White Paper
FUJITSU Software BS2000 SECOS

Sicherheit mit BS2000

Die Sicherheitsrisiken von kommerzieller Datenverarbeitung sind vielfältiger Natur. Sie reichen von Fehlern bei der Benutzung und Bedienung der IT-Systeme bis zu beabsichtigter Computerkriminalität. Folgen können der Verlust der Nutzbarkeit, der Integrität und der Vertraulichkeit der Daten sein. Daher ist es unumgänglich, diese Risiken zu bekämpfen und Sicherheitsmaßnahmen zu treffen, welche Zugriffsbefugnisse verwalten und kontrollieren, potentielle Risiken antizipieren und im Ernstfall abwehren.

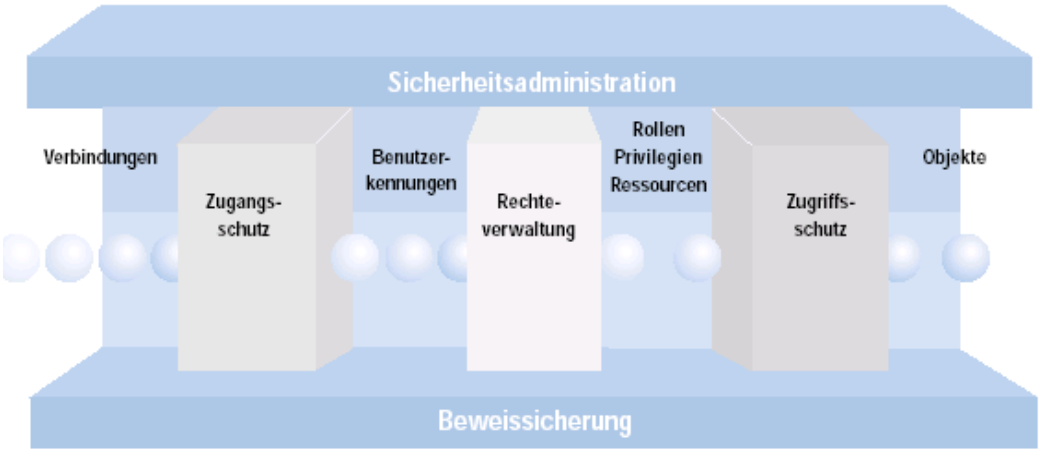
In diesem Meer von Unsicherheiten gibt es nach wie vor eine uneinnehmbare Insel – den Mainframe mit seinen bewährten Sicherheitsmechanismen. Anwendungen und Daten sind nach wie vor nirgends so sicher wie auf dem Mainframe.
Für die BS2000-Plattform garantiert FUJITSU Software BS2000 SECOS und die zugehörigen Verfahren ein sehr hohes, von den Kunden individuell skalierbares Niveau an Systemsicherheit.

Inhalt

Produktbeschreibung

Verlässlicher Datenschutz ist eine wesentliche Voraussetzung beim Einsatz von Systemen in der kommerziellen Datenverarbeitung. Unternehmenskritische Daten müssen gegen vorsätzliche und besonders gegen fahrlässige Modifikation oder Zerstörung wirksam geschützt sein. Das Produkt SECOS realisiert für BS2000 -Systeme einfache bis anspruchsvolle, kundenindividuelle Sicherheitskonzepte.

Die Sicherheits-Grundfunktionen im BS2000 und das Produkt SECOS bieten zusammen weitreichende und skalierbare Sicherheitsoptionen für den BS2000-Betrieb mit den Betriebsarten Dialog, Batch sowie die POSIX-Umgebung und darauf aufbauende Verfahren und Anwendungen. Zusätzlich stehen für das Produkt umfangreiche Services zur Verfügung. Sie reichen von Sicherheitsanalysen bis hin zu schlüsselfertigen SECOS-Lösungen für BS2000-Installationen.



