Mit virtuellen Smartcards die Unternehmenssicherheit erhöhen

Große wie auch kleine Unternehmen stehen heute vor der schwierigen Herausforderung, IT-Assets in einer scheinbar grenzenlosen Domäne schützen zu müssen. Das Identitäts- und Zugriffsmanagement wird dabei zu einem kritischen Aspekt der Verwaltung dieser Assets, da sich die Benutzer über eine Vielzahl mobiler und stationärer Geräte verbinden. Tagtäglich ereignen sich Sicherheitsverstöße, die dazu führen, dass Millionen von Benutzernamen, Passwörtern und damit verbundenen personenbezogenen Daten abgegriffen werden. Sind solche Daten für sich genommen schon wertvoll, werden sie von Kriminellen zusätzlich genutzt, um sich anderswo als die betroffenen Personen auszugeben, zum Beispiel auf Websites von Online-Händlern oder Banken. Multi-Faktor-Authentifizierung ist ein entscheidender Teil der Maßnahmen zum Schutz vor diesen laufenden Sicherheitsverletzungen.

Passwörter helfen nicht

Viele Anwender und Unternehmen halten ihre Benutzernamen und Passwörter nach wie vor für sicher – doch dieses Sicherheitsgefühl trügt. Phishing-Attacken werden immer ausgefeilter und gezielter, und kompromittierte Konten ermöglichen den Angreifern Zugang zum Netzwerk, wo sie weitere Identitäten sammeln und neue Konten einrichten können. Die IT-Abteilung im Unternehmen kann zwar Richtlinien für die Komplexität und häufige Änderung von Passwörtern durchsetzen. Doch können Benutzer diese Passwörter mehrfach vergeben oder auf öffentlichen Websites verwenden, auf denen die Sicherheitsmaßnahmen oft weniger strikt sind – und Angreifern damit weitere Möglichkeiten der Kompromittierung eröffnen. Und seit dem Einzug von Cloud Computing können sich Angreifer zudem online problemlos die nötige Rechenleistung für Brute-Force-Attacken verschaffen, um Passwörter zu knacken.

wave®

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung, die es in vielen verschiedenen Spielarten gibt, bietet erheblich größeren Schutz als die herkömmliche Passwort-Methode. Eine Multi-Faktor-Authentifizierung besteht aus mindestens zwei der folgenden Komponenten: „etwas, das man weiß“, „etwas, das man besitzt“ und „etwas, das man ist“. Ein Benutzername/Passwort für sich genommen ist „etwas, das man weiß“ und hat nur eine Dimension. Smartcards, Sicherheitstokens und Einmalpasswörter (OTPs) ermöglichen es, als zweiten Faktor etwas hinzuzufügen, „das man besitzt“, sodass ein Angreifer beide Komponenten überwinden muss, um sich Zugang zum Benutzerkonto seines Opfers zu verschaffen. Da sich der zweite Faktor im Besitz des Benutzers befindet, wird es wesentlich schwieriger, in den Account einzubrechen. Smartcards werden schon seit langem in vielen Behörden und großen Unternehmen verwendet und bieten einen zuverlässigen Mechanismus zur Zwei-Faktor-Authentifizierung, der allerdings hohe Kosten verursacht.

Herkömmliche Smartcards

Smartcards sind physische Authentifizierungsmittel, die das Passwort-Konzept verbessern: Um auf das System zugreifen zu können, muss der Benutzer nicht nur die PIN für die Smartcard kennen („etwas, das man weiß“), sondern die Smartcard auch tatsächlich bei sich haben („etwas, das man besitzt“). Drei Eigenschaften tragen dazu bei, die Sicherheit von Smartcards zu wahren:

Nicht-Exportierbarkeit: Die auf der Karte gespeicherten Informationen, wie etwa die privaten Schlüssel des Benutzers, können nicht exportiert und in einem anderen Medium verwendet werden.

Isolierte Kryptographie: Alle kryptographischen Operationen im Zusammenhang mit der Smartcard (wie etwa die sichere Verschlüsselung und Entschlüsselung der Daten) laufen direkt in einem Kryptoprozessor auf der Karte ab. Daher kann bösartige Software auf dem Host-Computer die Transaktionen nicht beobachten oder manipulieren.

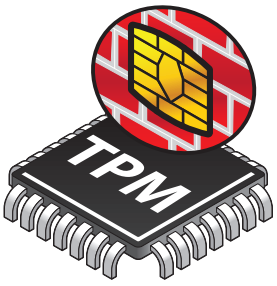
Anti-Hammering: Um Brute-Force-Zugriffe auf die Smartcard zu verhindern, sperrt sich die Karte nach einer Reihe erfolgloser PIN-Eingaben selbst. Diese Sperrung kann nur durch administrative Eingriffe aufgehoben werden.

