

## ServSicht Produktinformation

ServSicht kontrolliert die Sicherheits-Ereignisanzeige (Windows Server 2000/2003 Domänen-Controller) auf eventuelle Netzwerk-Eindringversuche und Angriffe auf Benutzer mit Administratorenrechten.

Administratoren wissen, daß die tägliche Überwachung der Ereignisanzeige auf mißlungene Anmeldeversuche eine Forderung des Datenschutzes ist. Administratoren wissen auch, daß fehlgeschlagene Anmeldeversuche auf Benutzer mit Administratorenrechten grundsätzlich ohne Sanktionen bleiben. Das bedeutet, eine eingestellte Kontosperrung erfolgt auch nach den zulässigen Fehlversuchen nicht. Eine Überwachung der Ereignisprotokolle aller Domänen-Controller ist daher für die Sicherheit unerlässlich. In der Praxis dürfte dies aufgrund der enormen Fülle der Ereignisanzeige kaum möglich sein. Eventuelle Angriffe auf das Netzwerk sind für den Administrator nur schwer erkennbar. Hacker wissen das, der Datenschutz auch und wir ebenso. Kopieren Sie einfach ServSicht auf einem Domänen-Controller und starten Sie das Tool im laufendem Betrieb. ServSicht durchsucht die Sicherheits-Ereignisanzeige (Windows Server 2000/2003) auf mißlungene Anmeldeversuche der Arbeitsstationen. In Sekundenschnelle wird Ihnen das Ergebnis in aussagefähigen und komfortablen Auswertungen angezeigt. Neben den verdichteten Daten stehen auch Einzelauswertungen zur Verfügung. ServSicht zeigt Ihnen die Fehlversuche mit den zugehörigen und fehlgeschlagenen Benutzernamen. Sie erkennen daher sofort Anschläge auf Administratoren oder andere wichtige Benutzer. Einzelauswertungen können ausgedruckt werden und sind somit für eine Datenschutzrechtliche Überprüfung dokumentiert.

### **Folgende Vorgaben für eine Auswertung sind möglich:**

Sicherheits-Ereignisprotokoll

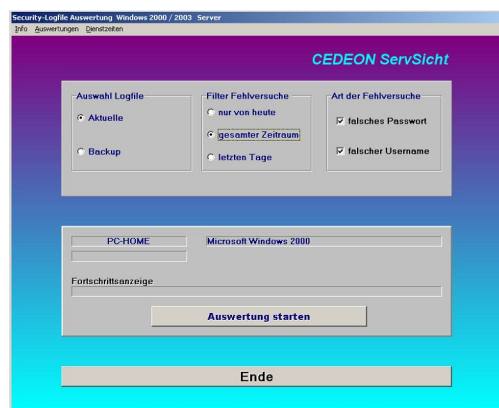
- aktives Ereignisprotokoll
- archiviertes Ereignisprotokoll für eine nachträgliche Auswertung (z.B., Kontrollnachweis)

Grund der fehlgeschlagenen Anmeldeversuche

- falsches Passwort
- falscher User/Benutzername

Zeitliche Begrenzung der Ereignisse:

- keine Begrenzung
- nur heutige Ereignisse
- einstellbarer Zeitraum



### **Folgende Auswertungen – Berichte stehen zur Verfügung:**

- Alarmierungsliste
- Übersicht: Verdichtung und Anzahl der Anmeldefehlversuche nach Arbeitsstationen
- Übersicht: Verdichtung und Anzahl der Anmeldefehlversuche nach Benutzernamen
- Einzelaufstellung der Anmeldefehlversuche mit verschiedenen Sortiermöglichkeiten
- Fehlversuche außerhalb der regulären Dienstzeiten, verdichtet und in einer Einzelaufstellung