Datenblatt

Fujitsu Software BS2000 SECOS V5.6

Security Control System

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 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.

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.

Die BS2000 Business Server können mit ihren Sicherheitsfunktionen, insbesondere SECOS, erfolgreich in Security Audits einbezogen werden und damit zur Zertifizierung des Sicherheitsmanagements eines Unternehmens beitragen.

Green IT

Merkmale und Nutzen

Hauptmerkmale	Nutzen
Erweiterter Zugangsschutz • Regeln für Kennwörter (Beschränkung der Lebensdauer, Mindest-Anforderung an die Komplexität) • Sperren und Überwachen von Kennungen/Terminals (Zeitabhängig, nach Anzahl von Fehlversuchen) • Persönliches LOGON (zusätzliche Authentisierung bei gemeinsam genutzten Kennungen) • Zuordnung einer Zugangsklasse je Benutzerkennung • Unterstützung von Single Sign On-Funktionen mit Kerberos	• Kein unerlaubter Zugang durch systematisches Ausprobieren des Passwortes • Kontrolle über Zugangswege • Benutzeranmeldung ohne Kennwort-Angabe im Sinne von Single Sign On möglich
Rechteverwaltung • Dezentralisierung der Systemverwaltung mit Hilfe von Privilegien für einzelne Benutzerkennungen • Einführung kundenspezifischer Rollenkonzepte • Zusammenfassen von Benutzer zu Benutzergruppen	• Dezentralisierung der Aufgaben der Systemverwaltung • Kundenprivilegien für kundenspezifische Sicherheitsrollen • Abbildung von org. Einheiten oder Projekten auf Benutzergruppen mit gemeinsamer Verwaltung
Erweiterter Zugangsschutz auf Objekte • Definition von Zugriffsbedingungen durch den Benutzer unabhängig vom Objekt mittels GUARDS • Default Protection (Objektschutz bereits zum Erstellungszeitpunkt) • Miteigentümerschaft für Dateien und JVs • Eingeschränkte Miteigentümerschaft für TSOS	• Lückenloser Schutz von Objekten • Festlegen der Zugriffsrechte übergreifend über mehrere Objekte • Definition von Zugriffsrechten bis auf die Ebene von Einzelbenutzer
Beweissicherung • Selektive Protokollierung von sicherheitsrelevanten Ereignissen • Speicherung und Auswertung der Beweissicherungsdaten für Revision und Sicherheitsanalysen	• Erkennen von Eindringversuchen und Verstößen gegen die Sicherheitspolitik • Lückenloser Überblick über Objektzugriffe • Rückführen sicherheitsrelevanter Ereignisse auf die verantwortliche Person

Themen

Erweiterter Zugriffsschutz

Durch die erweiterte Zugangskontrolle wird im BS2000 der Passwortschutz durch Maßnahmen verbessert, die ein systematisches Ausprobieren der LOGON-Passwörter im praktischen Betrieb wirkungsvoll verhindern. Zusätzlich zu den bestehenden Möglichkeiten (z.B. die Verschlüsselung von Passwörtern) werden folgende Mechanismen im Produkt SECOS angeboten:

- Die Vorgabe einer **minimalen Länge eines Passwortes** zwingt die Benutzer eine bestimmte Länge bei Passwörtern einzuhalten, um zu verhindern, dass ohne oder mit Trivial-Passwörtern im System gearbeitet wird.
- Durch **Mindestkomplexität von Passwörtern** soll verhindert werden, dass Passworte zu einfach definiert werden.
- **Begrenzung der Lebensdauer eines Passwortes**. Diese Vorgabe zwingt den Eigentümer einer Benutzerkennung, sein Passwort nach einer bestimmten Zeit zu ändern, dadurch wird die Sicherheit bei Verwendung von Passwörtern erhöht.
- **Unterstützung eines Initialpasswortes**.
  Der Systemverwalter erhält bei der Vergabe eines neuen Passwortes die Möglichkeit, neben der Angabe der ersten Passwortlebensdauer, das neue Passwort sogleich als verfallen zu kennzeichnen. Dies zwingt den Benutzer beim nächsten Dialog zur Vereinbarung eines neuen Passwortes.
- **Passwort-Historie**.
  Durch das Abspeichern bereits verwendeter Passwörter (in vorgebbarer Anzahl) wird das nochmalige Verwenden von Passwörtern verhindert.
  Damit ist die Gültigkeitsdauer eines Passwortes exakt nachvollziehbar.

