SecurEnvoy

Whitepaper

Die Risiken der Authentifizierung mit digitalen Zertifikaten

Inhaltsverzeichnis

Einleitung

Nichts ist so beständig wie der Wandel – dieses Zitat von Heraklit galt in der Antike ebenso wie heute. Insbesondere die Arbeitswelt hat sich in den vergangenen Jahren verändert, erst durch stationäre Rechner, dann durch mobile Endgeräte wie Laptops und Co. Smartphones haben sich zum „Büro für die Westentasche“ weiterentwickelt, dank mobilem Internet können Nutzer nahezu überall E-Mails abrufen und im Web surfen. Daher verlagert sich der klassische Arbeitsplatz vom Bürogebäude zunehmend in andere Örtlichkeiten, seien es das Home Office, das Café nebenan, das Hotelzimmer oder die Gäste-Lounge am Flughafen. In den späten 1990er Jahren kamen digitale Zertifikate (DZ) zur Authentifizierung von Endnutzern auf, konnten sich aber nicht durchsetzen. Noch eine ganze Dekade später erschweren dieselben Schwierigkeiten die Übernahme von DZ, während die weitverbreiteten Fehlschläge vergessen scheinen.

Dieses Whitepaper erklärt, wie Zertifikate funktionieren, zeigt auf, welche Probleme sich bei der Nutzung ergeben können, und vergleicht sie mit der tokenlosen Zwei-Faktor-Authentifizierung, die als Alternative in Frage kommt.

Was ist Remote Access?

Remote Access lautet die englische Bezeichnung für Fernzugriff. Der Begriff hat sich spätestens mit Aufkommen des BYOD(Bring your own Device)-Trends etabliert, der die geschäftliche Arbeit mit privaten, mobilen Endgeräten beschreibt. Beim Remote Access greift der Mitarbeiter aus der Ferne über einen stationären Rechner, Desktop, Laptop, Tablet-PC oder ein Smartphone über Wählverbindungen oder das Internet auf einen anderen Computer, das Unternehmensnetzwerk oder andere innerbetriebliche Kommunikationseinrichtungen zu. Die Verbindung läuft über den Anwendungsdienst Remote Access Service (RAS) und dessen Protokolle, wie z.B. das IPSec (Internet Protocol Security) und SSL (Secure Sockets Layer). Bevor der Zugang jedoch freigegeben wird, muss sich der Mitarbeiter in der Regel zuerst autorisieren und damit nachweisen, dass er erstens die erforderlichen Rechte für den Zugriff besitzt und zweitens auch wirklich die Person ist, die er vorgibt zu sein.

Authentifizierung mit digitalen Zertifikaten

Eine Möglichkeit der Autorisierung ist ein digitales Zertifikat (DZ). Dabei handelt es sich um eine Identitätsbescheinigung (quasi einen digitalen Ausweis), die einer

Person eine digitale Kennung zuordnet. DZ lassen sich einsetzen, um die Identität eines Nutzers zu bestätigen, der auf eine Website oder einen Remote Access Server zugreift. Vertrauensgrundlage ist dabei ein privater Schlüssel (s. nächstes Kapitel), der auf einer Smartcard oder einem tragbaren Gerät gespeichert ist, das vom User stets mitgeführt wird. DZ bestehen aus einem Datensatz, der Folgendes beinhaltet:

- den registrierten Namen des Zertifikatbesitzers,
- den öffentlichen Schlüssel des Zertifikatbesitzers,
- das Ausgabe- und Verfallsdatum des digitalen Zertifikats,
- den registrierten Namen der Zertifizierungsinstanz sowie
- die digitale Unterschrift der Zertifizierungsinstanz.

Mit kryptografischen Verfahren lassen sich Zertifikate auf Echtheit prüfen. Sobald das Zertifikat abgelaufen ist, kann es nicht mehr verwendet werden und muss ersetzt werden.

Asymmetrische Verschlüsselung

Bei DZ werden zwei Chiffrierschlüssel verwendet: ein privater und ein öffentlicher. Dies wird auch als asymmetrische Verschlüsselung bezeichnet, weil Daten mit nur einem Schlüssel verschlüsselt werden; für die Entschlüsselung hingegen wird ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel, benötigt. Den privaten Schlüssel verwahrt der Nutzer an einem sicheren Ort, während er den öffentlichen Schlüssel allen Teilnehmern bereitstellt, mit denen er Daten austauscht.

