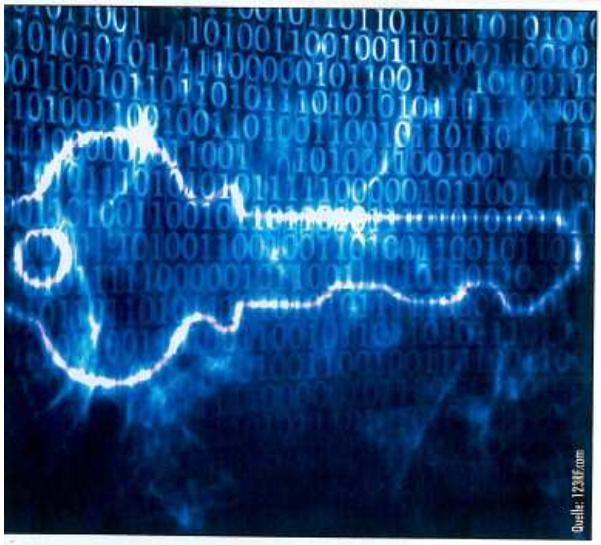
IT administrator
Das Magazin für professionelle System- und Netzwerkadministration
Ausgabe: 09/2011 Auflage: 10.144

Im Test: SecurEnvoy SecurAccess 5.4

Digitaler Passierschein

von Jürgen Heyer


Quelle: 123RF.com

Statt eine Zwei-Faktor-Authentisierung durch einen eigenen Token zu realisieren, bedient sich SecurEnvoy eines weit verbreiteten elektronischen Begleiters: des Mobiltelefons. Der Zugriff auf gesicherte Webinhalte oder Remotezugänge gelingt dann nur per Benutzeranmeldung und der zusätzlichen Eingabe eines Passcodes, der zuvor per SMS versandt wurde. IT-Administrator wollte wissen, wie praktikabel dieses Vorgehen im täglichen Umgang ist.

Die Idee von SecurEnvoy, das Mobiltelefon zur Übertragung von Schlüsseln (Passcodes) per SMS für die Anmeldung zu verwenden, geht von der berechtigten Annahme aus, dass sich das Handy zum ständigen Begleiter entwickelt hat. Warum also soll eine Firma seine Administratoren oder auch sonstige betroffene Mitarbeiter zur Realisierung einer sicheren Zwei-Faktor-Authentisierung mit eigenen Smartcards oder anderen USB-Token ausstatten, auf die sie zusätzlich aufpassen müssen? Dass jeder auch auf das Handy achtgeben muss, ist selbstverständlich, wobei jemand dessen Verlust vermutlich eher bemerkt als den eines kleinen USB-Sticks.

Die grundsätzliche Idee der Passcode-Übertragung per SMS hat SecurEnvoy mit verschiedenen Zugangsszenarien kombiniert, die letztendlich auch in unterschiedlichen Produkten münden. Dies sind SecurAccess für den Remotezugriff sowie den Zugriff auf Webdienste, SecurICE für den sicheren Zugriff in Notfällen, SecurPassword zur Implementierung eines Self-Service zum Zurücksetzen von Passwörtern und SecurMail zur sicheren Mailübertragung.

Genauer betrachtet haben wir SecurAccess, das letztendlich das größte Einsatzspektrum bietet, und für das laut Hersteller die größte Nachfrage herrscht. Hinsichtlich der Vorgehensweise interessierte uns sehr die Praktikabilität im täglichen Umgang, da hiervon die Akzeptanz entscheidend mitbestimmt wird. Wer SecurAccess selbst testen will, kann sich eine voll funktionsfähige Trialversion mit 30 Tagen Laufzeit herunterladen. Diese umfasst auch 100 Frei-SMS über einen der empfohlenen Provider, so dass der gesamte Ablauf komplett durchgespielt werden kann.

Einrichtung mit viel Handarbeit

Alle genannten Produkte von SecurEnvoy nutzen als Kernstück den so genannten Security Server, der eine Benutzerauthentisierung durchführt und den SMS-Versand steuert. Im Falle von SecurAccess wird auf den Endsystemen, die der Anwender eigentlich erreichen will, außerdem ein Agent installiert, der eine zusätzliche Anmeldemaske zwischenschaltet. Der Agent kontaktiert bei einem Login den Security Server, prüft die Anmeldedaten sowie einen per SMS übermittelten Passcode gegen und leitet den Anwender erst dann zur Applikation beziehungsweise zum gewünschten Dienst weiter oder verweigert den Zugriff.

