PKI und Smart Card: Das sichere „Sesam, öffne dich!“

Mit Smart Cards komfortabel anmelden, mit PKI sicher verschlüsseln – das ist der ideale Einstieg in eine sichere Netzwerkinfrastruktur.

Wie mache ich mein Netzwerk sicher? Die Suche nach der richtigen Antwort beginnt bei der Netzwerkanmeldung, der ersten Herausforderung für Administratoren. Denn: Der Anwender identifiziert sich gegenüber dem Active Directory von Windows Server, das ihm die adäquaten Berechtigungen zuweist.

Einfach und unsicher: Hund, Katze, Lebensgefährte

Die Geschichte der Parolen und Geheimwörter – und deren Sicherheit – ist so alt wie die Menschheit. Doch während früher ein einfaches „Sesam, öffne dich!“ ausreichte, benötigt ein Anwender in der digitalen Welt gleich eine Vielzahl von Kennwörtern, Geheimzahlen und Persönlichen Identifikationsnummern (PINs). Um sich diese leichter merken zu können, greift er häufig zu Namen, Zeit- oder Ortsangaben. Doch schon simple Hacker-Programme hebeln solch einfache Kennwörter in kurzer Zeit aus und nutzen sie als Schlüssel für unliebsame Besuche in fremden Datenwelten. Ein Großteil der Hacker-Attacken richtet sich daher konsequenterweise gegen Benutzerkonten und Passwörter.

Komplex – aber trotzdem unsicher: p@ßß#w0erT-er

Kluge Netzwerkadministratoren schlossen dieses Einfallstor bislang durch klare und verbindliche Richtlinien für eine bessere Passwortqualität. Diese bestimmen die Mindestzeichenanzahl, die Verwendung von verschiedenen Zeichensätzen inklusive Sonderzeichen sowie einer Kennwortchronik, die verhindert, dass der Anwender nur zwischen wenigen Passwörtern wechselt. Sicherheitstechnisch sind solche Vorschriften zwar ein echter Zugewinn. Aber sie verleiten die Anwender auch dazu, die komplizierten Kennwörter zu notieren und an einer leicht zugänglichen Stelle abzulegen – ein für die Sicherheitsbemühungen kontraproduktives Verhalten.

Sicherheit[2]: Smart Cards – Besitz und Wissen

Fortschrittliche Administratoren setzen heute auf Smart Cards als sichere und komfortable Alternative zur herkömmlichen Anmeldung mit Anwendernamen und Passwort. Die hohe Sicherheit wird dabei durch verschiedene Faktoren erreicht:

- Die Smart Card etabliert ein zweistufiges Sicherheitssystem. Der Anwender muss die Karte „haben“ (Stufe I: Besitz) und die PIN für den Zugang zu den Karteninformationen kennen (Stufe II: Wissen). Der Verlust der Smart Card allein ist daher noch kein sicherheitstechnisches Problem. Dem gleichen Schutzmechanismus vertrauen wir übrigens auch unsere Geldbestände an: Denn auch die ec-Karten, als „Smart Cards“ für unsere Geldkonten, machen erst mit der richtigen PIN den Zugang frei.
- Administratoren speichern sensible Daten wie Schlüssel und Zertifikate direkt im Mikrochip der Smart Card.
- Mit Hilfe der Smart Card können Schlüssel und Zertifikate sicher transportiert werden, wenn sie beispielsweise für den mobilen Einsatz oder für den Heimarbeitsplatz benötigt werden.
- Administratoren können ihre alltägliche Arbeit mit einem normalen Benutzerkonto erledigen. Für spezielle sicherheitskritische Aufgaben melden sie sich per Smart Card an.

Windows und Smart Cards

Bereits Windows 2000 verwendet die PKI-Technologie und unterstützt, da die Treiber der wichtigsten Hersteller integriert sind, Smart Cards. Die PKI der Windows Server erzeugt und verwaltet die Schlüssel und Zertifikate, die für eine Smart-Card-Anmeldung erforderlich sind. Der Anmeldedialog von Windows unterstützt wahlweise die AA-Authentifizierung mit Anwendernamen und Passwort oder per Smart Card.

Windows XP und Windows Server 2003 arbeiten mit verfeinerter Technik, um den Umgang mit Smart Cards noch weiter zu vereinfachen und dadurch die Administrationskosten zu senken. Zudem ermöglicht die aktuelle Generation der Microsoft-Betriebssysteme den teilweise automatisierten Verteilungsprozess für Smart Cards.