Sperren und Überwachen von Kennungen/Terminals

- Die **Begrenzung der Lebensdauer einer Benutzerkennung** ist in solchen Fällen angebracht, wo abzusehen ist, dass eine bestimmte Benutzerkennung nur über eine bestimmte Zeit Gültigkeit besitzen soll.
- **Auskunftsfunktion über letzten LOGON-Zugang**.
  Nach erfolgreichen Terminal-Logon erhält der Benutzer Informationen, welche die Sicherheit seiner Kennung betreffen. Mit diesen Informationen kann der Benutzer z. B. feststellen, wann zuletzt mit seiner Kennung gearbeitet wurde oder wie viel Fehlversuche zwischen dem jetzigen und dem letzten erfolgreichen Zugang erfolgt sind. Diese Informationen dienen dem Sicherheitsbedürfnis des Anwenders und machen ihn unabhängig von der Aufmerksamkeit des Sicherheitsbeauftragten.
- Kennungen / Terminals können nach n Fehlversuchen gesperrt werden (Bisher wurden Fehlversuche bei der Kennworteingabe mit Zeitstrafen oder Verbindungsabbau geahndet; dadurch konnten aber auch schon maschinelle Eindringversuche verhindert werden.). Ebenso können Kennungen gesperrt werden, die n Tage nicht mehr verwendet wurden.

Einschränkung des Dialog-Zuganges basierend auf der Funktion “Persönliches LOGON”.

Für die eindeutige Kennzeichnung einer bestimmten Person zusätzlich zur Benutzerkennung, insbesondere zum Zwecke der Beweissicherung kann zur Authentisierung von Dialogaufträgen das persönliche LOGON festgelegt werden.

Differenzierung verschiedener Zugangsklassen

- Für jede Benutzerkennung kann separat festgelegt werden, mit welchen Methoden (z.B. Dialog, Batch, POSIX rlogin) der Zugang erlaubt ist. Damit wird ermöglicht, dass die verschiedenen Zugangswege kontrolliert werden können. Weiterhin kann der Partner im Netz, insbesondere Terminals eingeschränkt werden.
- Zur Unterstützung von POSIX sind mehrere Zugangsklassen realisiert. Damit kann z.B. der Zugang von rechnerübergreifenden POSIX-Kommandos unabhängig vom POSIX-rlogin verwaltet werden. Eine weitere Zugangsklasse ermöglicht die gezielte Freischaltung von Benutzerkennungen für POSIX-Servertasks.

Unterstützung von Single Sign On-Funktionen mit Kerberos

SECOS bietet BS2000-Anwendern die Möglichkeit, mittels Kerberos-Authentifizierung die Benutzeranmeldungen (LOGON) im Sinne eines Single Sign On (SSO) ohne Kennwort-Angabe durchzuführen. Es wurde ein Kerberos Client im BS2000 realisiert, der den (in der Regel) im BS2000-Umfeld existierenden Windows Primary Domain Controller (PDC) als Server (Key Distribution Center) benutzt.
Auf der Client-Seite ist die Unterstützung der Kerberos-Authentifizierungsfunktion in der Terminal-Emulation MT9750 sowie in weiteren Emulationen von SW-Partnern erfolgt.
Die Kerberos Authentifizierungs-Funktionalität steht auch für TU-Anwendungen zur Verfügung. Erste Nutzer sind OMNIS, OMNIS-MENU und openUTM.

Rechteverwaltung

Privilegien - Dezentralisierung der Systemverwaltung

Mit SECOS wird eine Rechteverwaltung realisiert, welche die unterschiedlichen Administrationsaufgaben der Benutzerkennung TSOS auf mehrere andere Benutzerkennungen verteilen kann. Ziel dieser Vorgehensweise ist es, von den umfassenden Rechten der bisherigen Systemverwalterkennung abzukommen und den realen Gegebenheiten einer aufgeteilten Systemverwaltung Rechnung zu tragen.
Einzelprivilegien können zu einem Sammelprivileg zusammengefasst und RZ-spezifisch mit einer Rollenbezeichnung belegt werden. Damit können Tätigkeitsbereiche bestehend aus mehreren Einzelprivilegien gebildet werden.

