



© RainerSturm / PIXELIO

Seit Mitte der achtziger Jahre sind Token ein probates Mittel bei der Identity- und Access-Kontrolle. Je mehr sich IT-Systeme für den remoten Zugang von Heimarbeitsplätzen, mobilen Vertriebsmitarbeitern und externen Projektbeteiligten und anderen öffnen mussten, desto mehr gewann die Zugangskontrolle durch starke Authentisierung an Bedeutung.

Dass Passwörter allein allerdings keinen verlässlichen Schutz bieten, ist bereits seit mehr als 20 Jahren bekannt. Umso erstaunlicher ist, dass es heute überhaupt noch Stellungnahmen über Stärken und Schwächen von Passwörtern gibt, wie noch vor kurzem in der New York Times zu lesen. Inzwischen sollte es eigentlich gesellschaftlicher „Common Sense“ sein, dass ein guter Zugangsschutz andere Maßnahmen erfordert. Da diese Tatsache schon solange bekannt ist, wundert es natürlich auch nicht, dass bessere Authentisierungsmaßnahmen auch bereits lange verfügbar sind. Bereits vor mehr als 20 Jahren hieß das Zauberwort hier „Zwei-Faktor-Authentisierung“ – eine Authentisierung, die das klassische Passwort mit einem Token und/oder biometrischen Merkmalen kombiniert, und das zu einer Zeit, in der wir von der heutigen Durchdringung des Alltags mit IT und Internet noch gar nichts ahnten.

Verlässliche Sicherheit gesucht

Fast so alt wie die Passwort-Diskussion ist auch der Ruf nach sogenannten Single Sign-On-Systemen. Da man einem Benutzer (wohl zu Recht) nicht zutraut, sich mehr als ein oder zwei vernünftige Passwörter zu merken, wurden Systeme entwickelt, die sich Passwörter für den Anwender merken. Nach dem Motto „besser ein starkes Passwort als zehn schwache“ versprach man dem Anwender, und auch vielen Systemverantwortlichen, ein „Mehr“ an Komfort und Sicherheit. Letzteres allerdings oft trügerisch, da das Problem nie wirklich an der Wurzel gepackt wurde. Denn geht es um den Schutz wichtiger Daten (und welche sind a priori unwichtig?), sind Passwörter alleine einfach untauglich.

Verlässliche Sicherheit gibt es nur, wenn der Faktor Mensch bei

der Authentisierung durch einen zweiten Faktor unterstützt wird. Dieser zweite Faktor ist entweder ein Passwort-Generator (im Volksmund auch oft Token genannt) oder ein biometrisches Device. Beides erzeugt eine starke Authentisierung, wenn sichergestellt ist, dass der zweite Faktor im Besitz des rechtmäßigen Benutzers ist. Dies ist bei biometrischen Methoden quasi gegeben (wenn denn die Erkennungs-Hard- und Software richtig arbeitet). Bei Token muss sichergestellt werden, dass er nicht ohne weiteres durch eine andere Person benutzt werden kann. Dies erreicht man entweder durch PINs oder durch Kombination der Token mit User-IDs und Passwörtern. Bei Verlust muss darüber hinaus eine schnelle Sperrung gewährleistet sein. Lange Zeit galten biometrische Systeme noch als Science Fiction – dies hat sich mittlerweile geändert, obwohl Token-basierte Systeme gerade in

Industrienumgebungen nach wie vor weit mehr verbreitet sind, nicht zuletzt aufgrund von Kostenzwängen. Kannte man in den achtziger und frühen neunziger Jahren vor allem Challenge/Response-Token, hielten danach die Generatoren von Einmalpasswörtern (One Time Password Token, OTP-Token) einen Siegeszug durch die IT. Mittlerweile haben sich verschiedene Hersteller wie RSA, Vasco, Aladdin, u. a. am Markt etabliert.