Da bei einem Ausfall des Security Servers ein Zugriff auf alle derart geschützten Dienste nicht mehr möglich ist, ist es in einer produktiven Umgebung unbedingt erforderlich, mit zwei derartigen Servern zu arbeiten, die sich abgleichen. Der Installationsprozess sieht daher vor, entweder einen ersten Server oder einen zweiten zur Replizierung zu installieren.

Vor der Einrichtung des Security Servers sind die Installationsvoraussetzungen genauestens zu beachten. So werden das .Net-Framework 3.5 und der IIS-Webserver benötigt. Außerdem ist darauf zu achten, dass die Firewall-Regeln die angegebenen Ports nicht blockieren. Gut ist, dass das Setup eventuell fehlende IIS-Module automatisch nachinstalliert, sofern der IIS an sich eingerichtet ist. Wird der Security Server nicht auf einem englischen Betriebssystem installiert, ist darauf zu ach-

Systemvoraussetzungen

Security Server: Windows 2003 SP1 oder höher (32/64 Bit), Windows 2008 (32/64 Bit), Windows 2008 R2, installierter IIS, .NET 3.5

Für eine integrierte Benutzerverwaltung wird der Zugriff auf einen LDAP-basierten Verzeichnisdienst benötigt (MS Active Directory, Novell eDirectory, Sun Directory oder Open LDAP)

iT administrator
Das Magazin für professionelle System- und Netzwerkadministration
Ausgabe: 09/2011 Auflage: 10.144

ten, dass die drei Gruppen "Administrators", "Guests" und "Authenticated Users" vorher angelegt werden sowie mit den entsprechenden Benutzern der deutschnamigen Gruppen befüllt sind. Die Gruppenbezeichnungen sind fest im Programmcode hinterlegt, so dass die Software mit den deutschen Gruppennamen nichts anfangen kann. Der Hinweis auf diese Besonderheit ist an mehreren Stellen zu finden, allerdings fiel uns auf, dass der Inhalt nicht immer identisch war. So war teilweise nur ein Hinweis auf zwei der drei benötigten Gruppen zu finden.

Nach der Installation startete der erweiterte Konfigurationsassistent, der uns zunächst nach dem genutzten Webserver und den LDAP-Einstellungen für die Benutzerverwaltung fragte. SecureEnvoy unterstützt MS Active Directory, OpenLDAP, Novell eDirectory und den Sun Directory Server, so dass eine breite Einsetzbarkeit gegeben ist. Außerdem kann SecurEnvoy auf einer eigenen Benutzerverwaltung auf Basis von MS ADAM aufsetzen. Dies ist notwendig, wenn kein externer LDAP-Dienst zur Verfügung steht, kann aber auch als getrennte Benutzerverwaltung neben einem eigenen Verzeichnisdienst sinnvoll sein, wenn beispielsweise externe Anwender zu berechtigen sind, die aber nicht im eigenen LDAP erfasst werden sollen. Vorteilhaft ist, dass SecurEnvoy Multi-Domain-fähig ist und bei Bedarf auch gleichzeitig mit den oben aufgeführten LDAP-Diensten zusammenarbeitet.

Bei Nutzung von ADAM sieht das Setup vor, zu Redundanzzwecken zwei Server aufzusetzen und die Benutzerdatenbank zwischen diesen zu replizieren. Auch für einen Zugriff auf einen der genannten externen LDAP-Dienste kann der Administrator zur Redundanz jeweils zwei Directory-Server eintragen. Gefallen hat uns die integrierte Testmöglichkeit, ob die eingetragenen Zugriffsdaten passen.

