PROTECTSTAR™
AWARD
2008

Savernova

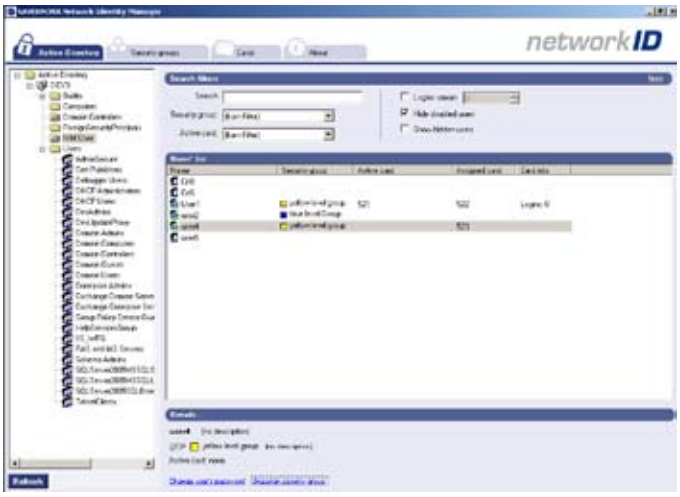
Network ID

EINLEITUNG

Die Schweizer Firma **Savernova** stellt Sicherheitslösungen für Privatanwender und Unternehmen her, die maximale Benutzerfreundlichkeit mit hoher Sicherheit und minimalen Kosten vereinen sollen. Im Jahr 2005 hat Savernova seine Kompetenzen mit der Passwort-Technologie CryptMe konsolidiert. Auf dieser Basis wurden seither mehrere Sicherheitslösungen entwickelt: Von der einfachen Passwortlösung bis hin zur umfassenden Benutzerauthentifizierung für lokale Netzwerke und Internet. Savernova verwendet die OTP (one-time-password) Technologie für höchsten Schutz mit nur einmal gültigen Passwörtern.

Eine sichere Authentifizierung ist laut Hersteller jederzeit garantiert, ohne dass sich der Anwender überhaupt ein Passwort merken muss. Nur eine einzige Lesemethode pro Anwender reicht. Damit ist Schluss mit vertraulichen Passwörtern auf Post-it Klebern, die am Bildschirm kleben oder an allen möglichen und unmöglichen Stellen am Arbeitsplatz versteckt werden. Gleichzeitig kann für Netzwerkadministratoren der Aufwand infolge vergessener Logins stark reduziert werden, da Benutzer sich leicht eine persönliche Lesemethode merken können.

Die Vorteile der Lösungen liegen auf der Hand: Unternehmen gehen nicht mehr das Risiko ein, dass Mitarbeiter am Arbeitsplatz die gleichen Passwörter verwenden wie zu Hause und somit deren Sicherheitsvorkehrungen



und Passwortpolicies unterlaufen. Auch kann gegen Angriffe von Innen ein wirksamer Riegel vorgeschoben werden. Dies ist mehr denn je entscheidend, werden doch über 70% der Angriffe auf Netzwerke durch eigene Mitarbeiter ausgeführt. Mit Savernova verfügen Unternehmen heute über sichere, kostengünstige und benutzerfreundliche Sicherheitslösungen. Aus diesen Gründen hat sich das **ProtectStar™ TestLab** entschieden, dass Flaggschiff des Unternehmens, **Savernova Network ID**, zu testen.