Bestechend einfache Lösung

Die Benutzer von OTP-Token profitieren von ihrer einfachen Bedienung und OTP-Token gelten als ideal im mobilen Umfeld. Auch einige Banken haben den Wert dieser Token erkannt und statten bereits ihre Online-Kunden, zumeist aus dem Premium-Bereich, mit OTP-Token aus, um das Online-Banking entsprechend sicherer zu machen. Der OTP-Token erzeugt in regelmäßigen Abständen einen numerischen Code überschaubarer Länge, der auf dem Display angezeigt wird

und anstelle des Passworts oder zusätzlich dazu beim Systemzugang eingegeben wird. Für den Anwender ist das auch schon alles, was der Token macht – insofern eine bestechend einfache Lösung. Die Kehrseite der OTP-Token ist bis heute allerdings einerseits ihr – je nach Hersteller – stolzer Preis und andererseits aber auch die Eindimensionalität ihrer Funktion als reines Authentisierungswerkzeug. Darüber hinaus wird der Administrationsaufwand von vielen IT-Abteilungen als hoch eingeschätzt – oft im Zusammenhang damit, dass es sich häufig um eine Insellösung in Bezug auf eine ansonsten integrierte Identity Management-Umgebung handelt.

Eine andere Variante von OTP setzt die Tatsache für sich ein, dass heutzutage fast jeder ein Handy besitzt: In diesem Szenario wird das Einmal-Passwort per SMS an den Anwender gesendet, falls dieser ein Portal für Online-Banking oder ähnliches betreten möchte. Im Unternehmenskontext findet man diese Variante eher in kleineren Projekten, selten in größeren Umgebungen. Auch dient sie manchmal als Fall-

back, wenn die standardmäßige Authentisierungslösung ausfallen sollte.

Der Paradigmen-Wechsel

Der Charme der OTP-Lösungen besteht für viele darin, dass der Nutzer absolut frei in der Wahl des Clients ist, an dem er arbeitet. So kann er zum Beispiel sicher auf seine E-Mails über Web Access zugreifen, egal ob vom PC zuhause oder unterwegs von einem fremden PC auf dem Flughafen, im Hotel oder in einem Internet-Café. Der OTP-Token funktioniert immer und unabhängig vom PC oder Notebook. Da Clients heute überwiegend mobil geworden sind, wird allerdings auch Mobilität anders definiert – die überwiegende Mehrheit der mobilen Mitarbeiter benutzt ihr Notebook, ihren Blackberry oder ihr Smartphone als alleiniges Device. Schon aus Opportunitätsgründen haben sich diese Geräte daher als Client der Wahl durchgesetzt, da man mit ihnen sein mobiles „Büro“ immer dabei hat.

Auch gibt es mittlerweile viele Unternehmen, die eine Benutzung

	Klassisches Passwort	OTP Token		Digitales Zertifikat		
		Hardware	Handy	Software-Zertifikat	Software-Zertifikat (TPM)	Hardware (Smart Card, USB Token)
Schutz gegen Abhören (Man-in-the-Middle-Attacken, Phishing Attacken)	Schwach	Mittel	Mittel	Sehr hoch	Sehr hoch	Sehr hoch
Schutz gegen Brute force Attacken	Schwach	Sehr hoch	Sehr hoch	Sehr hoch	Sehr hoch	Sehr hoch
Gerätesicherheit (tamper-resistance)	NA	Sehr hoch	Sehr hoch	Hoch	Sehr hoch	Sehr hoch
Schutz bei Verlust/Diebstahl	NA	Mittel*	Mittel	Hoch	Hoch	Sehr hoch
Mobilität	Sehr hoch	Sehr hoch	Hoch	Mittel	Mittel	Mittel/Hoch
Komfort für Anwender	Schwach	Hoch	Hoch	Sehr hoch	Sehr hoch	Hoch
Implementierungsaufwand Device (Rollout)	NA	Mittel/Hoch	Gering	Gering/Mittel**	Gering/Mittel**	Mittel/Hoch**
Implementierungsaufwand Backend	Niedrig	Hoch	Mittel/Hoch	Mittel***	Mittel***	Mittel***
Schulungsbedarf Anwender	Mittel (Security Awareness!)	Gering	Gering	Gering	Gering	Gering
Fortlaufender Administrationsaufwand/Support	Hoch (Help Desk)	Hoch	Hoch	Gering	Gering	Mittel
TCO	Hoch (Help Desk)	Hoch	Mittel	Mittel	Mittel	Mittel/Hoch
Universalität (Verschlüsselung, Signatur)	Keine	Keine	Keine	Sehr hoch	Sehr hoch	Sehr hoch

* Ohne PIN-Schutz

** Gering bei Benutzung von Microsoft AutoEnrollment

*** Bei On-Demand-Lösungen gering

Bild 1: Ein Vergleich der bestehenden Authentisierungsvarianten kommt nicht immer zu einem einheitlichen Ergebnis.

von Fremd-PCs zur mobilen Kommunikation aus Sicherheitsgründen nicht erlauben. Hier wird nur eine gesicherte VPN-Verbindung vom eigenen Gerät mit der entsprechenden Sicherheits-Policy zu Virenschutz etc. überhaupt zugelassen. Auch die fortschreitende Miniaturisierung (Stichwort Netbook) und Konvergenz mobiler Clients beschleunigt diese Entwicklung erheblich und man kann formulieren: Das Notebook wird zum Token.

