



SECUWARE

Ausgangslage

Die rasant steigende Zahl mobiler Mitarbeiter sowie immer strengere Sicherheits-Richtlinien und die mit Datenverlust verbundenen Aufwendungen erhöhen den Bedarf der Unternehmen nach einer Lösung, die den Schutz einer ganzen Reihe von Geräten, Anwendungen, Festplatten und Netzwerk-Ordnern umfasst.

Produktbeschreibung

Secuware Security Framework erweitert die Sicherheit von Windows-Netzwerken durch die Schaffung von geschlossenen Informationskreisläufen, in denen nur autorisierte Personen mit zugelassenen Geräten und autorisierten Anwendungen zugreifen können.

Secuware Security Framework gibt Unternehmen die granulare Verwaltung, die sie für die Kontrolle der Computer, Benutzer, Anwendungen, Daten und Geräte benötigen.

Die wichtigsten Merkmale:

- Entwickelt für Unternehmen
- Mehrschichtige Sicherheit
- Starke Authentifikation
- System- und Datensicherheit
- Anwendungskontrolle
- Geräte-Management
- Zentrale Verwaltung
- Einfache Bereitstellung und Bedienung
- Integration in bestehende Infrastruktur

Herausforderung für Kunden

Gefahren und Bedrohungen

Fragen Sie Ihre Kunden, wie sicher sie sind, dass

- ihre Unternehmensziele und Ihre Sicherheit im Einklang stehen?
- ihr Unternehmen die behördlichen Richtlinien erfüllt?
- ihre Unternehmenswerte und Kundendaten unversehrt sind?
- sie morgen keinen Artikel in der Zeitung über den Verlust von Daten oder Geräten aus ihrem Unternehmen lesen werden?



SECUWARE

Kundeninteresse

- ✓ Beschränken Sie den Zugriff auf Daten und Anwendungen um Missbrauch abzuwenden
- ✓ Sperren Sie Ihre Daten und Geräte um unbefugten Zugriff zu verhindern
- ✓ Vereinen Sie Richtlinien, Verzeichnisse und Benutzer-Aktivitäten
- ✓ Kontrollieren Sie multidimensional von einem zentralen Punkt aus
- ✓ Einfache Bereitstellung und Verwaltung
- ✓ Flexible Implementierung
- ✓ Integration mit bestehender Infrastruktur

Lösung

Secuware Security Framework ist ein sicheres Betriebssystem, das noch vor dem Start des Windows-Betriebssystem gestartet wird und das vom Boot-Prozess an alle Daten und Anwendungen schützt.

Praktische Vorteile

Sicherheit vom Start weg

- Systeme sind geschützt vom Boot-Prozess an.
- Der Schutz kann nicht durch einen Low-Level-Zugriff auf Tools umgangen werden.

Geschlossene Informations-Kreisläufe

- Anwender bekommen nur den Zugang, den Sie für ihre Arbeit benötigen.
- Informationen werden innerhalb definierter Gruppen geschützt

Geräte sind für unbefugten Zugriff gesperrt

- Alle Typen von Speichermedien – Festplatten, USB-Laufwerke, CD- und DVD-Laufwerke
- Autorisierte Benutzer erhalten einfachen Zugang



SECUWARE

Logische Verschlüsselung von Daten in Netzwerk-Ordern

- Geschützte Daten bleiben geschützt, wo immer sie gespeichert sind
- Verschlüsselte Daten sind für Administratoren – oder für Malware – unzugänglich.

Erhöhte Stabilität von Software und Hardware

- Zugriffsberechtigungen für Software und Geräte

Wirtschaftliche Vorteile

Risiko verringern

- Sensibler Schutz für firmeneigene oder schützenswerte Daten
- Verhindert Beschädigung von Vertrauen, Marke, Loyalität und Image
- Vermeidet rechtliche Folgen eines Sicherheitsverstößes
- Stellt sicher, dass keine Daten verloren gehen

Zeit und Geld sparen

- Reduziert Zeit und Kosten für die Einhaltung behördlicher Auflagen.
- Schließt Kosten für die Offenlegung eines Datenschutzverstößes aus.
- Verwenden Sie Datensicherheit als Wettbewerbsvorteil

Funktionale Bausteine

Secuware Security Framework's modularer Aufbau ermöglicht Unternehmen eine Umsetzung in Etappen, je nach Anforderungen, Budgets und den zur Verfügung stehenden Ressourcen.