Smartcards bieten erheblich mehr Sicherheit als Passwörter, da es für Unbefugte wesentlich schwieriger ist, in ein System einzudringen und sich dort einzunisten. Um Zugang zu einem System zu erhalten, das mit einer Smartcard geschützt ist, muss der Benutzer sowohl die gültige Karte besitzen als auch die PIN kennen, die den Zugriff auf diese Karte ermöglicht. An beides zu kommen ist für einen Dieb extrem schwierig. Dieser Sicherheitsansatz wird als Zwei-Faktor-Authentifizierung bezeichnet. Weiter erhöht wird die Sicherheit durch die Einzigartigkeit der Karte: Da nur ein Exemplar der Smartcard (und ihrer Inhalte) existiert, kann jeweils nur eine Person ihre Zugangsdaten verwenden, und der Benutzer wird den Verlust oder Diebstahl der Karte schnell bemerken. Dadurch ist das Risikofenster bei einem Diebstahl der Zugangsdaten deutlich kürzer als bei Passwörtern. Leider ist diese größere Sicherheit jedoch mit zusätzlichen Material- und Supportkosten verbunden. Herkömmliche Smartcards sind teuer (die Mitarbeiter müssen sowohl mit den Karten selbst als auch mit Lesegeräten versorgt werden). Zudem können Smartcards leicht vergessen, verlegt, gestohlen oder beschädigt werden oder aus anderen Gründen nicht zur Authentifizierung zur Verfügung stehen. In diesem Fall müssen sie zurückgezogen und ersetzt werden, was noch höhere Kosten pro Smartcard verursacht als die ursprüngliche Einführung. Die Betriebskosten und der Verwaltungsaufwand sind Hindernisse, die Unternehmen oft von der Implementierung abhalten.

Das TPM, oder Trusted Platform Module, hat viele Eigenschaften mit der physischen Smartcard gemeinsam. Die Standards für das TPM wurden von der Trusted Computing Group (TCG) entwickelt, einer Standardisierungsorganisation, die von führenden Technologieherstellern getragen wird. Auf nahezu allen professionellen Laptops und Desktops, die in den letzten sieben Jahren auf den Markt kamen, ist das TPM bereits installiert und somit auf Unternehmenscomputern in der Regel bereits vorhanden. Das TPM ist ein eingebetteter Sicherheitsprozessor, der manipulationssicheren Schutz und Krypto-Funktionen für das Betriebssystem und seine Anwendungen bietet. Es vereint folgende Funktionalitäten: RSA-Schlüsselgenerator und Kryptographie, Message Digest Generator, HMAC (Hashed Message Authentication Code), Zufallszahlengenerator (RNG), Protected Flash, NVRAM- und ROM-Speicher sowie Module (Zähler und Messung der Versorgungsspannung) zur Erkennung von Manipulationen. Die drei primären Funktionen einer physischen Smartcard (Nicht-Exportierbarkeit, isolierte Kryptographie und Anti-Hammering) werden alle auch vom TPM unterstützt.

Die Alternative: Virtuelle Smartcards

Die zentrale TPM Hardware-Technologie, die eine starke Authentifizierung und die Nutzung als virtuelle Smartcard (VSC) ermöglicht, existiert bereits seit einiger Zeit. Relativ neu ist dagegen der geschäftliche Fokus auf eine starke Authentifizierung und erhöhte Sicherheit. Einer der Hauptvorteile, die virtuelle Smartcards für ein wesentlich breiteres Publikum interessant machen als physische Smartcards, ist der Wegfall der Investitionskosten für die Hardware sowie der laufenden Wartungskosten.



In einem herkömmlichen Smartcard-Szenario muss ein Unternehmen, das diese Technologie implementieren möchte, sowohl Smartcards als auch Lesegeräte (bzw. Geräte mit eingebautem Smartcard-Reader) für alle Mitarbeiter anschaffen. Es gibt relativ preisgünstige Optionen für Smartcards, doch wenn die drei wesentlichen Sicherheitseigenschaften von Smartcards (insbesondere die Nicht-Exportierbarkeit) gewährleistet sein sollen, liegt der Preis höher. Virtuelle TPM-Smartcards lassen sich dagegen ohne zusätzliche Materialkosten einsetzen, sofern die Mitarbeiter über Computer mit eingebautem TPM verfügen, und diese sind auf dem Markt außerordentlich weit verbreitet.