Umfassende und lückenlose Sicherheit sind vital für das eBusiness

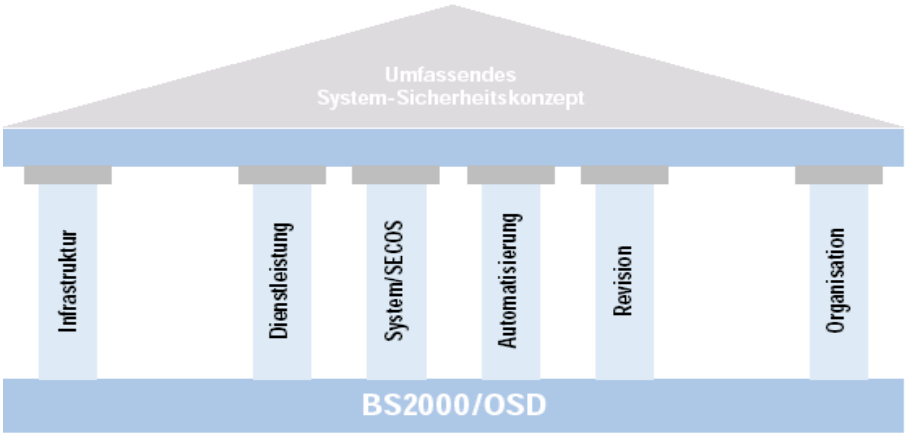
SECOS – Das Sicherheitsschloss zur BS2000-Systemsicherheit

Die BS2000-Plattform bietet die Schlüssel zu individuellen Sicherheitslösungen:

- openSEAS erschließt plattformübergreifende Transaktionssicherheit bis hin zum mobilen Client,
- *open*Networking eröffnet umfassende Netzsicherheit und
- SECOS (SEcurity COntrol System) ist das Sicherheitsschloss zur skalierbaren Systemsicherheit für BS2000-Server.

SECOS ermöglicht Nutzern und Nutzergruppen von BS2000-Systemen, ihre Daten, Aktivitäten, Verfahren und Programme vor Unberechtigten zu verbergen und Manipulationen zu verhindern. Zugleich kann garantiert werden, dass der versuchte Systemmissbrauch durch privilegierte Systembetreiber mit besonderen Befugnissen sofort entdeckt und lückenlos protokolliert wird.

Umfassend heißt, dass alle potenziellen Gefahren für ein System oder aus einem System erfasst und bewertet werden. Dies hängt nicht nur vom System, sondern auch von den individuellen organisatorischen Bedingungen und der IT-Verflechtung des jeweiligen Unternehmens mit Suppliern und Kunden ab.



Nur ein lückenloses Systemsicherheitskonzept führt ans Ziel

SECOS – Das flexible Sicherheitsmanagement

Identifikation von Benutzern

Die Standardmethode zur Nutzerverwaltung ist der Passwortmechanismus. SECOS ermöglicht grobe wie auch feingranulare Spezifikationen von Nutzungsprofilen. Der Zugang zu definierbaren Ressourcen lässt sich auf genau definierte Client-Gruppen für definierbare Zeitintervalle einschränken.
Für die Standardmethode des Identitätsnachweises mit Kennwörtern erlaubt SECOS Vorgaben für deren Gültigkeitsdauer und minimal erforderliche Komplexität, um bekannte Angriffsformen (dictionary attack) zu unterbinden.
SECOS ermöglicht es, BS2000 in ein rechenzentrumsweites, plattformübergreifendes Single-Sign-On-Konzept (SSO mit Kerberos) mit komfortablen Identitätsnachweisen einzubinden.

Der Nutzen der feingranularen Zugangssteuerung ergibt sich aus folgenden Sicherheitsszenarien:

- Der Zugriff von außerhalb des Unternehmens auf die Serverressourcen muss kontrollierbar sein, Attacken sind abzuwehren.
- Der Zugriff von innerhalb des Unternehmens auf die Serverressourcen muss kontrollierbar sein, insbesondere der von privilegierten Nutzern.

Strategie „Sicherheit durch Rollenverteilung“

Im BS2000 ist das Sicherheitsmanagement zentralisiert. Ein Sicherheitsbeauftragter legt fest, wer welche privilegierten Aktionen ausführen darf und in welchem Umfang protokolliert wird.

