



SECUWARE

Geschlossene Informationskreise
360° Datenschutz für das Unternehmen

(Diese Seite wurde absichtlich leer gelassen)

Zusammenfassung der Geschäftsführung

Die gewaltige Kombination aus Gesetzgebung, negative PR und Haftbarkeit hat sichergestellt, dass Datenschutz heute die vielleicht wichtigste informations-technologische Herausforderung an Unternehmen darstellt. Das Lösungsspektrum quillt über vor vielversprechenden Lösungen, welche aber alle nur einzelne Aspekte des Datenschutzes ansprechen. Diese können aber vom CIO eines typischen Unternehmens, dem wenig Mittel für die Implementierung von Mehrfach-Punktlösungen zur Verfügung stehen, kaum umgesetzt werden.

Das Secuware Security Framework (SSF) wurde entwickelt, um gerade diese Punkte zu überwinden und ein umfassendes Sicherheitsbetriebssystem anzubieten, das sich auf die Windows Oberfläche legt und sich integriert, um all Firmendaten, egal wo sie sich gerade befinden, zu schützen. SSF liefert geschlossene Informationskreise, die sicherstellen, dass nur befugte Anwender mit autorisierten Anwendungen Zugang zu den autorisierten Daten haben. Dadurch wird die Anwendung von hochgranularen Sicherheitsrichtlinien zur Speicherung oder Zugriff auf Daten, die sich auf mobilen wie auch immobilen Medien oder in Netzwerkordnern befinden, sichergestellt, so dass diese Information nur dem befugten Anwender zugänglich ist. Dieser Schutz und diese Kontrollen werden in einem Daten-zentrischen Design eingesetzt, was den Verwaltungsaufwand minimiert und es mit dem Active Directory und andere LDAP-basierenden Verzeichnisdienste straff integriert.

Dieses Dokument beabsichtigt die entscheidenden Datenschutzangelegenheiten, sowie die Erfolge von Secuware Security Framework auf diesem Sektor anzusprechen, bevor auf einen umfassenden Überblick und Analyse von Secuware Security Framework und seine Anwendbarkeit, um die kritischen Datenschutzbedürfnisse heutiger Unternehmen zu lösen, eingegangen wird.

Inhaltsverzeichnis

Zusammenfassung der Geschäftsführung	3
Das Datenschutzproblem	5
Kostenfaktor ungeschützte Daten	5
Was ist das Datenschutzproblem und wie kann es gelöst werden?	5
Das Secuware Security Framework	6
Überblick und Nutzen	6
SSF Kunden	7
Eingehende Analyse der Secuware Security Framework	9
Produktstruktur	9
Einfacher und skalierbarer Einsatz und Verwaltung	10
Clientverteilung	12
Erstellen und Ändern von Anwender Sicherheitsrichtlinien	13
Erstellen und Ändern von Computerrichtlinien	13
Erstellen und Ändern von Richtlinien zur Verschlüsselung von Festplatten	13
Erstellen und Ändern von Richtlinien zur Fremdspeicherung	14
Erstellung und Verwaltung von Datenzugangskontrollen für bestimmte Geräte	15
Anwender Zugangskontrollen	15
Transparenter Datenschutz für End-User Systeme	15
Das Booten	15
Login, wenn das System an eine Domäne angeschlossen ist	16
Login, wenn das System nicht an eine Domäne angeschlossen ist	16

Dieses Dokument ist nur zu Informationszwecke gedacht. Secuware gibt hierin keine Garantien oder Gewährleistungen, weder explizit noch implizit.

Einhaltung von urheberrechtlichen Vorschriften liegt in der Obliegenheit des Anwenders. Ohne Urheberrechte einzuschränken, darf kein Teil dieses Dokumentes vervielfältigt, gespeichert in oder in ein Datenwiederfindungssystem eingebracht werden, noch darf es in irgendeiner Form (elektronisch, mechanisch, fotokopiert, audiotecnisch oder anderweitig), oder aus irgendeinem Grund verbreitet oder vertrieben werden ohne eine schriftliche expressis-verbis Erlaubnis von Secuware, Inc.

© 2009 Secuware, Inc. All rights reserved. Secuware and the Secuware logo are registered trademarks of Secuware, Inc. Secuware Security Framework and Crypt4000 are trademarks of Secuware Inc. All other marks are the property of their respective owners.

Das Datenschutzproblem

Kostenfaktor ungeschützte Daten

Datenschutz war Nummer 1 auf der Liste der *Most Critical Issues for the Next Two Years* in der kürzlich fertiggestellten *2006 CSI/FBI Computer Crime and Security Survey*. Die dramatische Wichtigkeit von Datenschutz wurde dargestellt, Spam dagegen wurde nur von 15% der Umfrageteilnehmer als kritisch angesehen.

Diese Reaktion wird kaum überraschen angesichts des rechtlichen und regulatorischen Umfeldes in dem sich CIOs heute bewegen müssen. In den unterschiedlichen Wirtschaftssektoren, wie Finanzdienste, Herstellung und E-Commerce und auch in Behörden, muss ein Datenverlust oder Datenschutzverletzung öffentlich gemeldet werden, auch der vermeintliche Verlust oder die Verletzung. Bis zum Jahre 2006 hatten 35 Bundesstaaten Gesetze zu Datenschutzverletzungsmeldungen erlassen und Nichteinhaltung kann hohe Bußgelder bis in die Millionen von Dollar nach sich ziehen. Jedem sind die brisanten Nachrichten bekannt, die von verlorenen oder gestohlenen Laptops und CDs mit vertraulichen Informationen die hunderttausende, manchmal Millionen von Menschen betrafen, berichteten.