Die Planungsphase

Die Public-Key- und Smart-Card-Technologie in den Windows-Betriebssystemen ist sehr einfach zu implementieren und zu nutzen. Trotzdem sollte besonders vor dem Aufbau der PKI eine sorgfältige Planung erfolgen. Die nachfolgende Checkliste hilft dabei:

- **Verwendungszweck(e) der PKI definieren**

Eine Infrastruktur öffentlicher Schlüssel wird für viele Aufgaben genutzt. Ein Unternehmen sollte daher bereits in der Planungsphase den – auch zukünftigen – Einsatzzweck der PKI genau prüfen. Er bestimmt das grundlegende Design der PKI und klärt, ob eine unternehmensinterne Struktur ausreicht oder zusätzlich externe Dienstleister nötig sind.

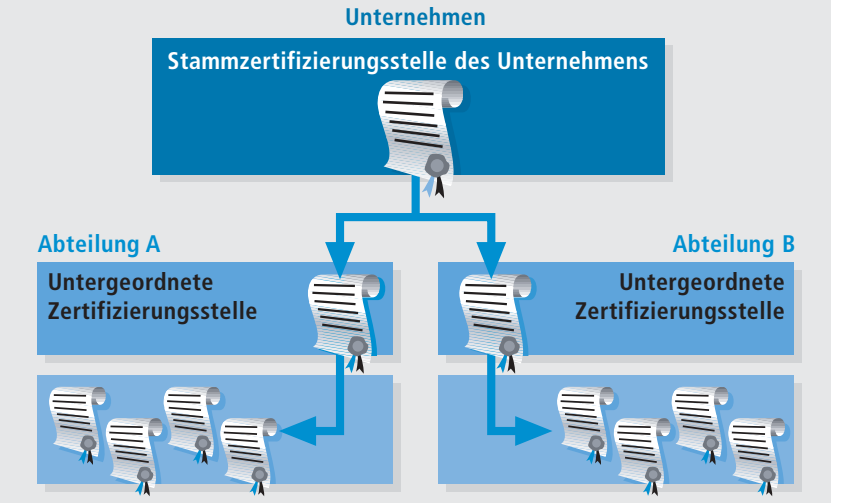
- **Design der PKI bestimmen**

Der im ersten Schritt der Planung festgelegte Verwendungszweck bestimmt die PKI. Für ein Smart-Card-Projekt benötigt ein Unternehmen ein einfaches PKI-Modell, für dessen Betrieb die Hilfe externer Dienstleister normalerweise nicht notwendig ist.

- **Sicherheitsrichtlinien festlegen**

Auch der effiziente Einsatz von Smart Cards erfordert vernünftige Sicherheitsrichtlinien, die unter anderem Folgendes regeln: Welche Anwender erhalten Smart Cards? Sind diese verpflichtet, Smart Cards zu verwenden? Was passiert, wenn die Smart Card aus dem Lesegerät entfernt wird?

PUBLIC-KEY-INFRASTRUKTUR IN EINEM UNTERNEHMEN



Große Netzwerke verwenden eine hierarchische PKI, die ähnlich der Unternehmenshierarchie aufgebaut ist – mit über- und untergeordneten Zertifizierungsstellen.

- **Smart-Card-Technologie und -Hersteller auswählen**

Smart Cards und die dazu passenden Schreib-/Lese-Geräte gibt es in zahlreichen Bauformen und Varianten für viele Anforderungsprofile. Einige Hersteller bieten sogar Kombinationen aus Zugangskontroll- und Arbeitszeiterfassungssystemen an.

- **Planung der Smart-Card-Ausgabe**

Aus sicherheitstechnischen Überlegungen empfiehlt sich eine persönliche Übergabe der Smart Cards an die Mitarbeiter, begleitet von einer kurzen Einweisung in die neue Technologie. Dadurch kann die Verteilung der Smart Cards in größeren IT-Umgebungen zur logistischen Herausforderung werden.

Um Kunden in der Planungsphase zu unterstützen, enthalten die Onlinehilfe von Windows Server und die Microsoft-Webseiten (Link siehe weiter hinten) zahlreiche Dokumente und Whitepaper zur Planung von PKIs und zum Einsatz von Smart Cards.

Der erste Schritt – der Aufbau der Zertifizierungsstelle

Vor dem Einsatz von Smart Cards im Unternehmen steht die Erzeugung von Schlüsseln und Zertifikaten für die Netzwerkanmeldung. Diese Aufgabe übernehmen Zertifikatsdienste, die als Komponente von Windows Server bei der Standardinstallation aber nicht berücksichtigt werden. Sie können jedoch schnell und einfach über die Systemsteuerung nachträglich zu den Serverdiensten hinzugefügt werden.

Für den Einsatz von Smart Cards wird mit Windows Server eine so genannte Zertifizierungsstelle vom Typ „Organisation“ benötigt. Bei der Erstellung von Smart Cards greift diese auf Informationen der Active Directory-Benutzerkonten zu. Die oberste Zertifizierungsinstanz in einer Organisation ist die „Stammzertifizierungsstelle“ – alle anderen Zertifizierungsstellen in der PKI-Hierarchie sind „untergeordnete Zertifizierungsstellen“.

