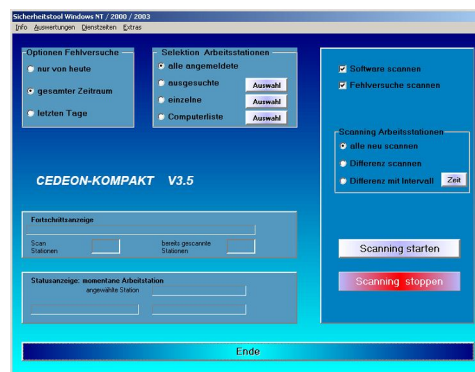


CEDEON Produktinformation

Vertrauen ist gut, **CEDEON** ist besser.

für Windows 2000/XP



Etliche weltweite Studien haben ergeben, dass die meisten Angriffe nicht von außen, z.B. übers Internet, sondern Netzintern erfolgen. CEDEON bietet zwei elementare wichtige Funktionen zur Unterstützung des IT-Sicherheitsmanagements.

1. Evtl. netzinterne Eindringversuche sind für den Administrator nur schwer erkennbar. Der Datenschutz verlangt verständlicherweise eine ständige Auswertung der System-Logfiles hinsichtlich Logon-Fehlversuche. In der Praxis ein kaum machbarer Aufwand. Eine Unterlassung wertet er dennoch als GROB FAHRLÄSSIG !
2. CEDEON scannt automatisiert von allen aktiven Arbeitsstationen die installierte Software. Mit diesem Tool erhalten Sie die Kontrolle, welche Software auf den einzelnen Arbeitsstationen installiert ist. Auf Grund der übersichtlichen Auswertungen entdecken Sie eventuelle unerwünschte Software sofort. CEDEON bietet Ihnen eine Unterstützung bei der Überwachung Ihrer Software – Lizenzen.

Sicherheitsmaßnahmen sind gefordert, um böse Überraschungen zu vermeiden.

CEDEON erfüllt diese Anforderung und wertet die Arbeitsstationen Ihres Windows - Netzwerkes automatisiert aus. Eine weitere wichtige Funktion der Auswertung aller Arbeitsstationen ist die Abschreckung, wenn bekannt wird, dass die Arbeitsstationen regelmässig auf Sicherheitsverletzungen ausgewertet werden. Sie reduzieren im erheblichen Maße evtl. stattfindende Eindringversuche, bzw. unerwünschte installierte Software. CEDEON unterstützt den Administrator beim IT-Sicherheitsmanagement und ist ein Sicherheitswerkzeug. Installieren Sie CEDEON auf Ihrem Arbeitsplatz und starten Sie einfach CEDEON im laufenden EDV-Betrieb. Fortschrittsanzeigen geben Ihnen Auskunft über die CEDEON – Aktivitäten und als Ergebnis erhalten Sie übersichtliche Berichte bzw. Auswertungen.

CEDEON

Installierte Software:

Unerwünschte installierte Software auf den Arbeitsstationen können eine Bedrohung für Ihr Netzwerk sein. Bedenkenlos wird oftmals von den Anwendern nur jede erdenkliche Software installiert und auch gestartet. Netzwerkprobleme sind die Folgen und Lizenzprobleme tun ihr Übriges. Sie können sich vor all diesen Beispielen nur schützen, indem Sie alle Arbeitsstationen einzeln und lokal durchsuchen, oder indem Sie einfach CEDEON einsetzen. CEDEON scannt automatisiert von allen aktiven Arbeitsstationen die installierte Software. Mit diesem Tool erhalten Sie die Kontrolle, welche Software auf den einzelnen Arbeitsstationen installiert ist. Auf Grund der übersichtlichen Auswertungen entdecken Sie eventuelle unerwünschte Software sofort. Außerdem bietet CEDEON Ihnen eine Unterstützung bei der Überwachung Ihrer Software – Lizenzen. Alle Informationen stehen Ihnen zusätzlich in verschiedene Dateien (Ascii Format) zur Verfügung. Eine Übernahme z.B. in diversen Datenbanken ist somit kein Problem.