Die finanziellen Konsequenzen beiseite, ist der Datenverlust eine Verletzung der Privatsphäre, in der Öffentlichkeit sehr peinlich mit entsprechendem Verlust von Ansehen und Ruf. Finanziell sind die Konsequenzen manchmal so schlimm, dass manche Unternehmen sich nie davon erholen – es müssen Anwälte und Ermittler eingesetzt werden, hinzu kommen hohe Verwaltungskosten, dann wäre da noch die nachteiligen Nebenwirkungen von Aktionär- und Kundenreaktionen, Chancenverlust und Krisenmanagement. Hinzu kommen Kosten für provisorische Informations-Hotlines um Kunden zu halten und die kostenfreien Kreditüberwachungssubskriptionen. Eine Studie fand heraus, dass 20% der Kunden, die von einem Firmendatenverlust betroffen sind, kündigen Ihr Geschäftsverhältnis mit der Firma, weitere 5% beauftragen einen Anwalt. Wahrscheinlich der schlimmste Albtraum eines CIOs heute ist die Aussicht den Namen seiner Firma in einer *Wall Street Journal* Story über Datenverlust wiederzufinden.

Was ist das Datenschutzproblem und wie kann es gelöst werden?

Datenschutz umfasst Datengeheimhaltung und Datenzugangskontrolle und dieses ist eindeutig ein großes, vielfältiges unternehmensumfassendes Problem mit vielen verschiedenen Fragen und Problemen:

- Im Büro abhanden gekommene oder außerhalb des Büros gestohlene Laptops mit vertraulichen Informationen.
- Angestellte, die unbefugt vertrauliche Information auf tragbaren Geräten wie Flash Drives kopieren.
- „Insider Jobs“ durchgeführt von unbefugten Angestellten, die vertrauliche Informationen zur Selbstbereicherung unterschlagen, oder Cyber-Kriminelle die Unternehmen infiltrieren.
- Angestellte die für ihren persönlichen Bedarf Anwendungen herunterladen, die mit Viren oder Trojaner infiziert sind, die dann die Firmendaten entwenden.
- Begrenzte Mittel zur Durchsetzung von Sicherheitsmaßnahmen.

*“Nur ein kleiner Teil der gemeldeten Datenschutzverletzungen stammen von Hacker, die in Computersysteme online einbrechen. Der Großteil der Datenverluste tritt durch die physikalische Entwendung von tragbaren PCs, Laufwerken und Disketten/CDs oder durch unbefugte Nutzung von Daten durch Angestellte ein. – **Regierungsreformkomitee, Staff Report, October 13, 2006***

Die Hauptherausforderung an IT und Sicherheitsmanagement heute besteht darin Lösungen, die vertrauliche Daten schützen und den Datenzugang unabhängig vom Standort kontrollieren, *und* in der Anwendung *effektiv sind*, zu finden und einzusetzen. Eine übermäßig komplexe Lösung bietet keinen ausreichenden Schutz, da sie weder gepflegt noch ausreichend erhalten wird in Zeiten von engen Budgets. Und End-User werden sich weigern mit einem Sicherheitsprodukt zu arbeiten, das zu viele Barrieren zwischen ihnen und ihre Produktivität stellt, egal wie viele Vorteile man ihnen daraus versprochen hat.

Im Aufbau und Einsatz einer umfassenden Datenschutz und Zugangskontroll-Lösung, bietet sich dem CIO und seinen Mitarbeitern eine verwirrende Auswahl an Lösungen, die alle meist nur Teillösungen darstellen. Eine zusammengeschusterte Kombination aus mehreren verschiedenen Ansatzlösungen leidet sicherlich unter funktionellen Überschneidungen, funktionelle Lücken, mannigfaltige Verwaltungskonsolen und die Duplikatur in der Verwaltung. Verwirrung, hohe Unterhaltungskosten, und Sicherheitsschwachstellen sind unweigerlich das Ergebnis dieser Zusammenstoppelung. Vorzuziehen ist eine Lösung die folgendes bietet:

- Umfassenden Datenschutz und Zugangskontrolle in einem einfachen, flexiblen Paket
- Niedrige Unterhaltungskosten (Headcount und Spezialkenntnisse)
- End-User Transparenz
- Straffe Integration mit der vorhandenen Infrastruktur

Das *Secuware Security Framework (SSF)* ist eine Unternehmenslösung die von Grund auf entwickelt wurde um Firmendaten und die Zugangskontrolle dazu zu schützen, egal wo sich die Daten befinden oder auf welchem Medium sie gespeichert sind.

Das Secuware Security Framework

Überblick und Nutzen

Secuware Security Framework (SSF) stellt sicher, dass nur *Befugte* mit *autorisierten Geräte* auf denen *autorisierten Anwendungen* ausgeführt werden, Zugang zu den *autorisierten Daten* haben. Während SSF sich direkt mit allen bedeutenden, auf LDAP basierenden Verzeichnisdiensten integriert, wird Active Directory als Beispiel Implementierung in diesem Schreiben verwendet.

Der Pre-Boot Authentifizierungsprozess, mit Windows und Active Directory eng eingebunden, stellt sicher, dass der Daten- und Systemzugang eine strenge Anwender Authentifizierung fordert. Dieser Prozess setzt Investitionen in eine vorhandene Sicherheitsstruktur wirksam ein und macht ein separates Identity – Verwaltungssystem überflüssig.

Die Durchsetzung von Datenschutz und Zugangskontrolle bietet eine Daten-zentrierter Herangehensweise an Media- und Dateiverschlüsselung. Zusätzliche Datenzugangskontrollen erlauben nur befugten USB und Firewire-Geräten Zugang zum System. Kontrolle über Anwendungen begrenzt User-Zugang auf eine vorher festgelegte Liste von freigegebenen Programmen. Ein nützlicher Nebeneffekt der Anwendungskontrolle ist eine zusätzliche Schutzebene gegen Viren, Trojaner und andere Malware in dem unbeabsichtigtes oder vorsätzliches Aktivieren von nicht genehmigten ausführbaren Programmen verhindert wird. Wie Anwendern bekannt, trägt Anwendungskontrolle auch wesentlich dazu bei das System zu stabilisieren durch geprüfte Applikationskonfigurationen.

Diese Kombination von Kontrollen schafft einen Geschlossenen Informationskreis (*Closed Circuits for Information*) – Sicherheitszonen die Firmendaten auf ähnlicher Weise schützen wie ein CCTV System, das nur Bilder aus einem eingegrenztem Gebiet zeigt. Die daraus resultierende enge Integration mit Windows ergibt ein sicheres Betriebssystem „Secure Operating System“ das in der Lage ist die Daten vom Boot Prozess aufwärts zu schützen.

