mit über 5000 Mitarbeitern eingesetzt werden
- Komfort für Enduser: Verarbeitung von geschützten Objekten auch außerhalb des Unternehmensnetzwerks, hohe Performance während der Verschlüsselung und Entschlüsselung

Starker Verschlüsselungs-Algorithmus

InfoWatch CryptoStorage Enterprise benutzt den modernen AES-Algorithmus (Advanced Encryption Standard).

Schutz der Netzwerk-Ressourcen

InfoWatch CryptoStorage Enterprise ermöglicht es, Daten zu verschlüsseln, die sich auf einem ‚remote‘ PC innerhalb des Unternehmensnetzwerks befinden, um ein zentralisiertes, geschütztes Informationsspeicher-System mit hierarchischem Multi-User-Zugang zu erstellen. InfoWatch CryptoStorage Enterprise bietet zudem die Möglichkeit, weitere Sicherheitsmaßnahmen für bestimmte Verzeichnisse und Dateien innerhalb von geschützten Objekte zu implementieren. Die Verzeichnistiefe ist dabei nicht limitiert

Einbindung in das Corporate Directory

Dank der Integration mit Microsoft Active Directory ermöglicht InfoWatch CryptoStorage Enterprise die Anwendung von Sicherheits-Richtlinien für Benutzer oder Benutzergruppen aus dem Corporate Directory. Der InfoWatch CryptoStorage Enterprise Client kann zentral an allen Arbeitsplätzen installiert werden.

Update der Sicherheits-Policies

InfoWatch CryptoStorage Enterprise wird zentral über eine remote angeschlossene Administrationskonsole installiert und eingerichtet. Die zentralisierte Anwendung der Security-Policies erlaubt die Erstellung von Regeln für den Zugang zu vertraulichen Daten für jeden einzelnen Benutzer. InfoWatch CryptoStorage Enterprise ermöglicht es, Nutzungsparameter der geschützten Objekte zu definieren, inklusive deren Aufbewahrungsort im Netzwerk, Zeitfenster für Zugriffszeiten und andere erlaubte Aktionen. Das System der Benutzerprofile gewährleistet einen sicheren Multi-User-Zugang zu Daten.

Garantierte Datenlöschung

Werden Dateien unter MS Windows gelöscht, können diese leicht mit speziellen Tools wiederhergestellt werden. InfoWatch CryptoStorage Enterprise hingegen ist in der Lage, Daten so zu löschen, dass es unmöglich ist, Daten selbst mit speziellen Tools wiederherzustellen.

Zugangswiederherstellung

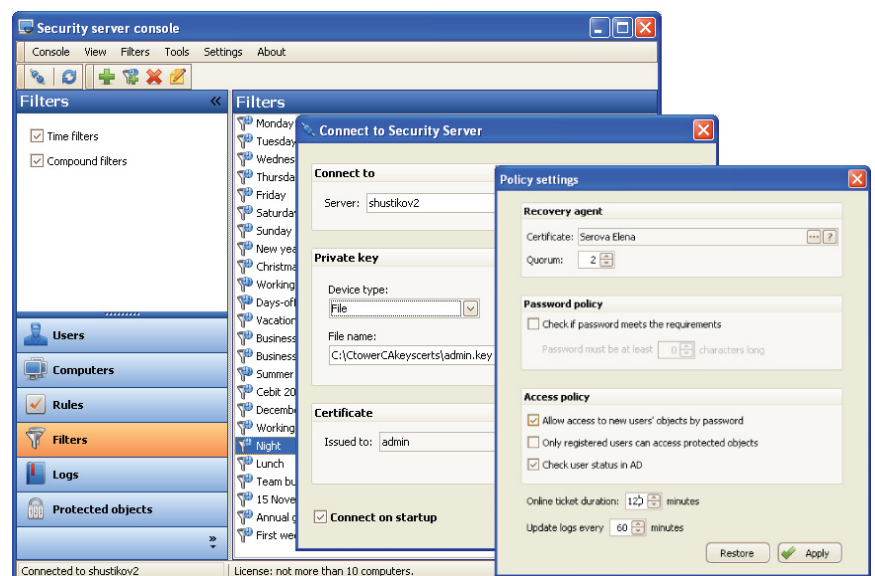
Im Falle des Verlustes des geheimen Schlüssels ist es möglich, den Zugang zu verschlüsselten Objekten mit Hilfe des 'Recovery Committee'-Tools von InfoWatch CryptoStorage Enterprise wiederherzustellen. Das 'Recovery Committee'-Tool erlaubt die Wiederherstellung des Zugangs mit den Schlüsseln autorisierter Systembenutzer.

Aktivitäts-Analyse

InfoWatch CryptoStorage Enterprise lässt den Systemadministrator umfassende Reports sowohl über den Umgang der Benutzer mit vertraulichen Daten, als auch Statistiken über Zugriffszeiten, spezielle Benutzer oder Computer, sowie geschützte Objekte oder andere Vorgänge erstellen.

System-Voraussetzungen

- **Clientanforderungen:** MS Windows (2000, 2000 Server, XP, 2003, Vista). Hardware: Celeron 1 GHz oder höher, 256 MB RAM, 30 MB Festplattenplatz
- **Serveranforderungen:** MS Windows (2000 Server, XP, 2003, Vista). Hardware: Pentium-4 3 GHz, 1 GB RAM, 50 MB Festplattenplatz



Kontakt:

www.infowatch.de
Tel.: +7 (495) 22 900 22
sales@infowatch.com
sales-oem@infowatch.com

Partner-Kontakte:

Österreich und Schweiz: sales-ach@infowatch.com, +49 (8152) 969340
Deutschland: sales-de@infowatch.com, +49 (4207) 689933
Benelux und Mittelmeerstaaten: sales-be@infowatch.com, +32 47792090