SICHERHEIT

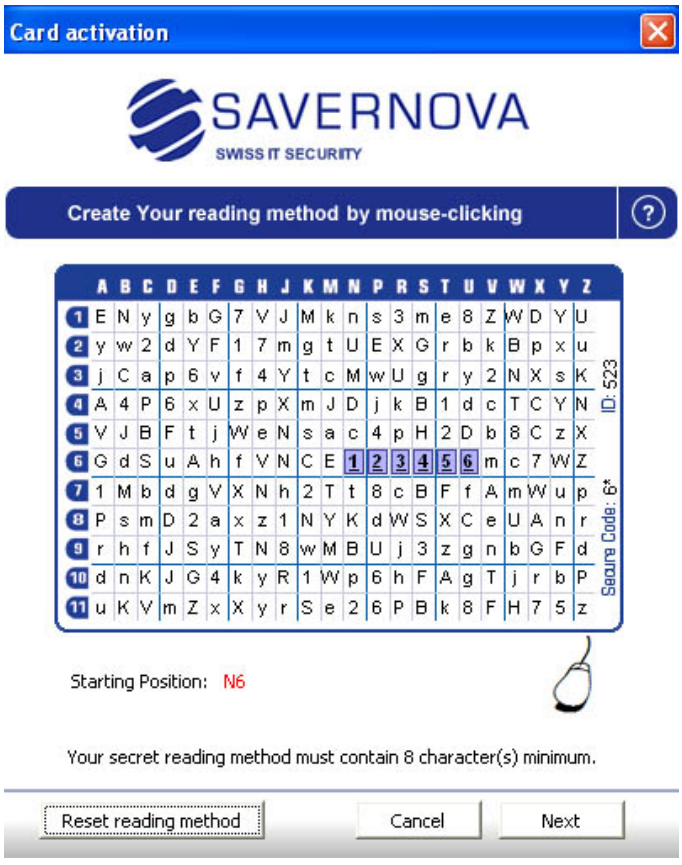
Savernova Network ID (zur Verfügung stand die aktuelle Version; Stand: November 2007) wurde sowohl unter **Laborbedingungen** als auch unter **realen Bedingungen** getestet.

Im Detail besteht **Savernova Network ID** aus den folgenden Server Komponenten:

1. Administrations-Konsole
2. MS SQL Datenbank
3. NIM-Service
4. SN-GINA

Die **Administrations-Konsole** dient dem Administrator, um beispielsweise Gruppenrichtlinien festzulegen, Savernova Passwortkarten zu erstellen und zu verwalten oder allgemeine Einstellungen der Softwarelösung vorzunehmen. Die **MS SQL Datenbank** speichert alle Informationen verschlüsselt ab. Zu diesen Informationen gehören beispielsweise die einzelnen Einstellungen, Anwender-Profile, Lesemethoden und Anzahl der Startpunkte Der **NIM-Service** stellt die Kommunikation zwischen der Datenbank und dem Active Directory sicher. Außerdem sendet er auf Anfrage den Startpunkt an den Client mit installierter SN-Gina. Die **SN-GINA** ersetzt die Windows Anmeldeoberfläche und gibt bei der User-Anmeldung den Startpunkt zum Anwender der Lesemethode vor. Sie kommuniziert via SSL mit dem NIM-Service auf dem Domain Controller. Zudem zeigt SN-GINA dem Benutzer allgemeine Firmen- oder Administrator-Informationen an noch bevor er den Desktop erreicht. Das Testszenario ist wie folgt aufgebaut worden: Serverseitig wurde als Basisbetriebssystem

Microsoft Windows 2003 Enterprise Server - auf Seiten des Clients, wurden aktuelle Computersysteme mit dem Basisbetriebssystem Windows XP Professional mit Service Pack 2 verwendet. Sowohl der Server als auch die einzelnen Clients wurden direkt über Crosskabel über das Netzwerk verbunden. Der Domaincontroller wurde serverseitig installiert und Benutzerkonten (testuser1, testuser2, usw.) sind für die Benutzer erstellt worden. Nach der Installation der Softwarelösung wurde die **Savernova Network ID** Lösung zunächst mit allen zum Testzeitpunkt bekannten **13.627** differenten **Angriffs- und Sicherheitstests** (Stand: November 2007) attackiert. Dabei konnten keine Anomalien oder Programmabstürze der Softwarelösung von Savernova festgestellt werden. Die Lösung hat die Testreihen erfolgreich bestanden. Getestet wurden hier die aktuell bekannten **Denial of Service** (DoS)-Angriffsarten, sowie die **Schwachstellen** in Betriebssystemen, Anwendungen, Brute Force, CGI abuses, Useless services, Backdoors und Sicherheitschecks.