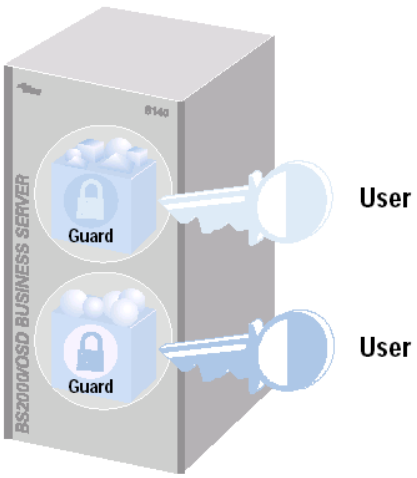
Er verteilt unter anderem die Rollen zur Sicherheitsverwaltung:

- Rolle „User verwalten“
- Rolle „Zugriffsrechte systemweit verwalten“
- Rolle „Protokollierung sicherheitsrelevanter Ereignisse steuern“
- Rolle „File Transfer Access Control verwalten“.

Die User-Verwaltung wiederum kann jeden User ermächtigen sein Kennwort selbst zu verwalten. Jeder User kann dann die Zugriffsrechte auf seine Objekte (die Objekte seiner Benutzerkennung) managen.

Strategie „Objektorientiertes Sicherheitsmanagement“

Für Dateien, Bibliotheken, Jobvariablen und Prozesskommunikation (FITC-Ports) bietet SECOS ein einheitliches Verfahren für den Zugriffschutz. Bei diesem Verfahren werden, unabhängig von den zu schützenden Objekten und Objektarten, Schutzprofile definiert. Diese Schutzprofile werden als Guards bezeichnet. Jedes Guard lässt sich mit beliebig vielen und verschiedenartigen Objekten verknüpfen.



In einem Guard wird festgelegt:

- Welcher Benutzer oder welche Benutzergruppe zugreifen darf,
- welches Privileg ein Zugreifer haben muss,
- zu welcher Zeit Zugriffe erlaubt oder verboten sind,
- mit welchen Programmen der Zugriff erfolgen darf.

Strategie „Sichern von Beweisen"

Ein Sicherheitssystem, in dem bei Sicherheitsverletzungen keine eindeutige Zuordnung zu Verursachern möglich ist, ist wertlos. Daher zeichnet SECOS für alle sicherheitsrelevanten Ereignisse den Zeitpunkt, die Benutzerkennung des Auslösers, das Resultat der Aktion und – soweit vorhanden – die persönliche Kennung des Auslösers auf.

Eine personenbezogene Rückverfolgung kann auch dann gewährleistet werden, wenn aus technischen oder organisatorischen Gründen mehrere User unter der gleichen User-Kennung arbeiten.

Darunter sind

- Logon, POSIX remote login, Batch-Job-Start,
- Modifikation einer Datei, eines Bibliothekselements,
- Vergabe von Privilegien,
- Zuteilung einer Operator-Rolle,
- Bearbeiten von Datenträgern (Bänder, Platten),
- Aktivierung von Subsystemen.

Das Eintreten wichtiger, potenziell bedrohlicher Ereignisse alarmiert automatisch die Operateure oder programmierte Automaten. Auch „Alarme" werden natürlich protokolliert.

Die Sicherheitsprotokolle können nach Sicherheits- und Revisionsgesichtspunkten ausgewertet und langfristig archiviert werden. Zusätzlich können der Sicherheitsbeauftragte, die Systembetreuung sowie die individuellen User die jeweils für sie relevanten Sicherheitseinstellungen jederzeit überprüfen.

Strategie „Umfassendes Sicherheitsmanagement mit Fujitsu Know-how"

Ein hohes Sicherheitsniveau für Systeme ist nur erreichbar, wenn vor dem Ergreifen von Sicherheitsmaßnahmen eine umfassende Analyse der Sicherheitsrisiken stattfindet.
Fujitsu Technology Solutions bietet seinen Kunden hierfür weiterreichende Unterstützung an.

Zusammenfassung

- Die Skalierbarkeit der Funktionen garantiert Sicherheit nach den individuellen Anforderungen des Kunden.
- Das umfassende Sicherheitskonzept von SECOS gewährleistet, dass auch die hohen Ansprüche der Revision (Datenschutzbeauftragter, Bankenrevision u.a.) erfüllt werden.

Kontakt:
Fujitsu
Barbara Stadler
Mies-van-der-Rohe-Straße 8, 80807 München
Deutschland
Telefon: +49 (0)89-62060-1978
E-mail: barbara.stadler@ts.fujitsu.com
Website: de.fujitsu.com
31. August 2015 EM DE