Bild: istockphoto.com: Barış Muratoğlu

conpal AccessOn

Durchsetzung von Sicherheitsrichtlinien - durch Kontrolle von Ressourcen und Anwendungen

Die schnelle und unkomplizierte Einbindung und Wartung von unterschiedlichen Endgeräten in die IT-Infrastruktur, spielt zunehmend eine Schlüsselrolle für die Leistungsfähigkeit einer Organisation – mit vielen potentiellen Schwachpunkten: sensible Daten, die auf mobilen Endgeräten, Desktop PCs und Netzwerkservern gespeichert werden, erfordern einen sicheren Zugang, einen umfassenden Konfigurationsschutz sowie eine lückenlose Zugriffskontrolle. Sichere Authentisierung und Zugriffskontrolle zählen damit heute zu den wichtigsten Anforderungen der IT-Sicherheitspolitik eines Unternehmens. Dies umfasst, unter anderem, den kontrollierten Zugang zu Endgeräten, Dateien und dem Unternehmensnetzwerk, sowie den Schutz vor unerlaubter Installation von Hard- und Software. IT-Organisationen fordern hier eine Lösung, die eine einheitliche Sicherheitspolitik innerhalb der gesamten IT-Umgebung ermöglicht, ohne die Produktivität der Nutzer zu senken und die Administrationsaufwände nach oben zu treiben. *conpal* AccessOn erfüllt diese Kriterien. Ob der Endanwender mit dem PC, einem Notebook oder in einer Terminal-Server-Umgebung arbeitet – die Sicherheitsmodule von *conpal* AccessOn bieten einen zuverlässigen und kostengünstigen Weg für eine kontrollierte, sichere Arbeitsumgebung.

Das Produkt *conpal* AccessOn besteht aus drei Modulbausteinen mit folgender Funktionalität:

- Im Base-Modul werden die Funktionen für Administration und Protokollierung bereit gestellt. Das hier realisierte, intelligente Administrationskonzept versucht dabei die Aufwände für einen Administrator auf einem möglichst niedrigen Niveau zu halten.
- Das Modul Application Specific Access Rights (ASAR) erlaubt die filigrane Einstellung der Benutzerrechte in Bezug auf die Verwendung von Daten und Verzeichnissen durch Anwendungen. Anwendungen müssen dafür nicht angepasst werden. Auch Legacy Applikationen lassen sich so in einer sicheren Umgebung betreiben. Der Datenim- und Export werden auf einfache Art kontrolliert.
- Das Plug & Play Management Modul ermöglicht eine zentrale Verwaltung und Kontrolle aller Plug & Play Geräte in einem Unternehmen, einschließlich einer Remote-Freigabe Funktion, zur schnellen Reaktion auf „Ad-hoc“ Anpassungen in verteilten Umgebungen.

Über *conpal*

conpal ist spezialisiert auf das Management von Benutzerinfrastrukturen und die Entwicklung sicherer Systemumgebungen. Das Unternehmen bietet in diesem Kontext Lösungen zum Identity Management, zum Enterprise SSO, zur starken Authentisierung, sowie zur Kontrolle von IT-Infrastrukturen an. Unsere Lösungen sind einfach in bestehende Systemlandschaften zu integrieren und für den Anwender transparent. Unsere Kunden schätzen die Zuverlässigkeit und Einfachheit, sowie die langfristige Investitionssicherheit unserer Sicherheitslösungen. Wir stehen für anerkannte Produktqualität, Bedienerfreundlichkeit der Software, exzellenten Support und ein marktgerechtes Angebot.

conpal®
Information Security Systems.

Vorteile

Hohe Sicherheit

- Einfache Implementierung und Durchsetzung einheitlicher und durchgängiger Sicherheitsrichtlinien bei Nutzung unterschiedlicher Endgeräte
- Verbesserte Systemsicherheit und -stabilität durch Schutz vor unerlaubtem Installieren oder Ausführen von Programmen
- Schutz vor unberechtigtem Zugriff und Missbrauch
- Schutz gegen den Einsatz von unerlaubten Peripheriegeräten
- Schutz vor unbefugtem Im- und Export von Daten

Einfache Integration

- Nahtlosen Einbindung in bestehende Infrastrukturen wie z.B. Active Directory
- Schnelle Realisierung / Erstellung einer Policy durch mitgelieferte Rechteprofile
- Reduzierte Helpdeskkosten durch Wahrung der Systemintegrität und Sicherheit