Sowohl durch die **automatisch** ablaufenden Testreihen des hauseigenen **ProtectStar™ Security-Scanners**, der zusätzlich **9634** weitere Sicherheitstests und Angriffstaktiken auf die Softwarelösung **Savernova Network ID** ausführte, als auch durch die **manuell** durchgeführten Prüfungen wurden **keine** Schwachstellen oder Sicherheitsrisiken festgestellt. Als weiteres essentielles Testziel ging es darum, herauszufinden ob eine nicht-autorisierte Infiltration in das durch **Savernova Network ID** geschützte System möglich ist.

So wurde im Einzelnen folgendes analysiert: Bei den Sicherheitsüberprüfungen bezüglich der **Administrations-Konsole** ist beispielsweise geprüft worden, welche Auswirkungen es haben könnte, wenn ein Benutzer im ActiveDirectory deaktiviert wird. Hier zeigt sich eine Anomalie, denn obwohl auch der NIM-Service den Benutzer deaktivierte, wurde dem Benutzer dennoch die Passwortkarte beim Login angezeigt. Allerdings ist es nicht möglich gewesen, sich in das System als deaktivierter User einzuloggen.

Als weiterer Test sind für den „testuser" zwei Passwordkarten erstellt worden. Die Anzahl der maximalen Logins wurde vom Administrator auf fünf festgesetzt. Der „testuser" loggte sich fünf Mal ein. Danach wurde die Anzahl der maximalen Logins auf drei User zurückgesetzt. Hier stellten die Sicherheitsexperten von **ProtectStar™** fest, dass als sich der „testuser" bei diesem Szenario versucht hat einzuloggen, ihm die Passwortkarte angezeigt wurde. Nach Eingabe des korrekten Passworts wurde dann – ohne irgendeine Nachricht – die zweite Passwortkarte initialisiert. Über diese beiden genannten **Anomalien**, welche jedoch kein Sicherheitsrisiko darstellen, haben wir den Hersteller Savernova informiert. Dort arbeitet man aktuell an einem Update, dass diese Ungereimtheiten beheben sollte.Alle weiteren Testreihen im Bezug auf die Administrations-Konsole von Savernova Network ID zeigten **durchwegs positive Resultate**. Es wurden **keine Sicherheitsrisiken** festgestellt.

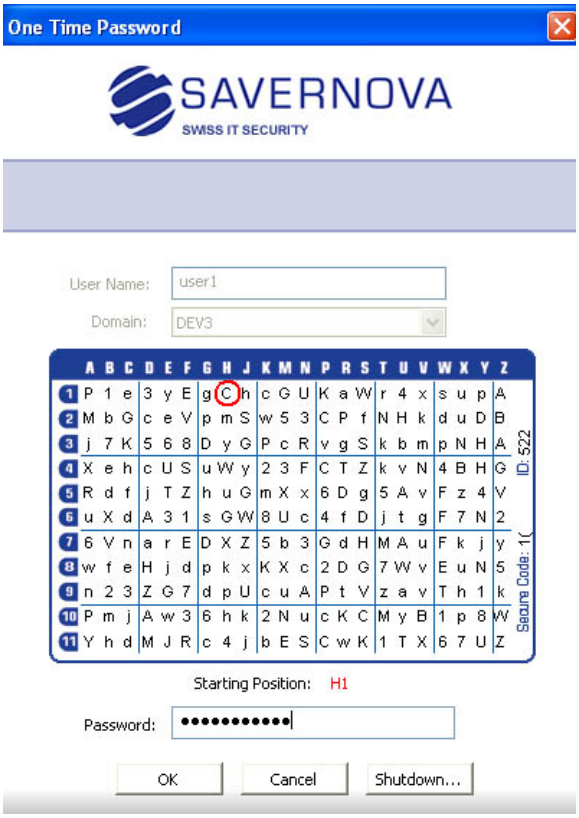
Für die weiteren Testanalysen wurde im nächsten Schritt die **SN-GINA** Anmeldekonsole überprüft: Zunächst wurde das Netzwerkkabel des Clientcomputers entfernt und es wurde versucht sich lokal am Computer als Domain

