

Starke Benutzerauthentifizierung im Unternehmensnetzwerk ohne teure Hardware

Was ist SAVERNOVA Network ID?

SAVERNOVA Network ID ist eine Client-Server Applikation, mit einer eigenen Management-Konsole. Die Konsole mit der dazugehörigen SQL Datenbank und einem Dienst, werden auf einem Windows Domain Controller installiert.

Die Benutzer werden aus dem Active Directory übernommen. In der Management Konsole bestimmt der Administrator den Sicherheitslevel von jedem Benutzer einzeln oder in Gruppen. Jeder aktive Benutzer wird zusammen mit seiner Passwortkarte und seiner geheimen Lesemethode verschlüsselt in der SQL Datenbank gespeichert. Im Active Directory werden diesbezüglich weder Informationen hinterlegt, noch wird das Active Directory erweitert.

Wie funktioniert's?

Schritt 1: Der Benutzer aktiviert seine unique Passwortkarte und wählt dabei seine geheime Lesemethode. Diese Benutzerdaten, sowie die virtuelle Kopie der Karte werden im SAVERNOVA Network ID verschlüsselt, dem Administrator unzugänglich, gespeichert.



Schritt 2: Bei jeder Anmeldung an das Netzwerk, wird dem Benutzer ein Startpunkt vorgegeben. Davon ausgehend muss er seine geheime Lesemethode auf der Passwortkarte anwenden. Sobald der Benutzer das Passwort vom angegebenen Startpunkt eintippt, ist das korrekte und einzig mögliche Passwort bereits im Active Directory hinterlegt, und der Benutzer wird angemeldet.

network ID

Server Komponenten (V. 3.0)

Administrations-Konsole

- Administrations-Tool für das Erstellen und Verwalten der Sicherheitsrichtlinien mit dem Einsatz der SAVERNOVA Passwortkarte
- Zuweisen dieser Richtlinien an unterschiedliche Benutzer und Gruppen, herausgelesen aus Active Directory
- Import, Übersicht und Verwaltung der virtuellen Karten
- Generelle Einstellungen der gesamten Software

Datenbank

- MS SQL Datenbank
- Speichert die einzelnen Einstellungen, und die Anwender-Profile mit aktiver Karte, Lesemethode und Anzahl der Startpunkte
- Alle Informationen sind verschlüsselt gespeichert

NIM-Service

- Kommunikation mit Datenbank und Active Directory
- Sendet auf Anfrage den Startpunkt an den Client mit installiertem SN-Gina

SN-Gina (Windows-Anmeldung)

- Ersetzt die normale Windows-Anmeldung
- Gibt bei der Benutzer-Anmeldung den Startpunkt zum Anwenden der Lesemethode vor
- Aktivierung der SAVERNOVA Passwortkarte und Erstellung des Benutzerprofils
- Zeigt dem Benutzer allgemeine Firmen- oder Administrator-Informationen bevor der Benutzer den Desktop erreicht

Funktionsweise des Programms

Nach der Installation der Server- und Client Komponenten wird die von SAVERNOVA mitgelieferte Karten-Datei in die Software eingespielt. Diese Datei enthält alle für die Lizenz verfügbaren SAVERNOVA-Passwortkarten.

Die Administrationskonsole bietet die Möglichkeit, einzelne Benutzer oder ganze Organisationsgruppen aus dem Active Directory für die Benutzung einer SAVERNOVA Passwortkarte zu aktivieren. Diese Benutzer werden dann einer Security Gruppe zugeteilt. In diesen Security Gruppen, kann man die verschiedenen SicherheitSAVERNOVAiveaus im Zusammenhang mit der Benutzung der SAVERNOVA Passwortkarte definieren.

(z.B. Bildschirmanzeige der Karte des Benutzers beim Anmeldevorgang oder Verwendung der ausgedruckten Karte; Anzahl möglicher Anmeldungen pro Benutzer und Karte; Gültigkeitsdauer einer Karte, etc.)

Sind all diese Einstellungen festgelegt, wird der Benutzer bei seiner ersten Anmeldung darauf hingewiesen, seine Karte zu aktivieren und eine geheime Lesemethode zu definieren.

Dies geschieht alles bei der Anmeldung an Windows. Nachdem dieser Vorgang abgeschlossen ist, erfolgt die Anmeldung an Windows, und der Benutzer erreicht seinen Desktop.

Ab diesem Zeitpunkt muss der Benutzer bei jeder Anmeldung seine Lesemethode an dem, bei der Anmeldung vorgegebenen Startpunkt auf seiner SAVERNOVA Passwortkarte anwenden, und das daraus resultierende Passwort eingeben.

Firmen schützen sich heute sehr gut gegen Gefahren von aussen. Dabei ist vielen gar nicht bewusst, dass rund 70% der Angriffe vom eigenen Personal erfolgt.

Kontakt

Savernova Ltd
info@savernova.com

Technische Beschreibung der Komponenten.

Administrations-Konsole

- Verwaltungskonsole für die Software
- Alle Informationen, Einstellungen, und virtuellen Karten werden aus der SQL Datenbank angezeigt
- In der Benutzerübersicht, findet nur ein visueller Import aus dem Active Directory statt

Datenbank:

- MS SQL Datenbank arbeitet mit SQL Server oder SQL Express
- Erst wenn ein Benutzer für das Verwenden der SAVERNOVA Passwortkarte aktiviert ist, wird dieser in der Datenbank registriert
- Karteninhalt und geheime Lesemethode der Benutzer werden verschlüsselt in der Datenbank hinterlegt
- Der Administrator hat keine Einsicht auf die Lesemethode

NIM-Service:

- Ein unter den Windows Diensten installierter Service.
- Muss auf einem Domaincontoller installiert sein
- Kommuniziert mit der SQL Datenbank. Sendet den Startpunkt an die anfragenden Clients
- Gleich das Passwort entsprechend dem angegebenen Startpunkt im Active Directory an

SN-Gina

- Wird auf Client's (Win 2000/XP pro) installiert
- Ändert die Windowsanmeldung auf dem Client
- Kommuniziert via SSL mit dem NIM Service auf dem Domain Controller