Die SSF Struktur ist preisgünstig und hoch-skalierbar und beinhaltet einen Windows Client und eine Verwaltungskonsole. Es werden weder eigene Server benötigt, noch einen festgeschalteten Datenspeicher oder -Server. Der Client ist mit normalen Software Hilfsprogrammen ganz einfach einzusetzen.

Sicherheitskonfiguration und Administration (Richtlinienerstellung) wird durch Verzeichnis Snap-Ins bewerkstelligt. Systemverwaltung (Zuteilung der Richtlinien an Anwender und Systeme) wird durch die Standard Verzeichniskonsole gehandhabt.

Sicherheitsrichtlinien, in Form von Anwender- und PC-Profilen, die Chiffrierungsschlüssel enthalten, werden im Verzeichnis als Schemaanhänge (Extensionen) gespeichert. Zur Sicherheit sind die Chiffrierungsschlüssel für Sicherheits- oder System Administratoren nicht direkt zugänglich. Die Richtlinien treten beim nächsten Log-In oder Gruppen-Richtlinien/Objektschub in Kraft.

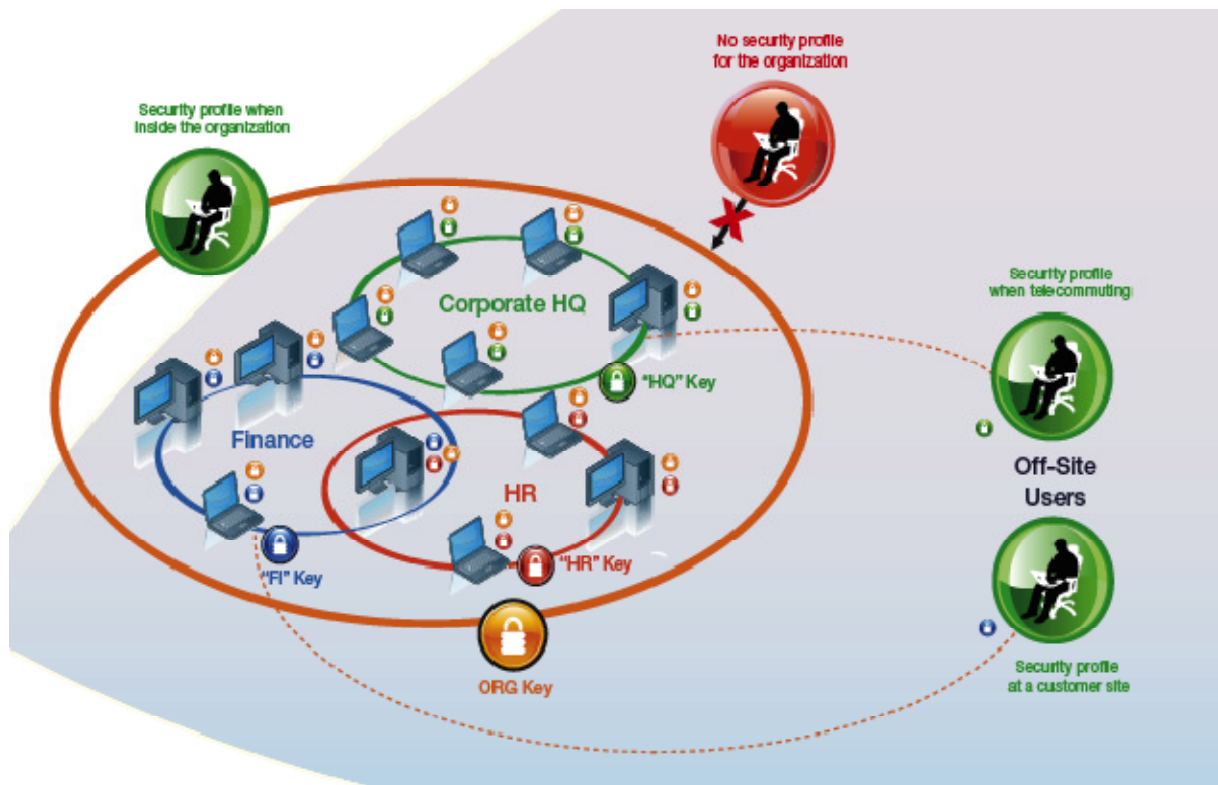


Abb. 1: Secuware Security Framework erzeugt Closed Circuits for Information

SSF bietet Datenschutz durch Verwendung von symmetrischen Chiffrierungsschlüsseln. Ein Schlüssel ist für die Verschlüsselung der lokalen Festplatte zugewiesen und zusätzliche Chiffrierungsschlüssel werden den Fremdspeicherorten zugeteilt, einschließlich tragbare Medien, USB und FireWiregeräten, und Netzwerkordner. Jeder Chiffrierungsschlüssel ist mit einem „benannten Gerät“ gekoppelt; es können mehrfachbenannte Geräte für jeden Gerätetyp sein, z.B. CD/DVD. Benannte Geräte können beliebig viele verschiedene Anwender und PC-Profilen zugeteilt werden, was hochgranulare Sicherheitsrichtlinien ermöglicht. Ein so eleganter und geradliniger Ansatz schließt die komplexen Fragen die mit PKI zusammenhängen aus, wie im folgenden Abschnitt über *PKI-verwandte Fragen* erläutert.

SSF bietet zusätzlich Datenzugriffskontrollen durch Profile für *autorisierte Geräte* und *autorisierte Anwendungen*. Wenn ein autorisiertes Geräteprofil in Kraft getreten ist, können nur noch vorher autorisierte Geräte mit dem System kommunizieren, ob jetzt die Daten auf dem Gerät verschlüsselt sind oder nicht. Wenn ein autorisiertes Anwendungsprofil in Kraft getreten ist, können User nur die Anwendungen, die vorher vom Sicherheitsadministrator genehmigt wurden, ausführen.

SSF Kunden

SSF wird weltweit von mehr als 500 Unternehmen und Regierungen benutzt und schützt über 500.000 Windowssysteme.