Einführung von Benutzergruppen

Benutzergruppen einzurichten hat den Vorteil, dass die Vielzahl von Benutzern, welche im System vorhanden sind, übersichtlicher strukturiert werden können. Außerdem wird es möglich, organisatorische Einheiten oder Projekte, welche durch bestimmte Personen mit Benutzerkennungen dargestellt werden, auch mit der entsprechenden Betriebsmittelzuordnung im System nachzubilden. Ziel dabei ist, dass die Verwaltung gemäß vorgegebenen Auflagen dezentral durch den Gruppenverwalter vorgenommen werden kann und damit die Systemverwaltung von diesen Aufgaben entlastet wird.
Zur besseren Verwaltung von Benutzergruppen wird für den Gruppenverwalter die Möglichkeit geboten, eine eigene Namenszuordnung zu wählen. Dies erfolgt mit Hilfe von Musterzeichen für die Festlegung von eindeutigen Namen für Benutzergruppen und Gruppenmitglieder.
Neben der grundsätzlichen Bedeutung der Gruppen bei der Verwaltung von Ressourcen, spielen die Gruppen auch beim Zugriff auf Dateien und Jobvariable eine Rolle.

Erweiterung des Gruppenzugriffs

Prinzipiell kann eine Benutzerkennung immer nur einer einzigen Benutzergruppe zugeordnet sein.
Dadurch ergeben sich Probleme, wenn ein Mitarbeiter gleichzeitig in mehreren Gruppen tätig ist, und damit Zugriff auf die entsprechenden Datenbestände benötigt.
In solchen Fällen kann beim Zugriff auf Dateien und Jobvariablen, die durch einfache Zugriffskontrollliste geschützt sind, zusätzlich zu den eigentlichen Gruppenmitgliedern weiteren Benutzern die gleichen Zugriffsrechte eingeräumt werden.

Ein Benutzer in mehreren Benutzergruppen

Die Benutzergruppen werden in der Praxis für die Zuordnung von Mitarbeitern zu einem bestimmten Verfahren/Projekten benötigt. Bisher gab es Probleme, wenn ein Mitarbeiter gleichzeitig in mehreren Verfahren tätig war. Mit SECOS kann ein Benutzer zum Zwecke der Prüfung von Dateizugriffen mehreren Benutzergruppen zugeordnet werden. Damit können die praktischen Anforderungen des Kunden besser abgebildet werden.

Erweiterter Zugriffsschutz auf Objekte

Möglichkeiten der Zugriffskontrolle auf Objekte

Zum Schutz der Dateien im BS2000 steht der bisherige und weitere Schutzmechanismen zur Verfügung, die unterschiedlich die Mehrbenutzbarkeit von Dateien und die Zugriffsrechte regeln.

- Mit der Standardzugriffskontrolle kann wie bisher festgelegt werden, ob die Datei nur für den Eigentümer oder für alle im System definierten Benutzerkennungen zugreifbar ist.
- Die einfache Zugriffskontrollliste erlaubt eine feinere Schutzmöglichkeit. An möglichen Zugriffsarten stehen Lesen, Schreiben und Ausführen zur Verfügung. Die Zugriffsrechte können voneinander unabhängig für den Eigentümer (Owner), die Mitglieder der Benutzergruppe des Eigentümers (Group) und alle anderen Benutzer (Others) festgelegt werden.

Mit dem Subsystem GUARDS wird ein unabhängiger benutzerbestimmbarer Zugriffsschutzmechanismus für Objekte unterschiedlichen Typs, wie zum Beispiel Dateien, Bibliothekselemente, FITC-Ports und Programme zur Verfügung gestellt. Die Schutzkriterien werden dabei zentral im System verwaltet und die Schutzdefinitionen, bezogen auf ein bestimmtes Objekt, in einem so genannten Guard zusammengefasst. Die Guards sind universell anwendbar und objektunabhängig im System realisiert.
Dies hat den Vorteil, dass mit einfachem Handling mehrere Objekte mit den gleichen Zugriffsrechten versehen werden können und der Zugriffsschutz von mehreren Objekten auch auf einfache Weise dynamisch geändert werden kann.
In einem Guard können zusätzlich Bedingungen spezifiziert werden, welche bei einem Zugriff auf das Objekt ausgewertet werden. Bedingungen können die Privilegierung des Benutzers, eine Zeitangabe oder ein Zeitintervall für den Zugriff oder eine Systembedingung sein.