Total Cost of Ownership. In der Praxis gibt es neben dem oben geschildertem „Pretty Good Privacy“ (PGP)-Verfahren vornehmlich das auf dem X.509-Standard beruhende Zertifikat. Dieses kann sowohl auf dem PC oder Notebook direkt als Software installiert oder auf Crypto-Hardware (Smart Card, USB-Token) aufgebracht werden. Gegen diese Software-Variante gab es lange Zeit Sicherheitsvorbehalte, wurde der geheime Schlüssel doch auf dem

natürlich auch vom jeweiligen Einsatzzweck ab. Deshalb können die folgenden Bewertungen nur einen Trend vermitteln, generell gültige Aussagen sind, wie so oft, problematisch.

Relativ eindeutig fällt allerdings der Vergleich zwischen OTP-Token beziehungsweise Zertifikatslösungen und Passwörtern aus, die in fast allen Bereichen schlechter abschneiden – was zu erwarten war. Ein Vergleich zwischen OTP-Token und Zertifikaten ist da schon weniger eindeutig, da hier auch das Einsatz-Szenario eine gewichtige Rolle spielt.

In Punkto unbeschränkter Mobilität sammeln OTP-Token nach wie vor Pluspunkte, auch wenn es hier enger wird. Wenn Mitarbeiter aber Zugang von beliebigen Orten (Home PC, Internet Cafe, Hotel etc.) aus benötigen, können Zertifikate nichts ausrichten – auch nicht, wenn sie auf Karten oder USB-Token aufgebracht sind. Denn diese benötigen in der Regel einen CSP (Cryptographic Service Provider), der selten auf einem Fremd-PC verfügbar ist.

Das andere Extrem ist die Universalität. Werden weitere Sicherheitsfunktionen wie E-Mail-Verschlüsselung benötigt, ist das Zertifikat unschlagbar. Bei gleichem Implementationsaufwand werden hier die erweiterten Mechanismen gleich mitgeliefert. Und vielfach benötigen gerade die Mitarbeiter, die die Mobilitätsanforderungen haben, auch weitergehende Verschlüsselungsdienste – und die elektronische Signatur von Dokumenten birgt bekanntlich erhebliches Prozesspotenzial.

Unterschiede in der Sicherheit

In Bezug auf die Sicherheit des Verfahrens beziehungsweise der Geräte gibt es ebenfalls Unterschiede. Bei Benutzung von TPM-Notebooks oder Smart Cards ist die Gerätesicherheit von untergeordne-



Bild 2: Die On-Demand-Lösung TC Enterprise ID QuickStart von TC TrustCenter – eine PKI mit vollem Funktionsumfang: sie unterstützt das Management international anerkannter X.509-Zertifikate sowie Key Recovery, fortgeschrittenes Reporting u.a.

Die Alternative – Digitale Zertifikate

Digitale Zertifikate basieren auf Public Key-Verfahren. Ein geheimer und nur dem Besitzer zugänglicher Schlüssel ergänzt sich mit einem öffentlich bekannten Schlüssel des Anwenders zu einem Schlüsselpaar, das verschiedene Dienste auf sehr sichere Art und Weise erbringen kann.

Dort wo das OTP Device bei der Authentisierung stehen bleibt, bietet ein digitales Zertifikat zusätzlich Verschlüsselungs- und Signatur-Funktionen – und dies in aller Regel bei einer geringeren

PC als Datei hinterlegt – und auch bei besten Sicherheitsvorkehrungen ist jede Datei letztendlich auslesbar. Die Nutzung von Trusted Platform Modules (TPM) in Notebooks macht diese Sorge allerdings jetzt hinfällig. TPMs sind Crypto-Chips im Notebook, die quasi wie eine eingebaute Smart Card funktionieren. Dort kann der geheime Schlüssel sicher hinterlegt werden.