C4K ist dabei das Herzstück von SSF. Es ist auf den Schutz von Informationen fokussiert und wurde ursprünglich im Auftrag eines europäischen Verteidigungsministeriums zum Schutz der Netzwerke des Geheimdienstes entwickelt. Es startet eine Zugangskontrolle vor dem Booten des Betriebssystems und verschlüsselt alle auf dem Computer gespeicherten Informationen sowie alle Informationen, die durch den Einsatz anderer Geräte kopiert werden könnten. C4K stellt sicher, dass der Computer und alle Daten und Anwendungen auf diesem Computer nur von autorisierten Personen genutzt werden können.



SECUWARE

Geschlossener Informationskreislauf

Um Informationsverlust zu verhindern, kann C4K Informationen, die den PC entweder auf physischen Datenträgern oder über das Netzwerk verlassen, verschlüsseln. Auf CDs und andere Wechselmedien, die innerhalb eines Unternehmens erstellt wurden, kann ein autorisierter Benutzer innerhalb des Unternehmens zugreifen, aber sie können ausserhalb des Unternehmens-Umfeldes nicht gelesen werden.

Umgekehrt kann C4K unverschlüsselte Medien blockieren, damit sie an firmeneigenen PC's nicht verwendet werden können. Es verhindert somit eine nichtautorisierte Nutzung der Firmen-Ressourcen.

Mit der Windows-Netzwerk-Infrastruktur sorgt es für eine schnelle und einfache Kreation von Arbeitsgruppen, die unter definierten Zugangsbedingungen Informationen austauschen dürfen.

Vollständige physikalische Festplatten-Verschlüsselung

Der einzige Weg, um sicherzustellen, dass alle Informationen geschützt sind, ist die vollständige physikalische Verschlüsselung der Festplatte. Die Verschlüsselung aller physischen Sektoren der Festplatten schützt auch temporäre Dateien und Spuren, die noch auf der Festplatte verbleiben und sonst von nichtautorisierten Benutzern anderweitig genutzt werden könnten.

Informations-Verschlüsselung über das Netzwerk

Heutige Datei-Systeme bieten eine hochwertige Zugangskontrolle aber jeder Benutzer mit Administrator-Rechten ist lesbar von jedem Benutzer mit Administrator-Berechtigungen. Ganz gleich wie gründlich Ihre Sicherheits-Richtlinien sind, wird jedes Ihrer nicht verschlüsselten Dokumente von jedem mit Administrator-Berechtigungen lesbar sein. C4K umfasst alle etwaigen Speicher-Ressourcen, die von Mitarbeitern und Geschäftspartnern genutzt werden, einschließlich der freigegebenen Ordner im Netzwerk. Wenn Benutzer also Informationen im Netzwerk speichern, sind diese verschlüsselt und deren Sicherheit ist gewährleistet.

Public Key Infrastructure (PKI) Integration

C4K ist „PKI-ready“ und kann dadurch sichere Anmeldungen mit einem digitalen Zertifikat, das jeden X.509 v3- und LDAP x.500-Standard-basierten Hersteller

unterstützt, durchführen. Das Kombinieren der Pre-Boot-Authentication mit der Verwendung von digitalen Zertifikaten auf den physikalischen Zugang-Token bietet



SECUWARE

maximale Kontrolle durch die Durchsetzung der netzwerkweiten Benutzer-Identifikation und –Validierung.

Device Management

Das Device-Modul steuert, welche Geräte zulässig sind, um eine Verbindung zum Netzwerk und die Art der Verbindungen dieser Geräte herzustellen. Seine Aufgabe ist es, zu verhindern, dass Unbefugte Hardware-Geräte wie CD- oder DVD-Brenner, USB-Laufwerke und andere Wechselmedien Verbindung zu Unternehmens-Systemen erhalten und die Einführung von Malware-Infektionen zu verhindern. SSF Device Management implementiert eine Geräte-Authentifizierung. Nur autorisierte

Benutzer haben Zugriff auf autorisierte Geräte. Es stoppt Informationsverluste durch die Sicherung von Informationen, die auf eine nicht für diesen Zweck autorisierte CD, DVD oder USB-Laufwerk kopiert wurden.

Application Control

SSF Applications führt eine Anwendungs-Kontrolle durch. Nur autorisierte Benutzer sind in der Lage autorisierte Anwendungen zu starten.