zu authentifizieren. In einem ergänzenden Test ist das Passwort der „testuser" grundsätzlich immer falsch eingegeben worden. Des Weiteren wurde umfassend der Initialisierungsprozess der **geheimen Lesemethode** (secret reading method) analysiert. Die Testreihen im Bezug auf die **SN-GINA** Anmeldekonsole von Savernova Network ID zeigten **durchwegs positive Resultate** und es konnten **keine Sicherheitsrisiken** festgestellt werden

Mit der sogenannten „**SQL Injection**" Methode versuchten die Sicherheitsexperten von ProtectStar™ nicht-autorisierten Zugriff auf die MS SQL Datenbank von Savernova zu erhalten. Mit dieser Methode kann das Ausnutzen von Sicherheitslücken im Zusammenhang mit SQL-Datenbanken, die durch mangelnde Maskierung oder Überprüfung von Metazeichen in der Benutzereingabe entstehen, getestet werden. So versuchten die Testpersonen von **ProtectStar™** eigene Datenbankbefehle einzuschleusen, um dadurch die Kontrolle über den Server zu erhalten. Im Allgemeinen wurden Befehle wie *SELECT * FROM users WHERE name = ," + username + „' and password = ," + password + „';"* usw. verwendet. Anstatt ein Passwort einzugeben, wurde versucht mit speziellen Befehlen eine SQL-Injektion durchzuführen. Zum Beispiel sind Befehle wie *, OR ,1' ='1* eingegeben worden, da so - in diesem „Stil" - der NIM-Service ein Passwort abfragt. Auch in diesem genannten Bereich der SQL-Datenbank zeigte Savernova Network ID **keine** Sicherheitsrisiken. Viele Web-Applikationen sind heutzutage mit SQL-Injection Attacken angreifbar. Die Architektur von **Savernova Network ID** bietet sicheren Schutz gegen diese Angriffe.

BENUTZERFREUNDLICHKEIT

Die Softwareauthentifizierungslösung **Savernova Network ID** ermöglicht Anwendern eine starke Benutzerauthentifizierung im Unternehmensnetzwerk ohne dafür teure Hardware erwerben zu müssen. Die Lösung kann in einfachen Schritten eingesetzt werden, denn **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 bestehenden Benutzerkonten werden einfach 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 selbst werden diesbezüglich weder Informationen hinterlegt, noch wird das Active Directory erweitert.

Passwort-Richtlinien werden umfassend in Savernova Produkten umgesetzt. Für Netzwerkadministratoren wie auch Anwender besticht die Savernova Technologie durch die Einfachheit und Benutzerfreundlichkeit. Mit **Savernova Network ID** wird das Windows Login durch eine **virtuelle Passwortkarte** ersetzt. Auf dieser Karte definiert der Benutzer seinen persönlichen Leseweg. Beim täglichen Login wird jeweils ein neuer Startpunkt auf der Karte vorgegeben. Von hier aus klickt der Benutzer einfach seinen Leseweg an und schon ist das Login eingegeben.

Anstelle einer umständlichen Buchstaben- und Zahlenkombination muss sich der Benutzer einzig an den immer gleichen Leseweg erinnern. Dies ist wesentlich leichter. Der jeweils wechselnde Startpunkt ermöglicht zudem ein täglich neues Passwort (one-time-password), das alle wichtigen Sicherheitsmerkmale aufweist. Manuell erstellte, komplizierte Passwörter gehören somit der Vergangenheit an. Zur Verwaltung des Savernova Network ID, wird auf einem Domain Controller im Netzwerk die **Administrationskonsole** und die Datenbank installiert. Diese Applikation kommuniziert mit dem Windows Login Client und sendet bei jeder Anmeldung den Startpunkt für die Lesemethode an den Client.