Zudem sind die Wartungskosten virtueller Smartcards geringer als die ihrer konventionellen Pendants. Physische Smartcards können leicht verlorengehen, gestohlen werden oder verschleißen. Virtuelle TPM-Smartcards können dagegen nur verlorengehen oder beschädigt werden, wenn der Hostrechner verlorengeht oder beschädigt wird, was in der Regel wesentlich seltener geschieht. Rechnet man alle oben aufgeführten Kostenfaktoren ein, die bei virtuellen Smartcards im Gegensatz zu physischen Karten entfallen, so ist eine VSC typischerweise um mehr als 50% kostengünstiger. Dabei bietet sie die Sicherheit und die starke Authentifizierung, die ein Unternehmen benötigt.

Wo kann ich eine VSC einsetzen?

Die Faustregel lautet: Wo Sie eine physische Smartcard verwenden können, können Sie auch eine virtuelle Smartcard einsetzen. Sie bietet die gleichen Funktionen und nutzt den gleichen Smartcard-Betriebssystemtreiber. Virtuelle Smartcards können nicht nur für das Windows Smartcard Logon verwendet werden, sondern auch für andere Anwendungen wie Microsoft DirectAccess, VPN, Microsoft Office 365, Terminal Services, Netzwerkzugangskontrolle (NAC) mittels 802.1x, Wi-Fi-Authentifizierung und viele weitere. Wenn die Sicherheit, die das TPM bietet, mit einem zertifikatsbasierten Zugriff auf diese primären Geschäftsfunktionen kombiniert wird, liegt es auf der Hand, dass sich die Sicherheit der Workstation oder des virtuellen Terminals ganz erheblich erhöht.

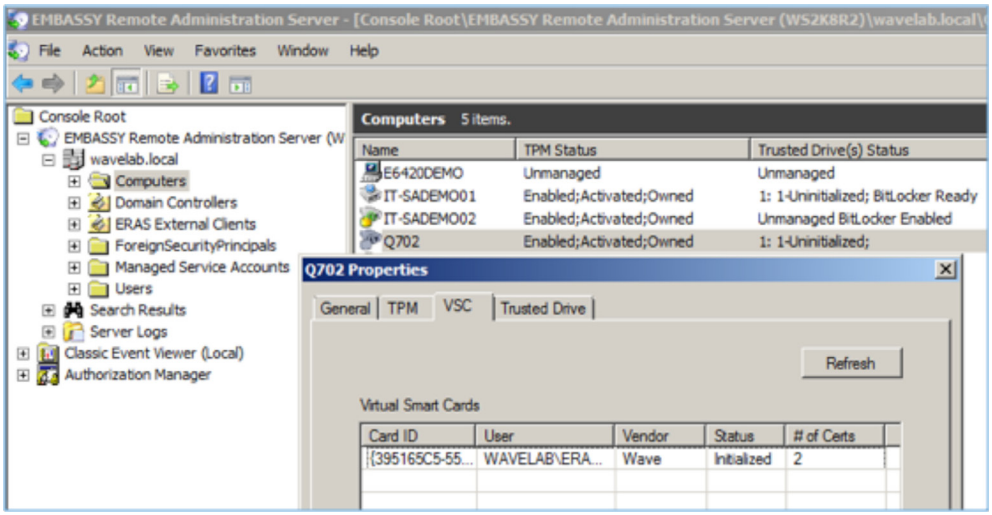
Einfache Bereitstellung

Die Bereitstellung virtueller Smartcards ist vergleichsweise einfach. Die aktuelle Wave Virtual Smart Card 2.0 bietet Unternehmenswerkzeuge für die Implementierung und das laufende Lebenszyklusmanagement der VSCs.

Der Lebenszyklus der Karte lässt sich in drei separate Abschnitte untergliedern:

