digitronic

Secure Logon

Wissen und Besitz - 2 Faktoren für die sichere Anmeldung

Grundvoraussetzung für die Bereitstellung von digitalen Ressourcen und Anwendungen für autorisierte Benutzer, wie bspw. Mitarbeiter, sind Authentifizierungssysteme. Klassische Verfahren zur Identifizierung von Benutzern, wie Benutzername/Passwort-Kombinationen, sind aus Sicherheitsgründen in Unternehmen längst nicht mehr ausreichend.

Ein sehr hohes Sicherheitsniveau dagegen bieten Authentifizierungssysteme, die auf einem USB-Token oder einer Smartcard basieren. Derartige Lösungen setzen für eine erfolgreiche Anmeldung an einem System "Besitz und Wissen" voraus - den Besitz eines Hardwareschlüssels und das Wissen einer speziellen PIN. Nur wenn beide Faktoren vorhanden sind, kann sich ein Benutzer erfolgreich anmelden.

Sicherer Anmeldeprozess mittels USB-Token oder Smartcard

Zahlreiche Zusatzoptionen für individuelle Anforderungen

Secure Logon ermöglicht die sichere Anmeldung am Windows Betriebssystem mittels Authentifizierungstoken wie bspw. Smartcard, USB-Token, biometrischer Token oder Wechseldatenträger.

Hierbei werden die Windows-Anmeldedaten verschlüsselt auf dem Token hinterlegt. Erst nach Freischaltung dieses Tokens durch die Eingabe der korrekten PIN bzw. Erkennung eines registrierten Fingerabdrucks werden die Anmeldedaten vom Token gelesen und der Nutzer wird erfolgreich am System angemeldet.

Da der Benutzer weder Benutzernamen noch Passwort eingibt, diese ihm nicht einmal bekannt sein müssen, können die Zugangsdaten so komplex gewählt werden, dass sie möglichen Angriffen standhalten und damit die hohen Sicherheits-anforderungen in Unternehmen erfüllen.

Verlässt der Benutzer kurzfristig seinen Arbeitsplatz und zieht dabei seinen Token ab, wird dieser standardmäßig gesperrt. Eine Vielzahl von individuellen Einstellungen lässt aber auch andere Reaktionen wie Abmelden des Benutzers oder Herunterfahren der Arbeitsstation zu.

Weitere Zusatzoptionen erlauben die Deaktivierung der Standardanmeldung sowie eine Sperrung des Startens im abgesicherten Modus.

Secure Logon unterstützt für die sichere Anmeldung PKCS#11-fähige Token, biometrische Token und Wechseldatenträger verschiedenster Hersteller.

digitronic

Secure Logon

Betriebssysteme:
Microsoft Windows 2000/XP/ VISTA
Microsoft Windows Server 2000/2003

unterstützte Token:
Aladdin eToken®
StarSign Token
GemSafe Xpresso
MARX CrypToken
SafeNet iKey
Siemens SmartCard
Wechseldatenträger

Standard:
PKCS#11

Mit **Secure Logon** lassen sich nicht nur stationäre Arbeitsplätze innerhalb eines Unternehmens absichern, sondern auch mobile Geräte zum Schutz bei Diebstahl oder Verlust. Für den Einsatz ist weder eine Windows-Domäne noch eine aufwendige Public Key Infrastruktur (PKI) Voraussetzung.

Zentrale Administration

Über administrative Vorlagen für den Gruppenrichtlinieneditor oder die digitronic Managementkonsole kann zentral festgelegt werden, welche **Secure Logon-**Funktionen von wem und in welcher Weise genutzt werden können.

Bei Einsatz des *Token Management Systems* zur zentralen und komfortablen Verwaltung von Token lassen sich automatisch komplexe Passwörter für das Windows-Logon generieren, die sowohl im Benutzerkonto des Active Directory als auch verschlüsselt auf dem Token hinterlegt werden. Der Administrator kann so die Token bereits für das **Secure Logon** vorbereiten und an die Benutzer ausgeben, ohne dass ihnen das Windows-Passwort bekannt sein muss.

Weitere Informationen finden Sie unter **www.digitronic.net.**

digitronic ag
Oberfrohnaer Str. 62
D-09117 Chemnitz

Tel.: +49 (0) 371 81539 0
Fax: +49 (0) 371 81539 900
E-Mail: info@digitronic.net