- *Agencia Estatal de Administración Tributaria (AEAT, das spanische Finanzamt)* benutzt SSF auf 35.000 Systemen um vertrauliche Steuerzahlerdaten zu schützen. AEAT verwendet geschlossene Informationskreise um einen Datenverlust durch lokale Festplatten, Floppies, CD/DVDs, USB-Geräte und Netzwerkordnern zu verhindern.
- *WalMart Mexico* verwendet SSF zur Datensicherung ihrer örtlichen Banken in ihren mexikanischen Geschäften zu sichern. Weil sich der Active Directory Forest im Hauptsitz in den USA befindet, setzt Wal-Mart Mexico das ADAM ein (siehe den Abschnitt unten über einfachen und skalierbaren Einsatz

und Verwaltung) um den Sicherheits- und Systemadministratoren die Verwaltung des örtlichen Einsatzes von SSF zu ermöglichen.

- *Warner Brothers Mexico* verwendet SSF um das geistige Eigentum seiner Kunden zu schützen und um Piraterie zu verhindern in dem strenge Zugangskontrollen auf den tragbaren Laptops der Angestellten herrschen.
- *Telefonica Móviles (die spanische nationale Handygesellschaft)* benutzt SSF auf ihren 10.000 Arbeitsplätzen um die Vertraulichkeit der Kundendaten, die in ihrem System gespeichert sind zu gewährleisten und um unbefugten Geräten daran zu hindern, sich mit Telefonica Systemen zu verbinden oder unbefugte Anwendungen auszuführen.
- *Iberdrola*, der größte Energieversorger Spaniens hat Kunden in ganz Südwesteuropa und benutzt SSF auf 12.000 Systemen um die Energieversorgungskette vor Cyber-Terroristen und anderen elektronischen Gefahren zu schützen.
- *BBVA*, eines der größten Banken in Spanien mit Zweigstellen in vielen Ländern Europas, Lateinamerikas und den USA, benutzt SSF um vertrauliche Informationen auf den Laptops seiner Führungskräfte zu schützen.

Eingehende Analyse des Secuware Security Framework

Produktstruktur

SSF besteht aus einem Verwaltungsmodul, das als Active Directory MMC snap-in implementiert wird, und vier separate Kundenmodule, wie unten gezeigt. Drei dieser Kundenmodule erstellen Richtlinien und setzen diese durch, das Vierte speichert sämtliche relevante Sicherheitsereignisse um später Analysen zu Sicherheitsereignis- und forensischen Zwecken auszuführen.

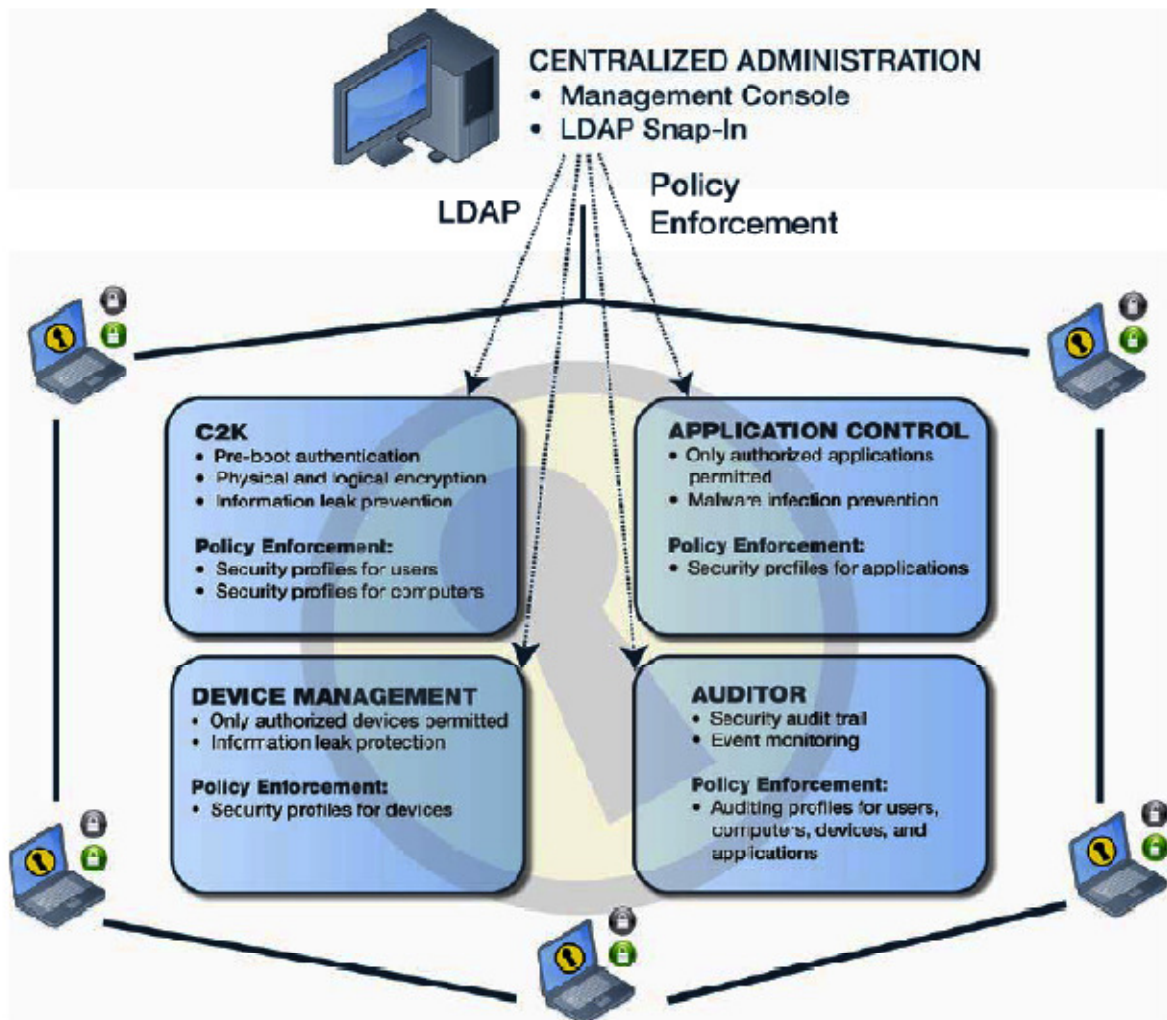


Figure 2: SSF client modules can be installed in any combination and execute policies created by the Administration module

Der Einsatz von SSF kann mit jedem einzelnen der Module beginnen, meist bewährt es sich mit Crypt4000 anzufangen. Das Administrationsmodul ist immer erforderlich, da es benötigt wird um die Richtlinien zu erstellen und zu verwalten. Abbildung 3 zeigt wie die einzelnen Module den Datenzugang schützen während der verschiedenen Stufen des Arbeitsablaufs des Systems, vom Start bis zum Herunterfahren.