Abschnitt	Schritte
Erstellung	• Die Verteilung der Wave Virtual Smart Card 2.0 kann mit der zugehörigen Verwaltungskonsole (ERAS), Domänenrichtlinien und dem Software-Verteilungssystem des Unternehmens vollständig automatisiert werden.
Benutzer-Login	• Nachdem die VSC erstellt wurde, loggt sich der Benutzer mit seiner Standard-Windows-Authentifizierung in seinen Account ein. • Wenn die automatische Zertifikatsregistrierung konfiguriert wurde, wird der Benutzer aufgefordert, ein VSC-Zertifikat zu registrieren; dazu muss er seine PIN eingeben. • Wurde die automatische Registrierung nicht konfiguriert, muss der Benutzer sein Zertifikat gemäß dem Standardverfahren registrieren, das das Unternehmen festgelegt hat. • Der Zertifikatsschlüssel wird im TPM erzeugt und kann nicht exportiert werden.
Verwendung der VSC	• Der Nutzer kann seine PIN leicht ändern, indem er die Tastenkombination Strg + Alt + Entf eingibt und Change Password -> Other Credentials auswählt. • Nach erfolgreicher Erstellung einer VSC kann diese zur Authentifizierung bei verschiedenen Programmen und Anwendungen eingesetzt werden, so etwa VPN, 802.1x und RDP. • Wenn die PIN zu oft falsch eingegeben wurde, wird die Smartcard gesperrt, und der Benutzer erhält einen Challenge-Code, den er beim Helpdesk angeben kann. Die IT-Mitarbeiter können ihm dann einen Antwortcode zur Verfügung stellen, den er eingeben kann, um seine PIN zu ändern und wieder Zugriff auf die Karte zu erhalten. • Die Wave VSC ermöglicht eine zentralisierte Verwaltung und Wiederherstellung. Der integrierte Challenge-Response-Wiederherstellungsmechanismus ist auch dann verfügbar, wenn der Computer des Benutzers offline ist (z.B. wenn das Passwort für ein VPN-Zertifikat vergessen wurde).

Ein Beispielszenario: Das Bereitstellungsteam eines Unternehmens legt zunächst den ersten Verwendungszweck und den Rollout-Plan fest. Nehmen wir an, das Team beschließt, die VSC für Windows Logon, DirectAccess und den Zugriff auf Office 365 zu verwenden. Mit der Management-Konsole von Wave EMBASSY Remote Administration Server (ERAS) und dem VSC Deployment-Tool wird die Agenten-Software auf den Zielrechnern verteilt. Mithilfe einer Zertifizierungsstelle werden dem Zertifikatsspeicher die System- und Benutzerzertifikate hinzugefügt. Weitere Fähigkeiten (z.B. Virtual Desktop) können im Lauf des IT-Lebenszyklus je nach Bedarf ergänzt werden.



Mit den verfügbaren automatisierten Deployment-Tools können IT-Abteilungen virtuelle Smartcards für ihre Anwender im gesamten Unternehmen schnell bereitstellen und einfach verwalten. Die Nutzung von Zertifikaten zur Authentifizierung erhöht die Sicherheit. Und noch wichtiger: Unternehmen, die sich vom reinen Passwortkonzept verabschieden, haben den zusätzlichen enormen Vorteil, dass die gesamte kryptographische Verarbeitung im TPM stattfindet, das für Einbrüche und Manipulationen weit weniger anfällig ist. Die wesentlichen Sicherheitskommandos werden nicht im Betriebssystem oder in der Haupt-CPU ausgeführt, die kompromittiert sein könnten.

Fazit

Virtuelle Smartcards bieten die gleiche Sicherheit wie die bewährten Sicherheitsprogramme mit physischen Smartcards. Sie nutzen Zertifikate zur Implementierung einer starken Zwei-Faktor-Authentifizierung. Mit dem Trusted Platform Module (TPM), das in mehr als 550 Millionen Geräten bereits eingebaut ist, steht Unternehmen eine chipbasierte Root-of-Trust zur Verfügung, die um zusätzliche Anwendungsfälle erweitert werden kann. VSCs und die zugehörigen Zertifikate sind flexibel und ermöglichen nicht nur Login, sondern auch anwendungsspezifische Sicherheit und lassen sich in bestehende PKI-Lösungen integrieren. Wenn Sie virtuelle Smartcards in ein umfassendes Sicherheitspaket einbinden, können Sie die Sicherheitsaufstellung Ihres Unternehmens erheblich verbessern – und das zu einem Bruchteil der Kosten, die andere Alternativen verursachen.

Für weitere Informationen wenden Sie sich bitte an Ihren zuständigen Wave-Mitarbeiter oder kontaktieren uns telefonisch unter (877) 228-WAVE.

wave®

Über Wave
Wave Systems Corp. (NASDAQ: WAVX) setzt im Inneren des Geräts an, um die Komplexität, die Kosten und die Unsicherheiten des Datenschutzes zu reduzieren. Dabei nutzt Wave die Hardware-Sicherheitsfunktionen, die direkt in die Rechnerplattform des Endpunkts integriert sind. Wave zählt zu den führenden Experten bei diesem wachsenden Trend und nimmt mit seinen First-to-Market-Lösungen eine Vorreiterrolle ein. Zugleich trägt Wave als Mitglied der Trusted Computing Group zur Gestaltung von Standards bei.

A4-DE-03-000405/ version 1.00 Release Date: Januar 28, 2015

Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238 USA
+1 (877) 228-WAVE • fax +1 (413) 243-0045
www.wave.com