Einfache Handhabung

- Kein Schulungsaufwand für Endanwender
- Schutz von Konfigurationen und Verzeichnisstrukturen steigert die Robustheit von Systemen, besonders bei mobilen Systemen
- Sichere Benutzerführung durch automatische Zuweisung von Ressourcen

Leistungsmerkmale

Basic Modul

- „Configuration Viewer“ bringt die Übersicht über die aktuellen Einstellungen für eine Revision

Plug & Play

- Kontrolle der Verwendung von Plug & Play-Geräten
- Verhinderung der Nutzung unbekannter Geräte sowie der Nutzung unbefugter Geräte bekannter Typen
- Plug & Play-Management verhindert, dass Daten und Anwendungen unerkannt in die IT-Infrastruktur eingebracht werden und somit die Stabilität der IT-Umgebung gefährden können
- “Enforced Drive Mapping” weist Speichergeräten automatisch vordefinierte Laufwerksbuchstaben zu
- Die Kontrolle erfolgt unabhängig vom Bus bzw. Protokoll
- Zentrale Administration des Moduls ermöglicht oder untersagt den Zugriff auf einzelne Plug & Play-Geräte oder ganze Geräteklassen
- Einfache Ausnahmenbehandlung: neue PnP Geräte können in der Administration durch Zugriff auf räumlich entfernte Arbeitsplätzen erlaubt werden
- durchgängige Zugriffskontrolle von der initialen Erkennung des USB-Devices bis zum Datenzugriff

Application Specific Access Rights (ASAR)

- Erweiterung der Zugriffsrechte des Dateisystems. Fügt die Ebene der Applikation zu den Zugriffsrechten hinzu. Es wird nur das Ausführen von definierten Applikationen erlaubt
- Administratoren können ein dreidimensionales Sicherheitskonzept mit ASAR umsetzen. Die Rechtevergabe kann nach Benutzern, Daten und Applikationen festgelegt werden
- Application Specific Access Rights erhöhen die Sicherheit durch Identifikation von Prozessen. Es werden keine Änderungen an den Applikationen nötig
- Sicherheit für alle Applikationen (auch Legacy-Anwendungen)
- Konfigurierbare Rechtevererbung für „Childprozesse“

System Administration

- Windows Installer (MSI) basierende Installation
- Konfiguration via Microsoft Management Console (MMC)
- Benötigt keine speziellen, zusätzlichen Server-Komponenten
- Policy-Verteilung durch
  - Active Directory oder kompatible Lösungen
  - Alternative Verteilungsmechanismen auf Basis von XML

Systemanforderungen

Betriebssysteme

- Microsoft Windows 7
- Microsoft Windows 8.1 (32/64 Bit)
- Microsoft Windows 10 (32/64 Bit)
- Microsoft Windows 2003 Server Standard Edition
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2

Netzwerk

- Alle Netzwerke, die von Windows unterstützt werden

Ergänzende Produkte

- *conpal* AuthomaticOn (SSO):
  Enterprise Single Sign-On zur automatisierten Anmeldung autorisierter Nutzer an unterschiedliche Plattformen und Applikationen
- *conpal* CerbalOn:
  starke Authentisierung mit Smartcards und USB Token. conpal CerbalOn ersetzt herkömmliche Windows-Passwörter durch zertifikatsbasierende Werte und schützt somit Anwender vor einer Kompromittierung ihrer Betriebssystempasswörter (keine Serverinfrastruktur erforderlich).

Drittthersteller

- Novell ZENWorks
- Citrix MetaFrame, inklusive Terminal Server
- VMware

Schnittstellen

- XML

Unterstützte Standards/Protokolle

- Active Directory
- MMC

Sprachversionen

- Englisch, Deutsch

Neue Funktionen

- PnP Wildcards
- Windows 10 Support
- Dateierkennung über Signaturen (Hashes)
- Eindeutige Applikationserkennung durch Prüfen von Hash-Signaturen

Kontakt

conpal GmbH
Dornhofstr. 67-69
63263 Neu-Isenburg
Deutschland
Telefon +49 (61 02) 75 198-0
Fax +49 (61 02) 75 198-99
info@conpal.de

www.conpal.de