Ausgabe

Die Erstellung dieser digitalen Ausweise wickelt eine Zertifizierungsstelle ab, kurz CA (certification authority). Diese kann organisationsintern angelegt sein; alternativ greifen Unternehmen auf eine kommerzielle CA zu. Bei erstmaliger Registrierung eines DZ müssen Nutzer zunächst ihre Identität nachweisen, um zu zeigen, dass sie diejenigen sind, die sie vorgeben zu sein. Das lässt sich manuell erledigen, indem z.B. persönliche Ausweisdokumente wie Personalausweise geprüft werden, was allerdings sehr zeitaufwändig ist. Alternativ lässt sich dieser Prozess mittels tokenloser Zwei-Faktor-Authentifizierung per SMS automatisieren, um die Identität zu belegen. Im Anschluss an die Authentifizierung generiert das lokale Gerät des Nutzers ein Schlüsselpaar und leitet den öffentlichen Schlüssel an die CA weiter. Er

wird signiert vom Root Key der CA, zusammen mit Informationen über den Nutzer, die CA und das Verfallsdatum (typischerweise ein Jahr). Es ist von immenser Bedeutung, dass der private Schlüssel in einem gesicherten Bereich des Gerätes (der virtuellen Smartcard) abgespeichert wird, sodass er nicht von Malware kopiert werden kann. Die meisten CA wissen nicht, wie der private Schlüssel gespeichert sein wird; daher müssen vor der Weiterleitung an die CA zusätzliche Prüfungen durchgeführt werden, um zu demonstrieren, wie der Schlüssel gesichert werden wird.

Life Cycle Management

Was passiert aber, wenn das DZ nach einem Jahr abläuft? Die User sind nicht mehr in der Lage, sich mit diesem Zertifikat zu authentifizieren, und können auch keinerlei Remote Access-Zugangsservices nutzen. Sie müssen ein neues Zertifikat beantragen und dazu erneut ihre Identität belegen. Außerdem wird der Nutzer vermutlich einen Anruf beim unternehmensinternen Help Desk tätigen, um ein neues Zertifikat ausstellen zu lassen oder sich durch den Prozess des „Re-Enrollings“ begleiten zu lassen, falls dieser mittels Zwei-Faktor-Authentifizierung automatisiert ist.

Und das Zertifikat der CA? Alle Zertifikate inklusive der CA-eigenen, selbst signierten besitzen ein Verfallsdatum, was meistens fünf Jahre beträgt. Läuft diese Frist ab, sind alle von der CA ausgegebenen DZ nicht länger gültig. Im schlimmsten Fall können Tausende Nutzer daraufhin nicht weiterarbeiten und müssen sich mit einem neuen CA-Zertifikat anmelden.

Der Umgang mit verlorenen Geräten

Backend-VPN- oder Webserver prüfen die Validität eines DZ mittels einer Online-Abfrage über das OCSP(online certificate status protocol)-Protokoll. Die Anfrage geht auf einem OCSP-Server ein, der mit „gut“, „gesperrt“ oder „unbekannt“ Auskunft über den Status des DZ gibt. Die Antworten kommen von der CA, die den Status der DZ im Server aktualisiert. Diese Überprüfung kann zu Verzögerungen beim Login-Prozess führen. Das OCSP erweitert die Zertifikatssperrliste CRL (Certificate Revocation List). Sie muss komplett heruntergeladen werden und wird in der Regel für 24 Stunden gespeichert. In einer CRL sind alle Seriennummern der aktuell ungültigen DZ eingetragen, die entweder gesperrt sind (temporär nicht

verfügbar) oder widerrufen wurden (d.h. endgültig nicht mehr verwendbar). Da CRLs nur in regelmäßigen Abständen heruntergeladen werden, gibt es weniger Verzögerungen bei der DZ-Auskunft, dennoch lassen sich verloren gegangene oder gestohlene Geräte noch bis zu 24 Stunden nach Bekanntgabe des Verlustes nutzen.

Die Gefahr verteilter Identitäten

Hinzu kommt die Gefahr verstreuter Identitäten. Mit der Etablierung des BYOD-Trends möchten immer mehr Mitarbeiter ihre Mobiltelefone und tragbaren Tablet-Geräte nutzen. Unter der Annahme, dass es nicht praktikabel ist, eine externe Smartcard mit diesen Devices zu unterstützen, benötigt jedes Gerät ein eigenes DZ und damit auch eine separate Ausrollanfrage. Je mehr Geräte ein Anwender einsetzt, desto weiter verstreut er seine digitale Identität.