Durch die Kommunikation mit dem **Active Directory**, müssen Benutzer nicht neu angelegt, sondern nur für die Benutzung von Savernova Network ID mit der Passwortkarte berechtigt werden. Von der zentralen Verwaltung aus verteilt dann der Administrator die virtuellen Karten manuell oder automatisch an die einzelnen Benutzer. **Individuelle Sicherheitslevel** für den Anmeldevorgang lassen sich leicht einstellen, indem optionale Sicherheitsmerkmale definiert werden. Z.B. wie oft sich ein Benutzer mit der gleichen Savernova Passwortkarte anmelden darf oder ob ihm beim Anmeldevorgang die Karte am Bildschirm gezeigt wird. Falls die Karte nicht am Bildschirm angezeigt wird, muss mit einer ausgedruckten Savernova Passwortkarte das Passwort vom vorgegebenen Startpunkt und mit seiner Lesemethode abgelesen und eingeben werden.

Jede Savernova Passwortkarte verfügt über eine einzigartige Buchstaben- und Zahlenanordnung. Die Karten werden von Savernova erstellt und in verschlüsselter Form an Kunden gesandt. In der Administrationskonsole hat der Administrator den Überblick über die Anzahl und die ID der Karten. Er kann sehen, welche Karten in Gebrauch, verbraucht und noch frei sind. Über eine Druckfunktion, können eine oder mehrere Karten auf angepasste Vorlagen gedruckt werden. Wenn fast alle Savernova Passwortkarten schon verwendet wurden, können neue Karten angefordert werden.

Bei einzelnen Unternehmen wird bis zu 50% der Zeit der Netzwerkadministratoren für Benutzeranfragen betreffend vergessenen Passwörtern in Anspruch genommen. Mit der Savernova Lösung kann dieser Aufwand reduziert werden, denn Benutzer können sich leicht an den immer gleichen Leseweg erinnern. Falls der Leseweg einmal vergessen werden sollte, verschickt der Administrator eine neue Karte und der Benutzer definiert erneut eine persönliche Lesemethode.

PERFORMANCE

Der Hersteller Savernova gibt als Mindestvoraussetzungen für die Software keine Angaben bezüglich der benötigten CPU und Hauptspeicher an. Lediglich technische Voraussetzungen müssen erfüllt werden, um Savernova Network ID verwenden zu können. So sollte ein Server mit Windows 2000/2003 Server mit aktivem Active Directory bereitstehen. In unseren Testreihen wurden Computersysteme mit einer Leistung von 1.2 – 3.2 GHz und 512 – 4096MB Hauptspeicher eingesetzt, auf denen die Softwarelösung Savernova Network ID problemlos und ohne Leistungseinschränkungen eingesetzt werden konnte. Überhaupt arbeitete die Software ohne Schwierigkeiten, Systemabstürze oder anderen Anomalien – selbst während der Penetrationstestphase.

SUPPORT

Interessenten, die sich für Savernova Network ID entscheiden, erhalten im ersten Jahr kostenlosen Support, Updates und Patches inklusive. Support kann via E-Mail oder telefonisch in Anspruch genommen werden. Ab dem zweiten Jahr kann der Support (inkl. Upgrade und virtuellen Karten) optional gekauft werden. In diesem Fall wird eine Support-Gebühr in Höhe von 15% des ursprünglichen Kaufpreises fällig – Minimum jedoch EUR 300.00. Anwender, die ab dem Folgejahr keinen Support in Anspruch nehmen möchten haben dann die Möglichkeit sich ohne einen Maintenance-Vertrag an eine kostenpflichtige Telefonnummer an Savernova zu wenden. Abgerechnet wird dann im Minutentakt.