Für den Versand der SMS unterstützt SecurEnvoy entweder die Verwendung eines eigenen SMS-Gateways oder die Nutzung eines SMS-Gateway-Providers, von denen mehrere im Internet ihre Dienste anbieten. Im Administrationshandbuch sind sowohl einige SMS-Gateways als auch eine

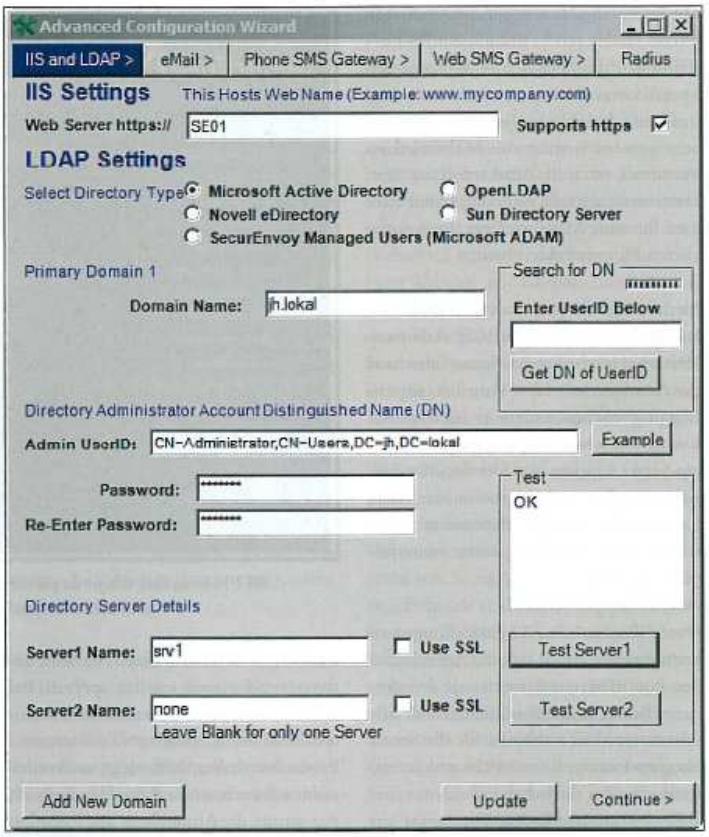


Bild 1: Der Security Server arbeitet bei Bedarf mit mehreren LDAP-Diensten gleichzeitig zusammen

Liste möglicher Provider aufgeführt. Bei den SMS-Gateways handelt es sich um Modems mit eigener SIM-Karte sowie Antenne, die teils seriell, teils per USB angeschlossen werden und die Kurzmeldungen wie ein Mobiltelefon verschicken. Abschließend ist im Assistent für SecureAccess der Radius-Server zu aktivieren, wodurch im Hintergrund der entsprechende Dienst eingerichtet wird. Der Administrator kann optional den Standard-Port 1812 ändern.

Statt die Passcodes per SMS zu versenden, unterstützt SecurEnvoy auch die Zustellung per E-Mail. Dann ist im Assistent auf dem E-Mail-Registerblatt ein SMTP-Server zu hinterlegen. Zu beachten ist, dass SecurEnvoy hier keine Authentisierung unterstützt, so dass eine direkte Weiterleitung an einen öffentlichen SMTP-Server meist nicht möglich ist. Hier empfiehlt es sich, ein SMTP-Gateway zwischenzuschalten, gegebenenfalls installiert auf dem gleichen System wie der Security Server selbst, das die E-Mails ohne Authentisierung annimmt und sich dann selbst zum Weiterreichen an den öffentlichen SMTP-Server dort anmeldet.

Module bedingen unübersichtliche Grundkonfiguration

Nach Abschluss des Assistenten starteten wir die Webkonsole des Security Servers, um dort weitere Einstellungen vorzunehmen. Diese Konsole erscheint vor allem anfangs etwas unübersichtlich, da hier alle Konfigurationen für die unterschiedlichen, eingangs erwähnten Module implementiert sind, SecurAccess aber nur ein Teil betrifft. So sind für die Einrichtung von SecurAccess letztendlich nur drei Registerblätter (Config, Radius und Users) abzuarbeiten.

iT administrator
Das Magazin für professionelle System- und Netzwerkadministration
Ausgabe: 09/2011 Auflage: 10.144

Unter "Config" findet der Administrator diverse Punkte für die grundlegenden Einstellungen des Security Servers wie die Sperre eines Benutzers nach einer bestimmten Anzahl von Fehlanmeldungen oder eine Validierung von Mobiltelefonnummern nach bestimmten Kriterien. Letzteres ist sinnvoll, wenn ein Unternehmen für seine Mobiltelefone einen dedizierten Nummernkreis besitzt.