Wie schon vorher angesprochen, ist kein Sicherheitsserver oder Richtliniendatenbank erforderlich, was den Einsatz erleichtert und die Einführungskosten reduziert.

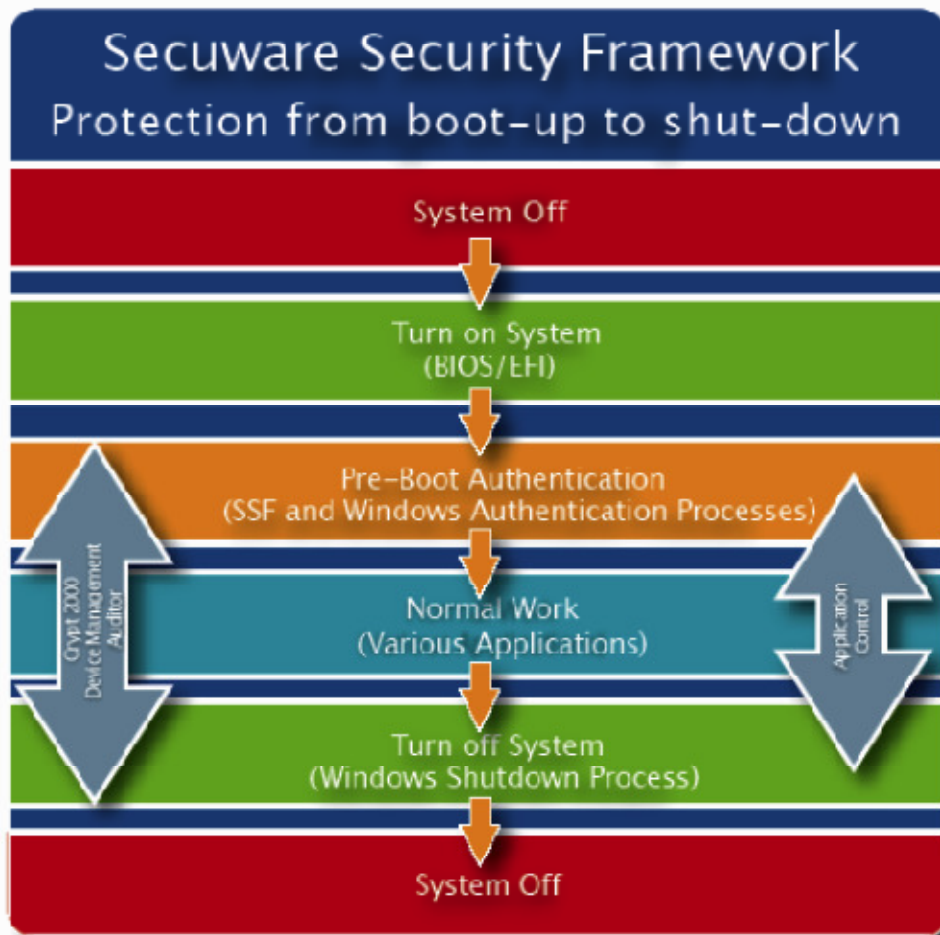


Figure 3: SSF provides protection the entire time that a system is active

Einfacher, skalierbarer Einsatz und Verwaltung

Zentral verwaltete Daten-zentrische Richtlinien für Endsysteme sind das Herz von SSF. Richtlinien werden erstellt und als Anhänge (Extensionen) in der Active Directory Anwender und Computer Schema gespeichert. Einmal in AD gespeichert, werden die Richtlinien beim nächsten Log-In des Anwenders oder dem nächste Group Policy Update greifen.

Die allgemeine Konfiguration des AD Forests, im Rahmen der Trees, Domains, Sites, Anzahl der Objekte, Trustverhältnisse, System Populationen, Weitergabe der Verantwortung, usw. ist in SSF absolut transparent.

Hinweis: An Kunden, die keine Ausdehnung des AD Schemas durch fremde Anwendungen wollen, oder die eine dezentralisierte Weitergabe von Verantwortung einsetzen möchten – SSF unterstützt auch ADAM oder die Verwendung des existierenden Schemas.

Active Directory Application Model, oder ADAM, wurde von Microsoft entwickelt um Anwendungsszenarien die mit seinen Verzeichnis-aktiven Anwendungen verbunden sind, anzusprechen. Es ist eine „leichte“ Version von Active Directory und kann als ein einfacher User-Dienst auf Windows 2003 Server oder sogar auf Windows XP mit SP1 laufen. Um die Anwendung zu vereinfachen, benutzt ADAM viele derselben Verwaltungsprogramme wie Active Directory. ADAM benutzt die gleichen APIs wie Active Directory um eine Integrierung zu vereinfachen.

