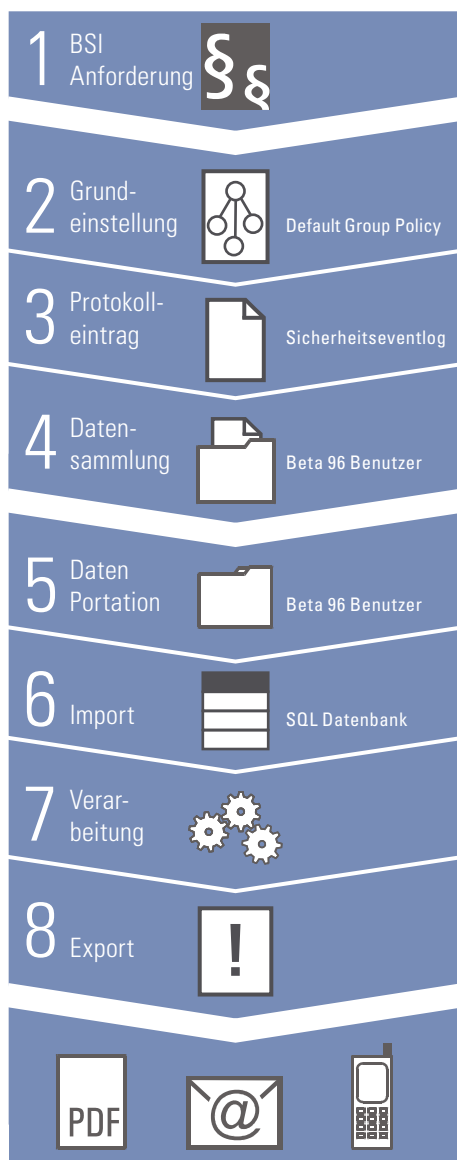


[Beta 96] Enterprise Compliance Auditor

Der Logfileentstehungs- und verarbeitungsprozess am Beispiel der Complianceanforderung M. 2.231 "Planung der Gruppenrichtlinien für Windowssysteme" der IT-Grundschutzkataloge des BSI.



Gemäß der Maßnahme 2.231 der BSI IT-Grundschutzkataloge sind für eine ausreichende Sicherheit von Windowssystemen die fehlgeschlagenen Anmeldeversuche zu protokollieren.

Grundvoraussetzung für die Überwachung und Auswertung fehlgeschlagener Anmeldeversuche ist es, am Windows Domain Controller die grundlegenden Einstellungen für die Protokollierung der Logfiles vorzunehmen. Dies geschieht in der entsprechenden Default Group Policy des Domain Controllers.

Durch diese Grundeinstellung produziert jeder Domain Controller, an dem eine fehlgeschlagene Anmeldung registriert wird, einen Eintrag in dem Sicherheitseventlog.

Das Sicherheitseventlog wird mittels bordeigener Mittel (z.B. DumpEL) ausgelesen, in eine ASCII Datei geschrieben und in einem Ordner, der durch Zugriffsrechte für den Beta 96 Enterprise Compliance Auditor gesichert ist, gesammelt.

Diese Eventdateien können mit vorhandenen Transportmitteln oder durch Beta 96 Transfer-Agenten zur Beta 96 Enterprise Compliance Auswertungseinheit portiert werden.

Der Beta 96 Enterprise Compliance Auditor selektiert die entsprechenden Felder in den Dateien und überführt sie in eine SQL Datenbank (die Kriterien hierfür werden vorher im Beta 96 Enterprise Compliance Auditor definiert).

Mittels der auf den BSI IT-Grundschutz-Maßnahmen aufbauenden Policies (Auswertungsvorschriften) werden die Dateien analysiert und ausgewertet.

Die Ergebnisse zeigen, wie viele Anmeldeversuche fehlgeschlagen sind, welcher User (anonymisiert, pseudonymisiert oder personalisiert) falsch angemeldet wurde und an welcher Einheit die Anmeldung versucht wurde. Zusätzlich erstellt der Beta 96 Enterprise Compliance Auditor einen Summenreport, aus dem schnell ersichtlich ist, wer bzw. wo eine mehrfach fehlgeschlagene Anmeldung versucht wurde.

Die Ergebnisse können in verschiedenen Dateiformaten dargestellt werden. Meldungen zu schwerwiegenden Problemen können per E-Mail oder per SMS an die Verantwortlichen versendet werden.