Default Protection

Durch den Einsatz der Funktion Default Protection wird der Zugriffschutz für Objekte (Dateien und JVs) wesentlich erhöht. Dem Anwender wird mit dieser Funktion die Möglichkeit geboten, Standardeinstellungen von Schutzattributen objektspezifisch vorzunehmen und damit Objekte schon zum Erstellungszeitpunkt wirksam zu schützen. Diese Einstellung kann kennungs- oder pubset-spezifisch für Dateinamensräume vorgenommen werden. Explizite Benutzerangaben überschreiben die Voreinstellungen.

Co-owner Protection / Miteigentümerschaft

Mittels der Co-owner-Funktionalität wird die Möglichkeit geboten, eine Miteigentümerschaft bezogen auf Dateien und JVs (wie sie von TSOS bisher schon bekannt ist) auch für andere Kennungen einzurichten.
Mit demselben Verfahren kann auch der Benutzerkennung TSOS die standardmäßig vorhandene Miteigentümerschaft entzogen werden.

Beweissicherung

Zur Beweissicherung dient im BS2000 das Subsystem SAT (Security Audit Trail), ein Bestandteil des Produktes SECOS. Dieses Subsystem unterstützt die selektive Protokollierung von sicherheitsrelevanten Ereignissen in besonders geschützten Dateien (SAT Logging Files). Mit Auswertung dieser Dateien erhalten entsprechend autorisierte Benutzer einen lückenlosen Überblick, welcher Benutzer, zu welchem Zeitpunkt, in welcher Art und Weise auf ein bestimmtes Objekt zugegriffen hat. Weiterhin ist es möglich, einen Rückblick auf spezielle Verarbeitungsschritte und Aktionen von bestimmten Benutzerkennungen zu erhalten, um eine missbräuchliche Benutzung des Systems oder den unerlaubten Zugriff auf gesicherte Daten zu entdecken.
Neben der Protokollierungs-Funktion wird zusätzlich eine ALARM-Funktion angeboten. Der Sicherheitsbeauftragte erhält die Möglichkeit, Bedingungen zu definieren, welche beim Aufruf von bestimmten Ereignissen einen Alarm auslösen. Tritt ein Alarm auf, erfolgt eine Meldung auf der Hauptkonsole und zusätzlich wird das Ereignis in die Protokollierungsdatei geschrieben.
Einer Voranalyse dient die Offline-Ausgabe von SAT-Statistikdaten. Dabei sind unterschiedliche Ausgaben möglich, wie z.B. SAT-Statistik von wichtigen Ereignistypen oder die Zusammenfassung von Ereignistypen.
Bei der Präselektion kann ähnlich einer Alarmdefinition ein Filter mit Bedingungen angegeben werden. Trifft eine dieser Bedingungen zu, wird abhängig von der Art des Filters protokolliert (Positivfilter) oder nicht protokolliert (Negativfilter). Zur genaueren Analyse von Schutzverletzungen kann neben dem Ergebnis auch die vollständige Parameterliste protokolliert werden.

Technische Details

Voraussetzungen	
Technische Voraussetzungen Hardware	Fujitsu Server BS2000 SE Serie
Technische Voraussetzungen Software	BS2000 OS DX V1.0 - SDF-P für die Funktion CONVERT-KEYTAB
Anforderungen an den Benutzer	BS2000-Kenntnisse
Installation und Betrieb	
Betriebsart	Dialog- und Batchbetrieb
Implementierungssprache	C, Assembler
Benutzeroberfläche	Kommandos englisch, Meldungstexte wahlweise deutsch/englisch
Installation	Durch den Kunden anhand des Benutzerhandbuchs
Dokumentation und Training	
Dokumentation	Benutzerhandbuch und Freigabemitteilung zu SECOS sind am Manual-Server verfügbar.
Schulung	Siehe Kursangebot.
Konditionen	
Bedingungen	Dieses Softwareprodukt wird den Kunden zu den Bedingungen für die Nutzung von Softwareprodukten gegen laufende Zahlung überlassen.
Bestell- und Lieferhinweise	Das Softwareprodukt kann über den für Sie zuständigen Sitz der Region von Fujitsu bezogen werden.

Kontakt

Fujitsu
BS2000 Services
Email: bs2000services@fujitsu.com
Website: www.fujitsu.com/de/bs2000
30.06.2022