Dieses Modul ermöglicht IT-Abteilungen, für Zwecke der Validierung eine Momentaufnahme aller Anwendungen und anderen installierten Komponenten auf einem bestimmten Computer durchzuführen. Sobald die Momentaufnahme gemacht worden ist, können auf diesem Computer nur validierte Anwendungen ausgeführt werden. Die Nutzung des Application-Moduls sorgt für die Stabilität des Computers; es schützt die Integrität vor Bedrohungen wie Viren und Trojanern; verringert die Anforderungen an den Helpdesk und hilft bei der Kontrolle und Prognose von Wartungskosten.

Secuware Security Framework (SSF)

Was bringt SSF meinem Unternehmen?

SSF erhöht die Sicherheit der Windows-Ebene, sorgt für Schutz im Hinblick auf Ihre System-Anwender und stimmt Ihre Wünsche auf die Anforderungen Ihrer Organisation ab. Dies ist ein Produkt, das Ihren PC sichert, das es zu einem Firmenwerkzeug macht, das zentral verwaltet wird und die Vertraulichkeit der Informationen und die Plattform-Stabilität gewährleistet.

Warum ist SSF ein Sicherheits-Betriebssystem?

Die Funktion eines Betriebssystems ist, Anwendungen von Hardware unabhängig zu machen und es bietet eine Reihe von Anwendungen auf die Benutzer zugreifen können.



SECUWARE

SSF kontrolliert die Identifizierung s- Geräte ausschließlich in der Preboot-Schicht und zwar aus zwei Gründen: erstens zum Schutz von Windows und zweitens, um letztlich selbst die Verantwortung über alles (Information, Betriebssystem und Anwendungen) zu erhalten.

Das Secuware-Betriebssystem nutzt alle seine Module um die Benutzer zu identifizieren, mit einer einzigartigen Technologie, die das Ergebnis langjähriger Erfahrung ist.

Wie sichert SSF die Vertraulichkeit von Informationen?

Durch das SSF Crypt4000-Modul beseitigt das System die Spuren, die auf dem PC oder Laptop zurückbleiben. Zum Beispiel denken viele Nutzer, ihre Informationen seien sicher, weil sie offline arbeiten, aber leider hinterlässt die temporäre Kopie eine Spur auf der Festplatte.

Wenn die Festplatte nicht komplett verschlüsselt ist, ist die temporäre Kopie physisch zugänglich. Etwas Ähnliches geschieht mit Zugangsdaten. Die Festplatte ist im Grunde voller Informations-Spuren, die physisch kompiliert (und versteckt) werden können.

Wenn eine Datei gelöscht wird, ist sie nicht für immer weg. Der Festplattenplatz, den sie verwendet ist lediglich als Speicher reserviert, der später wiederverwendet werden kann. Nur wenn die Festplatte voll ist, werden diese Räume genutzt, damit ihre Zuverlässigkeit auf der ganzen Linie im Einklang steht.

Festplatten haben heute genug Kapazität um diese „Lücken“ eher nicht zu besetzen (Wiederherstellungstools können hier auch verwendet werden) und sie sind daher voll von sensiblen Informationen, von denen der Benutzer glaubt, sie seien gelöscht und dennoch sind sie abrufbar.

Warum muss ich die Ausführung von Anwendungen kontrollieren?

Da Anti-Virus-Programme das Risiko einer Infektion nicht völlig beseitigen (sie funktionieren nur mit bekannten Viren) und sobald ein Virus in ein System eindringt, breitet es sich überall in den angeschlossenen Computern aus. Darüber hinaus ist das System ein Arbeitsmittel und sollte als ein solches benutzt werden – Unternehmen sollten nicht zulassen, dass seine Arbeitnehmer es verwenden, um Musik zu hören, illegale Software zu downloaden, etc.

C4K FAQ's

Warum brauche ich Crypt4000 um meine kompletten Daten zu sichern?

Die Festplattenverschlüsselung ist der effizienteste Weg, die Benutzer-Authentizität, Datenintegration und Datenschutz sicherzustellen.



SECUWARE

Wie schützt Crypt4000 die Benutzer-Authentizität?

Eine verschlüsselte Festplatte stellt sicher, dass das Betriebssystem nicht verändert werden kann, da es geschützt ist. Sie macht es unmöglich, den Computer aus einer alternativen Quelle, wie einer Diskette oder CD-ROM zu starten. Das Log-On-Verfahren ist der Weg, um sicherzustellen, dass die Person vor dem Computer ist, wer sie sagt sie sei. Es verwendet ein durch das Secuware Sicherheits-

Betriebssystem geschütztes kryptografisches Gerät - mit anderen Worten, eine verschlüsselte Festplatte.