Folgende Einstellungen sind bei CEDEON möglich:

Selektion der zu scannenden Arbeitsstationen einer Domäne:

- alle aktiven Arbeitsstationen
- ausgesuchte Arbeitsstationen
- eine gezielte Arbeitsstation

Folgende Auswertungen – Berichte stehen zur Verfügung:

- verdichtete Anzeige der gefundenen Software incl. der Anzahl
- Übersicht, auf welchen Arbeitstationen eine gesuchte Software installiert ist
- Übersicht, welche Software auf den einzelnen Arbeitsstationen installiert ist
- sofortige Lizenz-Überwachung
- Bereitstellung der Informationen in verschiedenen Ascii -Txt.Dateien

Logon – Fehlversuche:

Fehlgeschlagene Anmeldeversuche auf Administratoren bleiben grundsätzlich ohne Sanktionen. Das bedeutet, eine eingestellte Kontosperrung erfolgt auch nach den zulässigen Fehlversuchen nicht. Eine Prüfung der Ereignisprotolle aller Arbeitsstationen ist daher für die Sicherheit unerlässlich. Eine Netzwerküberwachung auf eventuelle Angriffe ist also nur möglich, wenn die Protokolle aller Arbeitsstationen lokal überprüft werden. In der Praxis dürfte dies kaum möglich sein und eventuelle Angriffe auf die Domäne sind für den Administrator daher nicht erkennbar. Hacker wissen das, der Datenschutz auch und wir ebenso. CEDEON zeigt Ihnen die verborgenen Fehlversuche auf Administratoren, oder andere wichtige Benutzer. CEDEON durchsucht alle Ereignisprotokolle jeder einzelnen Arbeitsstation innerhalb der Domäne auf misslungene Anmeldeversuche. Wenn CEDEON alle Arbeitsstationen gescannt hat, wird Ihnen das Ergebnis in komfortablen Auswertungen angezeigt. Neben verdichteten Daten stehen auch Einzelauswertungen zur Verfügung. Sämtliche Einzelauswertungen können ausgedruckt werden und sind somit dokumentiert.

Folgende Einstellungen sind bei CEDEON möglich:
Selektion der zu durchsuchenden Arbeitsstationen einer Domäne:

- alle aktiven Arbeitsstationen
- ausgesuchte Arbeitsstationen
- eine gezielte Arbeitsstation
- die lokale Arbeitsstation

Zeitliche Begrenzung der Ereignisse:

- keine Begrenzung
- nur heutige Ereignisse
- einstellbarer Zeitraum

Zusätzliche Optionen:

- fehlgeschlagene Anmeldeversuche ausserhalb der regulären Dienstzeit
- fehlgeschlagene Anmeldeversuche auf bestimmte User bzw. Administratoren

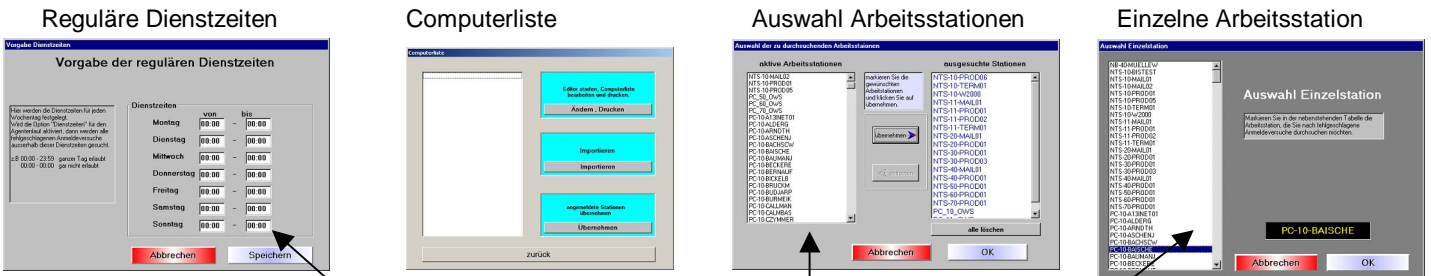
Folgende Auswertungen – Berichte stehen zur Verfügung:

- Gesamtergebnis mit Schnellübersicht
 - Verdichtung der Fehlversuche nach Arbeitsstationen
 - Verdichtung der Fehlversuche nach Benutzern
 - Einzelaufstellung der Anmelderfehlergebnisse mit verschiedenen Sortiermöglichkeiten
 - Fehlversuche ausserhalb der Dienstzeiten, verdichtet nach Arbeitsstationen
 - Fehlversuche ausserhalb der Dienstzeiten in einer Einzelaufstellung
 - Anmeldeversuche auf User/Administrator, sortierbar nach Namen und Arbeitsstationen.
 - Protokoll der gescannten Arbeitsstationen.
-