Gemeinsam mit den Zertifikatsdiensten wird eine Weboberfläche auf Basis der Internet Information Services von Windows Server installiert. Sie verwaltet die Dienste, und mit ihr werden die Zertifikate angefordert. Die PKI selbst wird mit der Microsoft Management Console (MMC) und dessen Snap-In „Zertifizierungsstelle“ verwaltet.

Die Smart-Card-Registrierungsstelle in Betrieb nehmen

Die Zertifizierungsstelle versorgt die Smart Card mit Schlüsseln und Zertifikaten. Allerdings müssen hierfür zunächst eine oder mehrere Registrierungsstellen aufgebaut werden. Dort erzeugt der Administrator die Smart Cards und gibt sie an die Anwender aus. Damit eine Registrierungsstelle funktioniert, sind jedoch einige Vorbereitungen nötig: Zunächst muss die Zertifizierungsstelle mit dem MMC-Snap-In so konfiguriert werden, dass sie Zertifikate vom Typ „Registrierungs-Agent“, „Smart-Card-Anmeldung“ und „Smart-Card-Benutzer“ ausstellen kann. Danach muss der Administrator für die Registrierungsstelle ein Zertifikat vom Typ „Registrierungs-Agent“ anfordern und installieren. Erst jetzt ist die Ausgabe von Smart Cards über die Registrierungsstelle möglich. Eine Besonderheit der Zertifikatvorlage „Smart-Card-Benutzer“ ist übrigens, dass sie ein zusätzliches Zertifikat für die sichere, verschlüsselte E-Mail-Nutzung enthält.

Der Einsatz am Client-Computer

Mit der einsatzfähigen Smart Card kann sich der Anwender sofort an seinem Computer anmelden. Nach der Installation eines von Windows unterstützten Lesegeräts bietet der Anmeldedialog wahlweise die Authentifizierung per Smart Card oder mit Anwendernamen und Kennwort an. Der Administrator kann mit Hilfe von Gruppenrichtlinien im Active Directory festlegen, ob beide Anmeldemethoden unterstützt werden oder nur die Smart Card. Sogar das Verhalten von Windows beim Entfernen der Smart Card lässt sich steuern.

Mit Hilfe der Infrastruktur öffentlicher Schlüssel und Smart Cards lässt sich mit geringem Aufwand die Netzwerksicherheit drastisch erhöhen.

Eine Liste der Hersteller, deren Smart-Card-Produkte die technischen Tests im Microsoft Windows Hardware Quality Lab bestanden haben, finden Sie unter

www.microsoft.com/hwdq/hcl/search.asp

Smart-Card-Technologie

Computer in der Brieftasche

Alle Smart Cards haben eines gemeinsam: Die Kartengröße und die Anordnung der Kontaktflächen auf der Kartenoberseite, die durch eine internationale Norm (ISO 7816) festgelegt werden.

Derzeit gibt es zwei Smart-Card-Typen. Einerseits die Memory Card, die ausschließlich Daten speichert. Andererseits die Mikroprozessor-Karte. Sie stellt einen vollwertigen Computer inklusive CPU, Speicher und eigenständigem Betriebssystem dar. Lediglich die grafische Benutzeroberfläche und Eingabegeräte wie Maus und Tastatur fehlen.

Dieser Minicomputer ist für sicherheitskritische Aufgaben besonders gut geeignet. Sein Mikroprozessor übernimmt eigenständig kryptografische Aufgaben und schützt den Speicherbereich der Karte vor unautorisierten Zugriffen von außen. Der Clou dabei ist, dass alle Rechenoperationen auf der Karte ausgeführt werden und kein externer Rechner auf die sicherheitsrelevanten Informationen im Kartenspeicher zugreift.

Die Smart Card verfügt über viele weitere Sicherheitsmerkmale und Schutzfunktionen gegenüber Manipulationsversuchen: Die Daten auf der Karte sind durch eine PIN geschützt, Speicher und CPU sind besonders abgesichert und jede Smart Card verfügt über eine eindeutige Seriennummer.

Die Smart Card erfordert ein spezielles Schreib-/Lesegerät, den Smart Card Reader. Er wird über die serielle Schnittstelle oder den USB-Anschluss an den PC angeschlossen.

Aufgrund der hohen Sicherheit von Smart-Card-Lösungen, werden Microsoft-Produkte diese Technologie auch zukünftig bestmöglich unterstützen.

Weitere Informationen zu den Smart Cards finden Sie unter

www.smartcardforum.org