Wie funktioniert die Verschlüsselung der Festplatte zum Schutz der gespeicherten Daten auf einem PC oder Laptop?

Secuware Technologie bedeutet, dass, sollte eine Festplatte oder ein Laptop gestohlen werden, ein Zugriff auf die Informationen unmöglich ist. Das Ziel von Secuware ist der Schutz Ihrer Daten vor unerwünschten Augen.

Der beste Weg zum Schutz der Informationen auf einer Festplatte ist die Verschlüsselung mit Secuware Technologie.

Hat die Secuware-Festplattenverschlüsselung Auswirkungen auf den Benutzer?

Die täglichen Aktionen des Anwenders sind durch die Verschlüsselung der Festplatte nicht beeinträchtigt, da alle Geräte in einer sehr transparenten Art und Weise verschlüsselt werden. Weder der Computer verlangsamt, noch muss ein Passwort oder Code verwendet werden. Beide verschlüsselten und unverschlüsselten Geräte garantieren eine benutzerfreundliche und transparente Verwendung.

Secuware-Technologie sorgt dafür, dass die Informationen im Zusammenhang mit wichtigen Mitgliedern einer Organisation nicht „verloren gehen“ und auf eine USB-Festplatte, eine DVD oder eine CD-ROM verschoben werden. Alle wichtigen Informationen, einschließlich der gespeicherten Daten auf einem Firmen-Laptop können nur vor Ort innerhalb des Unternehmens gelesen werden.

Kann der Benutzer seine normalen Programme weiterhin nutzen, sobald die Festplatte verschlüsselt wurde oder gibt es Einschränkungen?

Unser Produkt bietet native Unterstützung, was bedeutet, dass der Benutzer weiterhin die gleiche Software wie bisher - Windows, Nero, Roxio etc. – nutzen kann. Alle Programme, die Informationen speichern, können nun die Daten verschlüsseln, und zwar in einer für den Anwender völlig transparenten Art und Weise.



SECUWARE

Wie verschlüsselt Crypt4000 Netzwerk-Dateien?

Secuware ist in der Lage Netzwerk-Dateien mit symmetrischen Schlüsseln zu verschlüsseln, was bedeutet, der Benutzer nicht bei jedem Zugriff auf ein Dokument sein Passwort eingeben muss.

Wer ist für den Installations- und Inbetriebnahme-Service verantwortlich?

Secuware arbeitet mit einem Partner und Großhändler, die für die Einrichtung und Umsetzung der Secuware-Sicherheitslösungen verantwortlich sind. Natürlich werden

sie jederzeit von einem Secuware-Spezialisten betreut, mit aller Aufmerksamkeit und Engagement, wie es ein solches Projekt erfordert.

Sind Crypt4000 und SSF leicht zu verwalten?

Extrem leicht. Mit einem einfachen Klick haben Sie sofortigen Zugang zu einem ganzen neuen Informations-Sicherheits-System für einen oder für tausend Benutzer. Secuware kann Ihr Unternehmen in einen regelrechten Bunker verwandeln, in den Informationen nur durch sichere Kanäle ein und aus gehen.

Können die Kunden SSF unabhängig installieren und implementieren? Wenn ja, wie?

Ja, dies kann unabhängig gemacht werden, wie jedes Windows-akzeptierte MSI-Paket mithilfe von Windows selbst, SMS oder jede Vertriebs- oder Verwaltungssoftware.

Wie kann es meine Plattform und meine Software integrieren. Ist irgendeine Plattform oder Software inkompatibel?

Unsere Produkte sind perfekt kompatibel mit jeder Software. Sie wurden bereits über 200.000 Mal auf verschiedenen Systemen installiert mit der Vielfalt an Plattformen und Software, die die heutige Zeit mit sich bringt.

Wie viele Personen müssen speziell ausgebildet sein, um diese Anwendung an der täglichen Basis zu nutzen?

Die gleiche Anzahl an Personen, die derzeit die Aufsicht über die System-Administration haben. Es sind keine weiteren Mitarbeiter nötig. Secuware empfiehlt jedoch einen Security Administrator zu benennen, der die Wartung der Secuware Software übernimmt, damit aus Sicherheitsgründen Windowsadministratoren nicht den vollen Zugriff auf alle verschlüsselten Daten und Geräte haben.



SECUWARE

Secuware Deutschland GmbH
Eifelstraße 9
53119 Bonn

Tel: 0228 962979 11
Fax: 0228 962979 29
Email: sales@secu-ware.de
Web: www.secuware.com