Auch ließen sich hier andere Module wie SecurPassword und SecurICE aktivieren. Weiterhin ist die Lizenz einzuspielen und der Administrator kann Vorgaben für ein Logging machen, indem er Einträge ins Event-Log schreiben oder an einen Syslog-Server schicken lässt. Der Security Server unterstützt auch Migrationsszenarien, indem nicht gemanagte Benutzer an einen anderen Authentisierungsserver weitergegeben werden.

Unter "Radius" sind die Einstellungen zu konfigurieren, damit sich die Agenten auf den kontrollierten Servern mit dem Security Server abgleichen können. Der Administrator kann wahlweise für alle Server ein gemeinsames Passwort (Shared Secret) festlegen oder für jeden ein eigenes und außerdem diverse andere Parameter zur Authentisierung vorgeben. Auch eine Änderung des Standardports 1812 ist vorgesehen. Statt des in Secur-Envoy integrierten Radius-Dienstes kann alternativ ein externer Radius-Server verwendet werden wie beispielsweise der Cisco ACS Radius-Server.

Variable Konfiguration der Benutzer-Passcodes

Der wohl umfangreichste Punkt dürfte die Benutzerkonfiguration sein. Handelt es sich nur um einzelne Accounts, so kann diese gut hier erfolgen, andernfalls bieten sich die weiter unten beschriebenen Möglichkeiten zur Massenverteilung an.

Vorteilhaft ist, dass SecurEnvoy erforderliche Daten wie Mobilfunknummer und E-Mailadresse möglichst aus dem Verzeichnisdienst übernimmt, so dass diese hier nicht nochmals gepflegt werden müssen. Standardmäßig sind alle Benutzer als "Unmanaged" geführt, so dass sie bei SecurEnvoy keine Lizenz belegen. Der Administrator kann nun einen Account aktivieren oder auch explizit sperren. Bei einem gesperrten Account sind im Unterschied zu "Unmanaged" Daten zum Passcodeverhalten hinterlegt, es wurden eventuell auch schon Passcodes versandt, nur wurde die Anmeldung aus irgendeinem Grund gezielt deaktiviert.

Bild 2: Im Config-Menü erfolgen die globalen Einstellungen des Security Servers. Hier kann der Administrator unter anderem vorgeben, ob pro SMS ein oder gleich drei Passcodes übermittelt werden.

Der Security Server versendet die Passcodes standardmäßig per Handy, er kann diese aber alternativ auch per E-Mail verschicken. Um unterschiedliche Sicherheitsanforderungen abzudecken, lässt sich die Gültigkeitsdauer eines Passcodes vorgeben. Gefallen haben uns diesbezüglich die vielfältigen Möglichkeiten. Die beste Sicherheit bietet unbestritten der "One Time Code", der nur einmal verwendet werden kann. Das setzt aber voraus, dass für jede Anmeldung ein neuer Code benötigt wird. Aus diesem Grund lässt sich global für den ganzen Server einstellen, dass statt eines Codes stets drei verschickt werden. Die nächste Variante ist ein "Day Code", der eine vorgegebene Anzahl an Tagen gültig ist, wobei Samstag und Sonntag wahlweise mitgezählt werden.

Der "Tmp Static Code" ist für Benutzer gedacht, die ihr Handy verloren haben. Hier lässt sich ein fester, bis zu 14 Zeichen langer Code vorgeben, der eine bestimmte Anzahl an Tagen gültig ist. Anschließend wechselt die Software automatisch zum "One Time Code" oder zum "Day Code" zurück. Die letzte Variante "Static Code" ist für Benutzer ohne Mobiltelefon gedacht.