Tabelle 1 (nächste Seite) fasst die Implementierung der verschiedenen Aspekte des Schutzes und den Zugang zu vertraulichen Daten im Active Directory zusammen:

Security Policy Area	SSF profile (module)	Application Directory Object Class
Pre-Boot Authentication	Computer profile (Crypt2000)	Systems
Authentication and Local Disk Encryption Options	Computer profile (Crypt2000)	Systems
Data Privacy Protection for local Hard Disk	Device encryption key (Crypt2000)	Systems (via computer profile)
Data Privacy Protection and Data Access Control for removable media devices (CD/DVD, USB, FireWire, floppy disks)	Device encryption keys, one per named device. (Crypt2000) Assigned to one or more user profile(s).	Users (via user profile) Systems (via computer profile)
Data access to specific USE/FireWire devices	Device Management profile (Device Management)	Users Systems
Application control	Application control profile (Application Control)	Users Systems

Tabelle 1: Wie Sicherheitsrichtlinien implementiert werden mit SSF

SSF erzwingt eine Trennung der Verantwortung zwischen dem Sicherheitsadministrator und dem Systemadministrator. Nur der *Sicherheitsadministrator* kann Richtlinien erstellen oder ändern, kann Chiffrierungsschlüssel erstellen und an Anwender und Systemprofile vergeben. Nur der *Systemadministrator* kann die Sicherheitsrichtlinien mit Anwendern und Computern implementieren. Die Trennung von Verantwortungsbereiche garantiert, dass Administratoren die Aufgaben innerhalb ihrer Kompetenzbereiche ausführen, und damit insgesamt die Sicherheit des Unternehmens durch Ausschaltung menschlicher Fehlerquellen unterstützen.

Die Teilung der Verantwortung ist in Tabelle 2 (folgend) zusammengefasst:

Security Administrator	System Administrator
Implement corporate security policies for strong authentication	Create users
Implement corporate security policies for data privacy and data access	Create systems
	Apply policies to users and systems
Create whitelists (device management profile) of registered and approved USB and Firewire devices	Apply device management profile to users
Create whitelists (application control profile) of approved applications	Apply application profile to users
Creates auditing profile for files and folders	Apply auditing profile to users
Reviews audit reports for security incidents	

Tabelle 2: SSF erzwingt eine strikte Trennung von Verantwortung zwischen Sicherheits- and Systemadministratoren

Der *Sicherheitsadministrator* benutzt die Secuware Active Directory MMC snap-in wie in Abbildung 4 gezeigt. Alle Richtlinien werden vom Sicherheitsadministrator durch dieses snap-in erstellt und verwaltet. Das SSF snap-in sollte nur auf dem System des *Sicherheitsadministrators* installiert werden.



Abb. 4: Richtlinien werden vom Sicherheitsadministrator erstellt und verwaltet durch das Active Directory snap-in.

Der Systemadministrator wendet die Sicherheitsrichtlinien an und nutzt dabei die vier Schema-Extensionen der User und Computer Schema in Active Directory, wie in Abb. 5 dargestellt. Um die Verantwortungsteilung durchzusetzen sollte die AD Schemakonsole für Sicherheitsadministratoren nicht zugänglich sein.

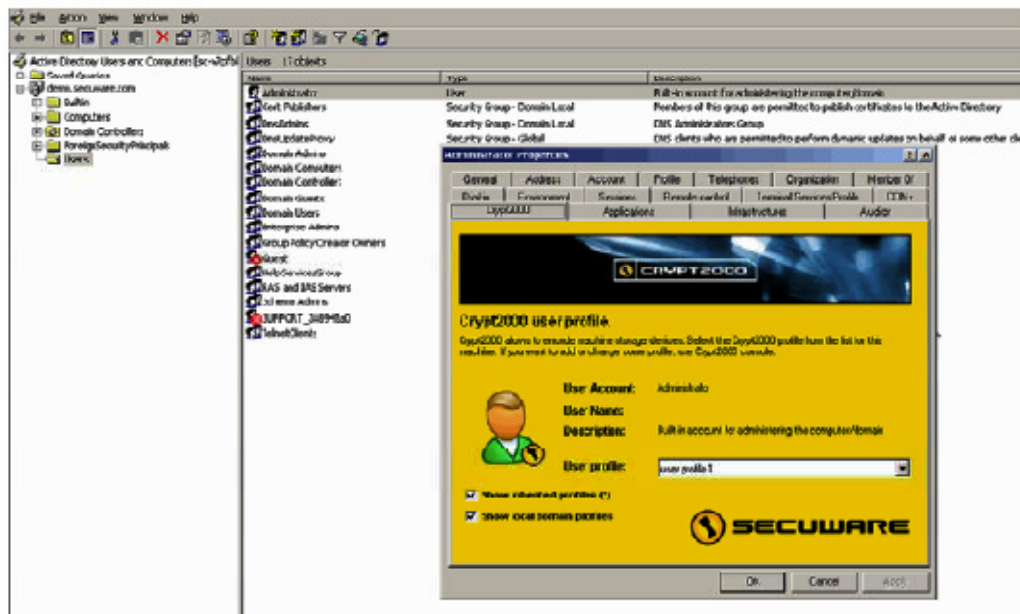


Abb. 5: Der Systemadministrator nutzt die vier Extension Tabs die von SSF in dem Users and Computers Schema erstellt wurden um Richtlinien an Users und Systeme anzuwenden

Clientverteilung

Der SSF Client ist ein „msi“ Modul das automatisch mit einer der großen auf Netzwerk basierende Softwareprogrammen wie Microsoft SMS oder ähnliches von Tivoli, Computer Associates, usw. installiert und angewendet werden kann. Der SSF Client kann auch alternativ mit einem Log-In Script installiert werden.

Erstellen und Ändern von Anwender Sicherheitsrichtlinien

Richtlinienprofile und Geräte-Chiffrierungsschlüssel werden vom Sicherheitsadministrator erstellt, unter Zuhilfenahme des Crypt4000 SSF Snap-in. Einmal erstellt, können diese Richtlinien dann durch den Systemadministrator den einzelnen Anwender oder Anwendergruppen zugeteilt werden, durch Einsatz des in Abb. 5 gezeigten User und Computer Administrative Properties Windows.

Anwendern wird nur ein einziges Crypt4000 Userprofil zugeteilt, was eine Verwechslung zur Frage welche Richtlinien welche Anwender betreffen ausschließt. Dieses Vorgehen erleichtert die Erstellung, Durchsetzung und Verwaltung von Richtlinien. Ein Crypt4000 Userprofil ist Pflicht, wahlweise können Anwender einem Geräteverwaltungs- oder Anwendungsprofil zugeordnet werden.