CEDEON

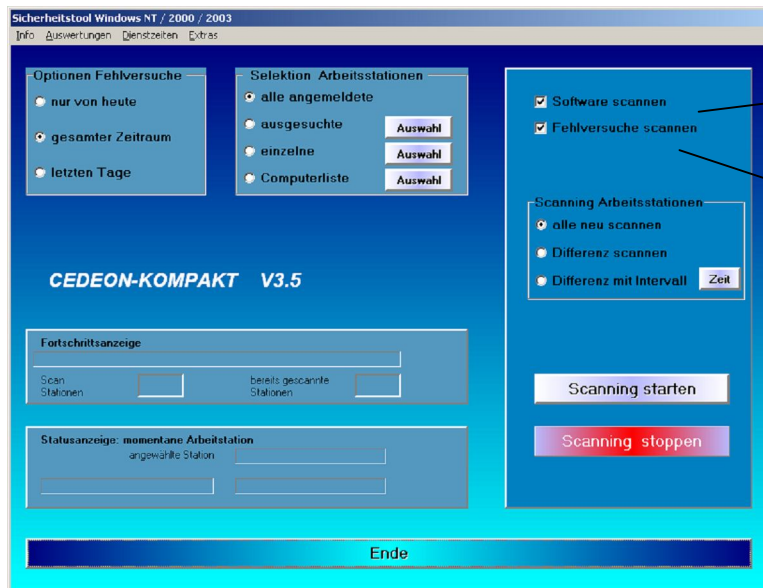
Netzwerktool Windows 2000 / 2003 / XP / Vista / Win 7

Vorgabemöglichkeiten für das Scanning



Folgende Einstellungen sind möglich:

scanning



Software
Wenn aktiviert, wird von allen Arbeitsstationen die installierte Software ausgelesen.

Logon
Wenn aktiviert, wird von allen Arbeitsstationen die misslungenen Logon-Versuche ausgewertet.

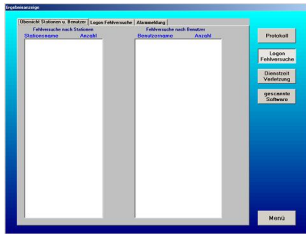
Selektion der Arbeitsstationen einer Domäne:
 ➤ alle angemeldeten Arbeitsstationen
 ➤ ausgesuchte Arbeitsstationen
 ➤ eine einzelne Arbeitsstation
 ➤ Computerliste

Zeitliche Begrenzung der Ereignisse:
 ➤ keine Begrenzung
 ➤ nur heutige Ereignisse
 ➤ einstellbarer Zeitraum

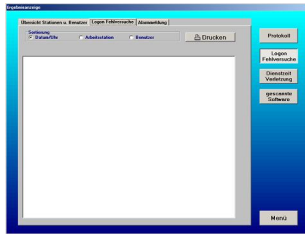
Zusätzliche Optionen:
 ➤ fehlgeschlagene Anmeldeversuche außerhalb der regulären Dienstzeit

Auswertungen - Berichte

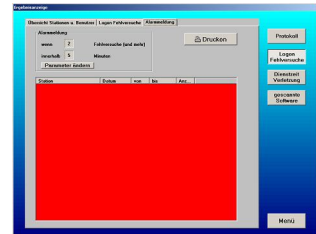
Fehlversuche Schnellüberblick



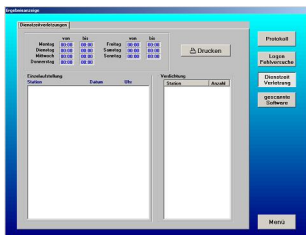
Fehlversuche im Detail



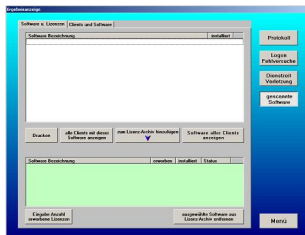
Alarmliste



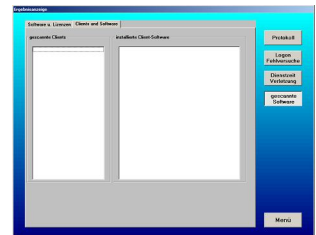
Dienstzeitverletzungen



gefundene Software



installierte Software der Arbeitsstationen



Folgende Auswertungen – Berichte stehen zur Verfügung:

Logon - Fehlversuche

- Verdichtung der Fehlversuche nach Arbeitsstationen
- Verdichtung der Fehlversuche nach Benutzern
- Einzelaufstellung der Anmeldefehlversuche mit verschiedenen Sortiermöglichkeiten
- Fehlversuche außerhalb der Dienstzeiten, verdichtet nach Arbeitsstationen
- Fehlversuche außerhalb der Dienstzeiten in einer Einzelaufstellung

Software Scan

- verdichtete Anzeige der gefundenen Software incl. der Anzahl
- Übersicht, auf welchen Arbeitsstationen eine gesuchte Software installiert ist
- Überblick, welche Software auf den einzelnen Arbeitsstationen installiert ist
- Unterstützung bei der Lizenz-Überwachung
- Bereitstellung der Informationen in verschiedene TXT.Dateien zum Export