Auf den ersten Blick ungewöhnlich, aber durchaus sinnvoll ist der als Standard eingestellte Zeitpunkt, an dem die SMS versendet werden, denn SecurAccess arbeitet im so genannten Pre-Load-Verfahren. Das bedeutet, dass sofort nachdem ein "One Time Code" verbraucht oder ein "Day Code" abgelaufen ist, ein neuer verschickt wird. Ein Anwender erhält also den nächsten Code, den er irgendwann benötigt, schon rechtzeitig vorher. Das schützt vor Problemen und Verzögerungen, wenn beispielsweise am Einsatzort kein Empfang vorhanden ist oder auch in einem Rechenzentrum das Mobiltelefon gegebenenfalls nicht benutzt werden darf. Auf Wunsch lässt sich die Arbeitsweise von Pre-Load auf Real Time Passcodes umstellen. Indem der Anwender dann bei einer Anmeldung zuerst das Passcode-Feld freilässt, bekommt er prompt eine SMS mit dem Schlüssel zugesandt.

Statt sich mit Benutzerkennung, Windows-Passwort und Passcode anzumel-

iT administrator
Das Magazin für professionelle System- und Netzwerkadministration
Ausgabe: 09/2011 Auflage: 10.144

den, gibt es noch ein spezielles Verfahren, das so genannte "Integrated Desktop Management", das sich allerdings nicht mit dem "One Time Code" kombinieren lässt, sondern die Verwendung eines "Day Code" verlangt. Hier ändert SecurAccess das Windows-Passwort regelmäßig. Dieses setzt sich dann aus einem fixen Teil und einem Passcode zusammen. Der fixe Teil kann dabei vom Administrator oder vom Benutzer vorgegeben werden. Der Benutzer muss sich dann mit seiner Kennung und diesem zusammengesetzten Passwort anmelden. Um die Windows-Vorgaben hinsichtlich der Passwortstärke einzuhalten, kann der Administrator vorgeben, wie komplex der fixe Teil sein muss, da der Passcode selbst immer aus Zahlen besteht.

Clientkonfiguration im IIS-Manager

Auf allen Webservern und Systemen mit Remotezugriff, auf denen SecurAccess den Zugriff kontrollieren soll, ist ein Agent zu installieren, der mit dem Security Server kommuniziert und die Authentisierung durchführt. Voraussetzung ist hierbei ein installierter IIS. Für den Webserver sollte weiterhin SSL für eine sichere Kommunikation aktiviert sein. Außerdem sind wie bei den Security Servern die drei englischsprachigen Gruppen Administrators, Guests und Authenticated Users anzulegen, sofern nicht auf einem englischen Windows installiert wird. Wurden bei der IIS-Installation vom Client benötigte Module vergessen, so weist das Setup auch hier darauf hin und startet erfreulicherweise gleich deren Nachinstallation, so dass die Routine nicht verlassen werden muss.

Im Rahmen der Installation wurden zwei Security Server für die Clientverbindung abgefragt. Hier mussten wir deren IP-Adressen, das an den Servern konfigurierte Shared Secret und den zu verwendenden Radius-Port eingeben. Gut ist, dass der Administrator auch hier die Verbindung gleich testen kann. Ein Hinweis im Handbuch zu möglichen Fehlermeldungen hilft bei der Eingrenzung, wenn der Test fehlschlägt.

Die weitere Konfiguration erfolgte über den IIS-Manager, der um ein Plug-In erweitert wurde, so dass es dort auf allen relevanten Ansichten ein zusätzliches Icon "SecurEnvoy Two Factor Authentication" gibt. Indem der Administrator zuerst den physikalischen Server markiert und das Plug-In aufruft, kann er vertraute Netze oder auch einzelne Systeme eintragen, die keine Authentisierung benötigen. Weiterhin lässt sich hier ein Kommando (beispielsweise eine Abmeldesequenz) vorgeben, das beim Schließen des Browsers ausgeführt wird. Anschließend lassen sich entweder komplette Webseiten auf dem Webserver schützen oder aber innerhalb einer Webseite nur einzelne Bereiche, was natürlich entsprechend aufwändig ist, da dann alle virtuellen Verzeichnisse einzeln bearbeitet werden müssen. Ein typisches Beispiel für eine teilweise Absicherung wäre ein geschützter Zugang für eigene Servicemitarbeiter, während der Rest der Webseite öffentlich zugänglich bleibt.