Einmal erstellt, kann der Systemadministrator das Userprofil der

- Ganzen Domäne
- Mehrere Domänen innerhalb eines AD
- Einer Organisationseinheit (OU) innerhalb einer Domäne, z.B. eine Abteilung oder Zweigstelle
- Einem einzelnen Anwender
oder
- Eine Kombination dieser Möglichkeiten

zuordnen.

Es gibt praktisch keine Obergrenze wie viele verschiedene Userprofile in einem Active Directory Forest erstellt werden können. In der Praxis hat ein großer Secuware Kunde mit über 10.000 Anwendern nur drei verschiedene Richtlinien erstellt – eine für die Führungsetage, eine für das mittlere Management und eine für alle anderen Angestellte. Andere Unternehmen haben eine größere Anzahl von Profilen erstellt, mit gesonderten Profilen für Angestellte in den verschiedenen funktionellen Unternehmungen.

Erstellen und Ändern von Computerrichtlinien

Jedes System ist mit einem Computerprofil verbunden, das für alle Anwender dieses Systems greift. Dieses Profil wird eingesetzt um eine strenge Authentifizierung durch Authentifizierung vor dem Windows Start durchzusetzen, um die Auswahlmöglichkeiten der erlaubten Authentifizierungsberechtigungen festzulegen, um Windows Advanced Authentifizierungsoptionen zu aktivieren/deaktivieren und um Anwender bei jedem Log-In zur Namenseingabe zu erzwingen/nicht zu erzwingen. Dieses Profil enthält auch den Schlüssel für lokale Festplattenverschlüsselung und die Auswahl der User-Profile um die Zeiten in der ein Anwender in der Domäne angemeldet ist einzugrenzen.

Wenn der Pre-Boot Authentifizierungsprozess beendet ist wird der Festplattenchiffrierungsschlüssel, der im *Computerprofil* enthalten ist, für die Entschlüsselung von Dateien verwendet. (Vermerk: Die Festplatte bleibt immer verschlüsselt um alle Dateien zu schützen, für den Fall, dass das System während der Arbeit plötzlich heruntergefahren wird.)

Erstellen und Ändern von Richtlinien zur Verschlüsselung von Festplatten

Der Sicherheitsadministrator kann bestimmen ob eine lokale Festplatte verschlüsselt wird oder nicht; er/sie muss erst ein „benanntes“ Gerät kreieren, wie in Abb. 6 gezeigt. Dieses „benannte Gerät“ wird dann einem oder mehreren Computerprofilen zugeteilt. Der Systemadministrator teilt dann diese Computerprofile an Systeme, wie oben beschrieben.

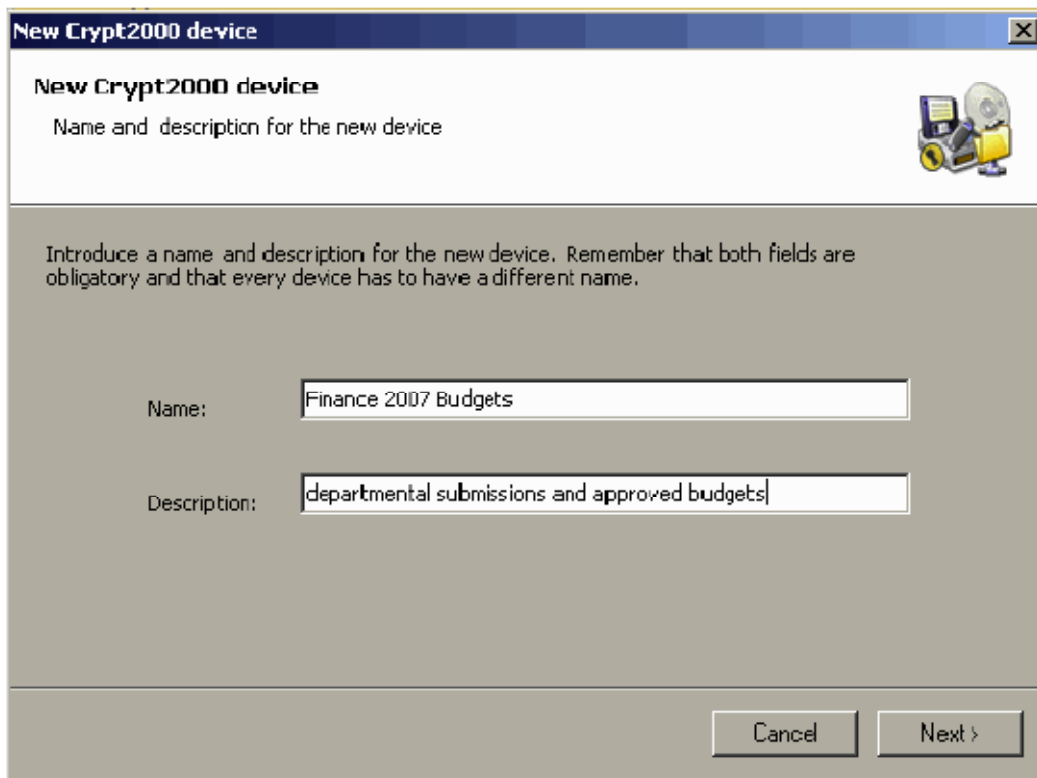


Abb. 6: SSF kann ein neues Gerät „benennen“ welches einem oder mehrere Anwender und Computerprofile zugewiesen werden kann

Erstellen und Ändern von Richtlinien zur Fremdspeicherung

Der Sicherheitsadministrator kann bestimmen welche Arten von Fremdspeicherplätzen benutzt werden dürfen, um auf gesicherte Daten zugreifen zu können. Fremdspeicherplätze sind z.B. CD/DVDs, USB und FireWire Geräte, Floppies und Netzwerkordner.

Um hoch-granulare Sicherheitsrichtlinien zu ermöglichen, wird die Zugangssteuerung jedes Fremdspeicherplatzes „benannt“. Es können mehrere „Namen“ für eine bestimmte Art von Speicherplatz existieren und einzigartiger Chiffrierungsschlüssel wird für jedes dieser Gerätesteuerungen erstellt.