Trends: Alternativen im Vergleich

Ein Vergleich (siehe Bild 1) der bestehenden Authentisierungsvarianten kommt nicht immer zu einem einheitlichen Ergebnis und hängt

ter Bedeutung, aber im Verfahren gibt es Unterschiede. Während bei OTP-Token das „Geheimnis“ (= OTP) – auch wenn es nur einmal verwendet wird – übermittelt wird, ist das bei Zertifikaten nicht der Fall. Denn hier wird das eigentliche Geheimnis, der private Schlüssel, nie übertragen, so dass ein Abhören des Passwortes für eine Man-in-the-middle oder Phishing-Attacke bei Zertifikaten erfolglos ist. Solche Attacken hat es bei OTP-Token aber schon gegeben (siehe Quelle: c't 16/2006; Brian Krebs blog on Washington-Post).

Beim Aufwand unterscheiden sich die Systeme teilweise erheblich. OTP-Token gelten nicht nur als

Um die Kostenvorteile von Zertifikats-basierter Authentisierung voll zu nutzen, bietet sich die Nutzung eines On-Demand-Services für das Zertifikats-Management an.

Eine solche Plattform, wie sie etwa TC TrustCenter anbietet, ermöglicht die schnelle Nutzung von X.509-Zertifikaten ohne Investitionen in Hard- und Software, ohne Installation von Client-Software und ohne Konfigurationsänderungen.

Der Provider übernimmt das vollständige Management der Backend-Infrastruktur. Bei Software-Zertifikaten entfällt zudem das Management von physikalischen Geräten.

Fazit

OTP-Token sind nach wie vor ein probates Mittel für die Absicherung des remoten Zugangs. Allerdings haben sie aufgrund der veränderten Mobilitätsanforderungen eine ernstzunehmende Konkurrenz bekommen durch Digitale Zertifikate. Digitale Zertifikate können in vielen Fällen eine bessere Alternative sein, die sich vor allem besser in eine bestehende IDM-Landschaft integrieren lässt und erhebliche Mehrwerte liefert. Unternehmen, die bereits OTP-Token einsetzen, sollten daher prüfen, ob sich das Einsatzszenario nicht geändert hat. Denn oft liegt die Entscheidung für OTP bereits



„Digitale Zertifikate können gegenüber OTP-Token in vielen Fällen eine sinnvolle Alternative sein.“

Dr. Artur Heil, TC TrustCenter GmbH

teuer in der Anschaffung und beim anfänglichen Ausrollen, sondern auch im Management während ihres Lifecycles. So kommen zur physikalischen Verwaltung (Bestellung, Lager, Ausgabe) Aufwände hinzu für

- Unterhalt der Backend Server Infrastruktur,
- Ersatz für verlorene Token,
- Ersatz für abgelaufene Token/Batterien,
- Rücknahme der Token von Zeitarbeitern oder Ex-Mitarbeitern,
- Upgrade-Kosten für neue Versionen.

Anwendungsintegration

Neben der Implementierung und dem Lifecycle-Management spielen aber natürlich auch Fragen der Anwendungsintegration eine Rolle. Bei Standardanwendungen wie Remote Access (zum Beispiel via Radius-Protokoll) sind sowohl OTP-Token als auch x.509-Zertifikate in der Regel problemlos einsetzbar. Auch viele andere Anwendungen werden gut unterstützt, solange man sich im Standardbereich (etwa. x.509) bewegt. Verlässt man diesen in Richtung Eigenentwicklungen, können aber bei allen betrachteten Alternativen Integrationsaufwände entstehen. Diese sollten in jedem Fall bei der Berechnung des TCO's einkalkuliert werden.

eine geraume Zeit zurück und der Wandel der Mobilität ist in vollem Gange. Eine Migration abgelaufener Token in Richtung Zertifikate kann sowohl aus Kosten- als auch aus strategischen Gründen sinnvoll sein. Unternehmen, die bisher weder in die eine noch die andere Technologie investiert haben, sollten bei entsprechenden Anforderungen die zukunftssträchtigere X.509 Technologie erwägen, falls nicht erweiterte Anforderungen an die Mobilität dem im Wege stehen.

Dr. Artur Heil