Wie schon erwähnt lassen sich nicht nur Webseiten, sondern auch diverse Fernzugriffe mit SecurAccess kombinieren. Einige Beispiele sind Windows 2008 R2 mit Remote Desktop Web Gateway, Outlook Web Access, Citrix Secure Gateway Presentation Server und Astaro Security Gateway. Auf der Webseite von SecurEnvoy waren zum Testzeitpunkt 38 Integrationsanleitungen zu finden, die genau beschreiben, wie die Konfiguration in Verbindung mit diversen Remote Access Servern oder auch externen Radius-Servern zu erfolgen hat. Wir haben die Konfiguration an einem Beispiel für einen Windows 2008 R2 Server mit Remote Desktop Web Gateway durchgespielt und waren auf Anhieb erfolgreich. Die Beschreibungen sind mit Screenshots reich bebildert, so dass es keine Probleme geben sollte.

Bild 3: Über einen eigenständigen Verteilungs-Assistenten lassen sich viele Anwender gleichzeitig aus einem LDAP auslesen, analysieren und für die Nutzung von SecurAccess einrichten

Passcodes in Massen

SecurAccess berücksichtigt auch den Bedarf größerer Unternehmen, die gegebenenfalls eine Vielzahl an Anwendern für eine Nutzung vorbereiten müssen, und liefert einen Verteilungsassistenten mit. Am einfachsten klappt die Arbeit mit dem Assistenten, wenn Unternehmen einen der oben genannten LDAP-Verzeichnisdienste nutzten und darin auch die Mobilnummern der Anwender pflegen. Alternativ können Benutzer mittels einer Datei importiert werden. Ist LDAP angebunden, so ermittelt der Assistent noch nicht administrierte Benutzer, aktiviert diese für SecurAccess, sucht die Mobilnummern oder E-Mailadressen heraus und verschickt

IT administrator
Das Magazin für professionelle System- und Netzwerkadministration
Ausgabe: 09/2011 Auflage: 10.144

die erste Passcode-SMS. Auf diese Weise können neu hinzugekommene Benutzer jederzeit erfreulich einfach nachadministriert werden. Auch findet der Assistent nicht erfolgreiche Verteilungen, ermittelt die Anzahl der gemanagten Benutzer und kann ebenso das Management für mehrere Benutzer in einem Auftrag beenden. Insgesamt ist bei der Arbeit mit diesem Tool aber Vorsicht geboten, denn bei unachtsamer Bedienung können mit wenigen Klicks viele Benutzer umkonfiguriert werden und womöglich ihren Zugriff verlieren. Statt der Nutzung des Assistenten gibt es auch ein Kommandozeilentool, das eine weitere Automatisierung erlaubt. Die möglichen Parameter sind sehr detailliert beschrieben.

Wer die Funktionsweise und Konfigurationsmöglichkeiten von SecurAccess genauer betrachtet, erkennt schnell, dass der Hersteller alle Vorkehrungen getroffen hat, um einen redundanten Betrieb zu ermöglichen, vorausgesetzt, alles wird auch entsprechend umgesetzt. Dies ist wichtig, da sonst bei einem Ausfall alle geschützten Bereiche nicht mehr erreichbar sind. Bei der Installation gibt der Administrator vor, ob er den ersten Security Server oder einen zweiten zur Replizierung einrichten will. Zu beachten ist, dass alle Server mit der gleichen Konfigurationsdatei *config.db* arbeiten. Es ist daher sehr zu empfehlen, von dieser nach der Installation des ersten Servers eine Kopie an einem sicheren Ort zu speichern. Jeder Security Server wiederum kann sich zu zwei LDAP-Servern verbinden, damit auch hier Redundanz gegeben ist. Ebenso lassen sich bei jedem Agenten zwei Security Server angeben. Im Administrationshandbuch sind die entsprechenden Konfigurationsmöglichkeiten detailliert beschrieben.

Angemessenes Backup und Reporting

Behandelt wird im Handbuch auch das Thema Backup und Restore. Es empfiehlt sich, aus dem Installationsverzeichnis drei spezielle Dateien sowie das Unterverzeichnis "Data" zu sichern. Hier sind unter anderem die Radius-Konfiguration sowie die SMS-Warteschlange untergebracht. Sofern ein externer LDAP-Dienst genutzt wird, sind die Benutzerdaten inklusive der Telefonnummern dort gespeichert, so dass hierfür der dort eingerichtete Replizierungs- und Backupprozess verantwortlich ist. Wird stattdessen MS ADAM genutzt, sind die entsprechenden Verzeichnisse auf den Security Servern zu sichern.

