JET SOFTWARE

JET-SECURITY

Identity- und Accessmanagement

für Linux/Unix

Übersicht

Funktionen

Sicherheit

Produktbeschreibung

Pool-Verwaltung der Datenstationen unter einem Namen
Zusammenfassung der Kennungen zu Gruppen
Dynamische Veränderungen der Zugangsberechtigungen
Optionales Verhalten bei LOGON-Fehlversuchen
Vereinfachung der Verwaltung durch Zusammenfassung
Optionale Protokollierung der (auch ungültigen) LOGON-Versuche
Zentrale und revisionssichere Protokollierung aller Eingaben

Allgemeines

Das Gesamtpaket *JET-SECURITY* bietet über bestehende Standards hinaus, eine zusätzliche Stufe der System-Sicherheit und des System-Journals. Der Zugang zu *JET-SECURITY* ist nur über ein zeitbegrenztes Passwort möglich. *JET-SECURITY* basiert nicht nur auf Systemstandard-Routinen, sondern verwendet eine besondere vorgeschaltete Schnittstelle und ist so unabhängig von bestimmten Derivaten der Linux/Unix-Systeme. Bestehende Standard-Sicherheiten bleiben erhalten und benötigen auch keine Veränderungen an bestehender Ausrüstung des Systems.

Beim Einsatz des *JET-SECURITY*-Verfahrens können für Benutzerkennungen präzisere Einschränkungen sowie Freigaben des Systemzugangs und der Protokollierung vereinbart werden, die über den Standard des Systems hinausgehen. Diese werden durch den Administrator des *JET-SECURITY*-Verfahrens für die entsprechenden Benutzerkennungen spezifiziert. Er muss nicht notwendigerweise auch der Systembetreuer sein, somit benötigt er auch keinerlei Systembefugnisse. Die vereinbarten Zugangsbeschränkungen können zentral verwaltet werden. Einschränkungen sowie Freigaben des Systemzugangs werden individuell für jeden Benutzer nachgehalten.

- Übersicht
- **Funktionen**
- Sicherheit

Revisionssichere Protokollierung

Über ausgewählte Systemfunktionen kann ein revisionsicheres Protokoll erstellt werden. Nach erfolgreichem Zugang zum System werden ausgewählte Funktionen verschlüsselt und revisionssicher mitprotokolliert. Das gilt für die Aktivitäten des Systemadministrators, sowohl als auch für jeden Benutzer separat. In einem gesonderten Protokoll werden die Aktivitäten des Systemadministrators registriert. Die Auswertung dieser Protokolle kann nur durch den Verwalter des Security-Systems erfolgen. Weder der Systemadministrator, noch die Anwender haben Zugriff darauf.

Die Protokolle werden verschlüsselt, mit Prüfungen erzeugt und abgelegt. Wegen den Verschlüsselungen und Querverbindungen untereinander, ist eine Manipulation dieser Dateien und deren Inhalte nicht möglich. Auch eine versuchte Manipulation wird durch das System zuverlässig entdeckt, zusätzlich erfolgt ein sofortiger Hinweis und der entsprechende Benutzer wird sofort vom System abgemeldet. Dieser kann sich nicht mehr ohne Freischaltung durch den Systemadministrator anmelden. Darüber hinaus wird der Zugang zum System verhindert, indem Änderungen der Einstellungen jetzt nicht mehr vorgenommen werden können bevor der Security-Verwalter eingegriffen hat

Zugangserkennungen

Besteht für eine Benutzerkennung ein Eintrag in der SECURITY-Datei, ist dann ein LOGON nur in den angegebenen Betriebsarten und von den angegebenen Datenstationen möglich. Grundsätzlich geschieht die LOGON-Überprüfung auch für Benutzerkennungen, welche keinen eigenen Eintrag in der SECURITY-Datei haben. Für Solche gelten die Parameterwerte, die bei globaler Anweisung angegeben werden.

Benutzer- und Stationsgruppen, Pool

Zur Vereinfachung der SECURITY-Verwaltung und zur gezielten Zugangskontrolle gleichartiger Benutzerkennungen, können Diese und Stationsnamen gruppiert werden. Stationen und auch Stationsgruppen können mit gleichen Berechtigungen zu einem "Pool" zusammengefasst werden. Dieser Pool wird mit einem frei wählbaren Namen verwaltet und angesprochen. Dessen Konsistenz wird auch überwacht.

Ausnahmen

Mit der Funktion "Ausnahmen" können Stationen bzw. Stationsgruppen vereinbart werden, von denen ein LOGON immer abgewiesen wird, außer wenn sie explizit in einem Benutzereintrag berechtigt sind und sich dann darunter anmelden. Mit dieser Funktion kann der Zugang für bestimmte Stationen ganz oder teilweise unterbunden werden (z. B. Stationen, die nur im Teilnehmerbetrieb arbeiten sollen oder bei Wählleitungen).