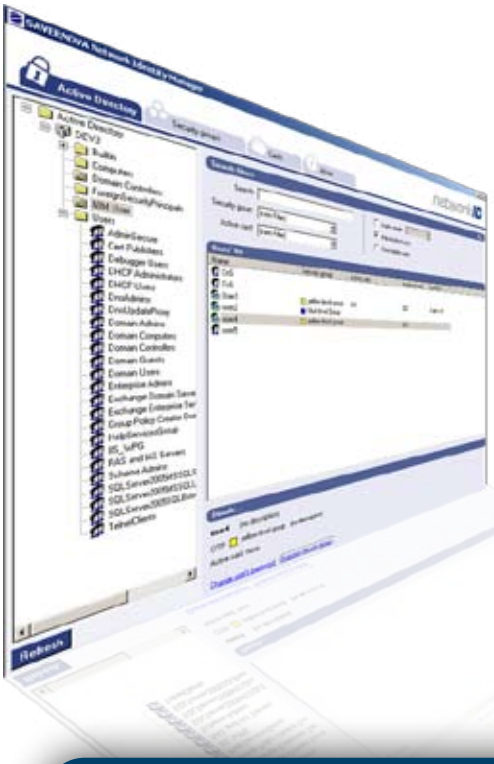
PREIS / LEISTUNG

Gegenüber einer herkömmlichen Authentifizierungslösung, welche mit Security Token oder anderer Hardware arbeiten, weist die Savernova Technologie einen markanten Preisvorteil von bis zu 80% auf. Bei der Savernova Network ID, eine reine Softwarelösung, fallen zudem keine Kosten für den Unterhalt der Hardware an (bspw. Batterie für Token). Auch im Vergleich zu individuellen Passwortpolicies ist die Savernova Lösung günstiger, denn der Produktivitätsverlust und der Aufwand für Netzwerkadministratoren infolge vergessener Passwörter kann stark reduziert werden. Savernova Network ID ist ab einem Preis von **EUR 28.40 pro Enduser und Jahr** erhältlich. Bei kleineren Unternehmen bis zu 49 Benutzern sind EUR 31,50 pro Enduser fällig. Das Software Development Kit basiert auf Java oder PHP und wird von Savernova kostenlos bereitgestellt. Dies ermöglicht Unternehmen, die Savernova Technologien in eigenen Lösungen einzusetzen. Unternehmen, die auf die virtuelle Passwortkarte verzichten möchten, stellt Savernova optional Passwortkarten aus Papier oder PVC preiswert ab EUR 185.00 für 500 Passwortkarten zur Verfügung. Auf Wunsch auch mit eigenem Firmenlogo.

FAZIT

Die Testreihen haben deutlich gezeigt, dass **Savernova** mit seiner softwarebasierten Sicherheitslösung **Savernova Network ID** eine Vielzahl an positiven Verbesserungen gegenüber ähnlicher Konkurrenzprodukte besitzt, die vor allem hardwarebasiert sind. Die Lösung von Savernova ist auf der einen Seite problemlos für Benutzer und Administrator eines Firmennetzwerkes einfach einzusetzen und anzuwenden, und auf der anderen Seite besticht Savernova Network ID durch ein ausgezeichnetes Preis- und Leistungsverhältnis. Hervorzuheben sind neben der innovativen Techniken und der angenehmen Benutzerfreundlichkeit, der sehr gute Grundschutz und die hohe Zuverlässigkeit des Produktes. Privatanwender, welche die Savernova Passwortkarten für den Heimcomputer anwenden möchten, bietet Savernova über die Webseite www.secureloginmypc.com eine kostenlose Lösung an.

Savernova Network ID von **Savernova** wird aufgrund der durchwegs sehr guten Testergebnisse mit dem „**ProtectStar™ AWARD 2008**“ ausgezeichnet.



PROTECTSTAR™ Inc.

1901 60th Place
Suite L 3604
Bradenton, FL
34203 USA
http://www.protectstar.com
testcenter@protectstar.com