Für eine Auswertung der Konfiguration des Security Servers wird ein einfacher Report-Assistent mitgeliefert. Dieser bietet vorgefertigte Abfragen, um beispielsweise alle gemanagten und (de)-aktivierten Benutzer aufzulisten. Weiterhin ist eine Auswertung nach Administrationsrechten möglich oder die Zuordnung zu verschiedenen Passcode-Verfahren. Auch kann sich der Administrator die Nutzer auflisten lassen, die sich in den letzten n Tagen angemeldet haben, oder diejenigen, die SecurAccess die letzten n Tage nicht genutzt haben. So lassen sich bei Bedarf Anwender herausfiltern, die den Dienst vielleicht nicht mehr benötigen. Für eine weitere Verwendung der Reports lassen sich die Ergebnisse in einer CSV-Datei speichern.

Fazit

SecurAccess von SecurEnvoy ist eine interessante Alternative zur Verwendung eines Tokens zur Zwei-Faktor-Authentisierung bei der Bereitstellung besonders gesicherter Zugänge für Webdienste und Remotezugriffe. Statt eines Tokens kommt das Mobiltelefon des Mitarbeiters zum Einsatz, an das im festgelegten Rhythmus zur Anmeldung benötigte Passcodes per SMS übertragen werden. Entsprechend der geforderten Sicherheit kann die IT mit nur einmal oder auch mehrere Tage gültigen Codes arbeiten. Durch die Übertragung der Passcodes rechtzeitig im Voraus verfügt der Anwender stets über den oder die nächsten benötigten Schlüssel. Dieser ist dann zusätzlich zur normalen Anmeldung mit Benutzerkennung und Passwort einzugeben. Statt dieses Pre-Load-Modus wird auch eine SMS-Zustellung in Real Time unterstützt.

Alternativ zur SMS-Übertragung ist auch eine Zustellung von Passcodes per E-Mail möglich, doch der Fokus liegt eindeutig auf der SMS-Nutzung. Insofern sollte im Vorfeld genau bewertet werden, ob das Verfahren tatsächlich praktikabel ist. Der SMS-Versand kann entweder über einen entsprechenden Anbieter im Internet oder über ein eigenes SMS-Modem erfolgen.

Etwas umständlich hat sich die Installation erwiesen, da auf nicht englischsprachigen Servern einige manuelle Nacharbeiten erforderlich sind. Allerdings sind dies einmalige Tätigkeiten, die die Anwender nicht betreffen. Gut gefallen haben uns die breite Verzeichnisdienstunterstützung sowie die Möglichkeit, den gesamten Betrieb redundant auszulegen so dass auch bei Ausfall eines Security Servers Anmeldungen weiterhin möglich sind. Eine umfassende Dokumentation zur Zusammenarbeit mit einer Vielzahl an Remote-Access-Lösungen erleichtert die Einrichtung. *(jp)*

Produkt
Programm zur Zwei-Faktor-Authentisierung beim Zugriff auf Webseiten und für Remote-Access-Lösungen.

Hersteller
SecurEnvoy
www.securenvoy.com

Preis
SecurAccess wird anhand der administrierten Benutzer lizenziert, wobei eine Staffelpreisliste zur Anwendung kommt. Bei 100 Lizenzen liegt der Preis bei rund 28 Euro pro Benutzer pro Jahr.

So urteilt IT-Administrator *(max. 10 Punkte)*

Grundkonfiguration	5
LDAP-Unterstützung	9
Administration vieler Nutzer	9
Redundanter Betrieb	9
Passcode-Verwaltung	8

Dieses Produkt eignet sich

optimal in Unternehmen, wo viele Anwender eine Zwei-Faktor-Authentisierung benötigen und die Nutzung des Mobiltelefons zur Schlüsselübertragung praktikabel erscheint.

bedingt bei Anwendern, die häufig in Rechenzentren oder vergleichbaren Lokalitäten arbeiten, in denen die Handynutzung untersagt ist. Hier dürfte sich der Prozess als zu umständlich erweisen.

nicht für Unternehmen, wo keine Zwei-Faktor-Authentisierung für Web- und Remotezugriffe benötigt wird.

SecurEnvoy SecurAccess 5.4