JET-SECURITY besteht aus mehreren Modulen: Module zum Erstellen der Funktionalität, zur Ausführung und zur Auswertung der Aktivitäten. Die Aufteilung in verschiedene Module bietet zum einen eine höhere Stufe der Sicherheit, als auch zum anderen einen flexiblen Einsatz auf unterschiedlichen Systemen (auch ohne grafische Oberfläche), und die Überwachung des Zugangs über LDAP.

Freigaben und Beschränkungen

Die Systemzugänge können für die Benutzer einzeln freigegeben werden. Diese Einstellungen können in Kombination nach verschiedenen Kriterien erfolgen: Abschnittsweise nach Tagen, Wochentagen, Wochen oder Monaten und dabei wieder nach mehreren Uhrzeiten gestaffelt. Dies gilt auch für den Ausschluss vom System, wann sich Benutzer keinesfalls anmelden dürfen.

LOGON

Für einen LOGON wird der Anwender zur Eingabe seines individuellen Kennwortes aufgefordert. Informationen über den letzten erfolgreichen und evtl. fehlerhaften LOGON werden ausgegeben. Nach Ablauf der maximalen Geltungsdauer des Kennwortes wird der Benutzer zur Eingabe eines neuen Kennwortes gezwungen. Wenn die Maximalanzahl von Fehlversuchen erreicht ist, können Einträge für die Benutzer gesperrt werden und nur der Security-Verwalter kann diese Sperre aufheben. Diese Vorgänge werden automatisch protokolliert.

Zusätzlich zur eigentlichen Anmeldung kann zwangsweise ein individuelles Programm benutzerspezifisch ausgeführt werden. Besondere Anmeldungen können nur erfolgen, wenn sie vom Administrator zusätzlich manuell individuell bestätigt werden. Die Protokollierung kann für alle oder einzelne Einträge zugeschaltet werden. Dann werden alle Kommandoeingaben und Systemausgaben der definierten Dialog-Tasks revisionssicher und zentral protokolliert.

Übersicht

Funktionen

Sicherheit

Präambel- Programm

Zusätzlich zur eigentichen Anmeldung kann benutzerspezifisch zwangsweise ein individuelles Programm ausgeführt werden.

Verwaltung der SECURITY-Datei

Die SECURITY-Datei des Verwalters wird automatisch mitverwaltet. Der Änderungsstand dieser Datei wird revisionssicher und verschlüsselt fortgeschrieben. Bei Bedarf kann eine Prüfung auf logische Unverträglichkeiten der Einstellungen durchgeführt werden, um zu verhindern, dass bspw. alle Benutzer vom System abgewiesen würden.

Unsere Software ist seit über 30 Jahren aktiv im Einsatz bei:

- Deutschen Bundes- und Landesbehörden
- Sozial- und Privatversicherungen
- Landes-, Privat- und Großbanken
- nationalen und internationalen Dienstleistern
- dem Mittelstand und Großunternehmen

MADE IN GERMANY

Unberechtigte Benutzer

Beim Ausscheiden eines Mitarbeiters sollte dessen Zugang zum System schnellstmöglich gesperrt werden. Dies ist jedoch eine manuelle Tätigkeit des Systemverwalters. Irrtümlich kann diese Sperre unterblieben sein und der ehemalige Mitarbeiter kann unter Umständen beliebigen Zugang zum System erlangen. Dieses stellt besonders bei Zugang über Wählleitungen eine erhebliche Sicherheitslücke dar. Zur Feststellung dieser unbenötigten Benutzerzugänge kann eine Prüfung durchgeführt werden. Dabei fallen diese schlafenden Zugänge auf und können gelöscht werden. Auch hierüber wird ein revisionssicheres Protokoll erstellt.

Protokolle

In den individuellen Zugangsdateien werden weitere Einzelheiten überwiegend für die Datei- (geplante Option) und Systemüberwachung, wie OPEN, ERASE, READ, WRITE, CD, ABORT, TERMINATE und Dialog-Kommandos, verschlüsselt gespeichert. Über diese Funktionen und auch deren evtl. Missbrauch, kann ein revisionssicheres Protokoll erstellt werden.

Auswertungen

Protokolle können unabhängig vom eigentlichen Systemlauf ausgewertet werden. Das Protokoll des Verwalters und Protokolle der einzelnen Benutzerprogramme werden separat nachgehalten und können somit auch separat ausgewertet werden.

- Übersicht
- Funktionen
- **Sicherheit**

System-Protokoll

Sollten Unstimmigkeiten an den Einstellungen oder Protokollen festgestellt werden, so wird die Ursache in Klartext angezeigt und der Zugang zum System erschwert. Ursache könnte beispielsweise eine versuchte Manipulation der Einstellungsparameter sein. Die Überprüfung erfolgt zwangsweise automatisch.

Kontakt

Für weitere Informationen und für eine kostenlose Testversion wenden Sie sich bitte an:

JET-Software GmbH
Steinweg 1
D-64832 Babenhausen
Tel.: +49 (0) 6073-71140-3
E-Mail: info@jet-software.com
Web: www.jet-software.com