Nach der Erstellung „benannte“ Gerätesteuerungen, werden diese durch den Sicherheitsadministrator einem oder mehreren User- oder Computerprofile zugeteilt. Alle Anwender oder alle Computer mit einem bestimmten Profil teilen sich den Gerätechiffrierungsschlüssel und haben so Zugriff auf Dateien und Medien, die durch diesen Schlüssel geschützt sind. Weil ein „benanntes“ Gerät in mehreren User- und Computerprofilen enthalten sein kann, können auch User und Computer mit anderen Profilen Zugriff auf diese Dateien und Medien haben, während allen Usern und Computern, deren Profile diesen „benannten“ Gerätechiffrierungsschlüssel nicht enthalten, der Zugriff verwehrt wird.

Zur maximalen Absicherung von tragbaren Laufwerken, Floppies und CD/DVDs, USB und FireWire Speicherplätzen, wird jedes Medium mit einer physikalischen Verschlüsselung versehen. (siehe *Physikalische Verschlüsselung* und *Tragbare Medien* unten.)

Erstellung und Verwaltung von Datenzugangskontrollen für bestimmte Geräte

Das Geräteverwaltungsmodul wird benutzt um *Gerätemanagementprofilisten* für bestimmte Geräte zu erstellen durch das Filtern von USB und FireWire. Nur auf die gelisteten Geräte kann zugegriffen werden, ob die Dateien auf diesen Geräten verschlüsselt ist oder nicht.

Das genaue Gerät wird auf einer Liste durch den Sicherheitsadministrator registriert und die Seriennummer notiert. Einmal auf der Liste, werden autorisierte Geräte den Anwendern durch den Systemadministrator zugeteilt indem er das Geräteverwaltungsprofil dem einzelnen Anwender verbindet.

Anwender Zugangskontrollen

Anwendungskontrolle garantiert, dass Anwender diese Applikationen und Browser plug-ins nur nach vorheriger Freigabe durch den Sicherheits-Administrator anwenden können. Keine anderen Anwendungen oder plug-ins können installiert oder ausgeführt werden, inklusive diejenigen die vom Anwender heruntergeladen werden sollten.

Das Anwenderkontrollmodul kann auf verschiedener Weise eingesetzt werden, von minimal oder keine Anwendung für ausgesuchte Einsatzgebiete bis hin zur voller Firmeneinsatz. Weil diese Anwenderkontrolle das System sehr stark kontrolliert, kann es sehr nützlich sein um spezielle Arbeitsgruppen, z.B. Lieferanten oder Auftragnehmern, auf die Anwendung bestimmter Applikationen zu beschränken. Dies ist besonders von Interesse in Firmen wo wenig standardisierte Systemkonfigurationen durch viele verschiedene Abteilungen verwendet werden.

Jede verschiedene Anwenderrichtlinie ist in einem Anwendungsprofil enthalten, welches vom Sicherheitsadministrator erstellt wurde. Die Anwendungskontrollrichtlinie wird durch den Systemadministrator am User angewendet.

Potential der granularen Sicherheitsrichtlinien in SSF
Es gibt keine Abhängigkeiten zwischen Anwenderprofilen, Computerprofilen, Geräteverwaltungsprofilen und Anwenderkontrollprofilen. Verschiedene Anwender- und Computerprofile können einige gemeinsame Chiffrierungsschlüssel haben.

Transparenter Datenschutz für End-User Systeme

Das Booten

SSF kontrolliert den PC ab dem Moment wo er eingeschaltet wird. Pre-Boot Authentifizierung stellt sicher, dass nur ein autorisierter Anwender das System hochfahren kann oder auf den Inhalt der lokalen Festplatte zugreifen kann.

Der Pre-Boot Authentifizierungsprozess verhindert einen Angriff durch übergehen der internen Festplatte und hochfahren des Systems mit Methoden wie:

- Rescue Disketten von Windows oder einem Anti-Virus oder Festplattenpartitionierungutility erstellt
- Windows Installationsmedien
- Startbare USB Flashdrives mit geladene Windows
- CD mit eigenständiger Live Operating System wie Knoppix

Diese Methode verhindert auch, dass ein Einzelner eine SSF-Verschlüsselte Festplatte entfernt und in ein anderes System als zweite Festplatte einsetzt, da er nicht in der Lage sein wird, den Pre-Boot Authentifizierungsprozess, der die Entschlüsselung ermöglicht, erfolgreich abzuschließen.

Wenn das System die BIOS (oder EFI) Initialisierung abgeschlossen ist, zeigt SSF ein Log-In Bildschirm, ähnlich der, der in Abb. 7 unten dargestellt wird. Dieser ist beliebig anpassbar.



Abb. 7: Der Pre-Boot Authentifizierungsprozess öffnet das System und startet Windows

Das Pre-Boot Authentifizierungsfenster kann wie folgt angepasst werden:

- Veröffentlichung von Firmennachrichten und anderen Informationen
- Sicherheits- und Richtlinieninformationen an Angestellte
- Anzeigen von Help-Desk Informationen

Der Pre-Boot Authentifizierungsprozess ist im normalen Windows Log-In Prozess völlig integriert. Anwender nutzen ihre normalen Windows UserIDs und Passworte, Smartcards, um sich anzumelden.

Login wenn das System an eine Domäne angeschlossen ist:

- Anwender Credentials werden durch das Active Directory validiert.
- Windows fährt normal hoch.
- Das Anwenderprofil wird vom Active Directory geladen.
- Das Computerprofil wird vom Active Directory geladen.

Login wenn das System nicht an eine Domäne angeschlossen ist:

Der Prozess ist der gleiche wie oben, nur dass:

Die Anwenderausweise durch eine Cache-Kopie der verschlüsselt gespeicherten Windows Anmeldeinformation validiert werden.

Ein anderes Anwenderprofil geladen wird. Dieses Profil ist typischerweise restriktiver als das, welches geladen wird wenn das System an einer Domäne angeschlossen ist, da das Risiko, dass dieser Anwender evtl. nicht mehr bei der Firma ist, oder ein „lost system“ angemeldet hat. Das ist bei einer Online - Authorisierung ausgeschlossen, aber nicht bei einem offline Log-In.