Was passiert außerdem, wenn ein Gerät durch ein neues ersetzt wird? Meist ist der private Schlüssel in einer „virtuellen Smartcard“ gespeichert, die Teil der Geräte-Hardware ist, sodass das neue Gerät komplett von Grund auf neu eingerichtet werden muss. Diese Vorgehensweise führt dazu, dass Nutzeridentitäten noch mehr verstreut werden. Unternehmen sollten daher sicherstellen, dass alte Devices, die nicht mehr gebraucht werden, korrekt annulliert werden.

Kombinieren statt zertifizieren

Einen sichereren Weg bietet die Zwei-Faktor-Authentifizierung (kurz 2FA), da sie personengebunden ist und zwei Komponenten miteinander koppelt, die erst in korrekter Kombination den Login ermöglichen. Zur eindeutigen Identifizierung eines Anwenders sind mindestens zwei von drei Faktoren nötig:

- etwas, das nur der Nutzer selbst kennt, wie z.B. eine PIN,
- etwas Materielles, das ausschließlich der Nutzer besitzt, wie z.B. Schlüssel, Kreditkarten oder ein Mobiltelefon, und/oder
- etwas, das untrennbar zu einem Nutzer gehört, wie z.B. der Fingerabdruck.

Bekannt ist dieses Prinzip z.B. vom Geldabheben am Bankautomaten: Für eine erfolgreiche Transaktion benötigt der Kunde seine persönliche Bankkarte und seine PIN. Fehlt eine der beiden Komponenten oder wird die PIN nicht korrekt eingegeben, bleibt der Zugriff auf das Konto gesperrt. Bei anderen Methoden kann

der User eines seiner Endgeräte (und damit etwas, das er besitzt) als tokenloses Authentifizierungswerkzeug auswählen – z.B. sein Mobiltelefon. Darüber authentifiziert er sich bei allen weiteren Endgeräten, PCs, Laptops, Internet-Café- oder Business-Lounge-Logins, ohne seine Identität weiter zu verteilen.

Doppelt sichere Gerätewechsel

Auch das sogenannte Life Cycle Management ist besonders abgesichert. So kann nur ein Gerät zur Authentifizierung genutzt werden; alle weiteren angemeldeten Geräte sind zu diesem Zeitpunkt nicht nutzbar. Wechselt der Anwender also z.B. vom Smartphone aufs Tablet, ist nur noch darüber der Login möglich. Auf dem Smartphone werden hingegen ggf. noch verbliebene OTPs gelöscht. Ähnlich läuft ein Gerätewechsel auf ein anderes/neueres Modell ab: Der User verwendet sein bisheriges mobiles Device, um sich auf dem neuen zu authentifizieren. Anschließend löscht das System automatisch alle Spuren auf dem alten Gerät. Dadurch ergeben sich keine Risiken beim Weiterverkauf.

Die tokenlose Zwei-Faktor-Authentifizierung SecurAccess von SecurEnvoy erhöht die Sicherheit zusätzlich durch die Aufteilung des Seed Record, eines speziellen Algorithmus zur Erstellung der OTPs. Ein Teil des Record wird lokal am Server des Klienten erzeugt und per QR-Code an das Endgerät gesendet, während der zweite Abschnitt durch charakteristische Eigenschaften des mobilen Endgeräts bestimmt wird. Dabei handelt es sich um eine Art „Fingerabdruck“, bestehend aus Informationen über die CPU-Seriennummer u.Ä. Jedes Mal, wenn der User einen Passcode abfordert, entschlüsselt das Endgerät den ersten Seed Record-Part und leitet den zweiten Teil entsprechend ab. Auf diese Weise ist immer nur ein Teil des Record auf dem Gerät hinterlegt.

Im Überblick: Vorteile der tokenlosen 2FA

- Der Nutzer wählt ein Endgerät aus, das er als Hardware-Token nutzt und mit dem er sich für alle weiteren Geräte authentifiziert.
- Keine Identitätsstreuung über mehrere Devices
- Keine regelmäßigen Neueinrichtungen notwendig
- Kein Massenausfall durch abgelaufene DZ
- Keine Verzögerungen, ausgelöst durch Zertifikatsüberprüfungen

- Keine Risikoperiode von bis zu 24 Stunden im Verlustfall, da sich die tokenlose Zwei-Faktor-Authentifizierung in Echtzeit sperren lässt
- Keine zusätzlichen Hardware Token notwendig, die angeschafft, konfiguriert, gewartet und turnusmäßig oder bei Verlust/Diebstahl ersetzt werden müssen
- Funktioniert mit allen gängigen Mobiltelefonen, Smartphones, Laptops, Tablets, Microsoft-PCs und Apple Macs.

Fazit

DZ sind Teil der Entwicklungsgeschichte im Bereich IT-Sicherheit. Als Vorläufer sind sie noch nicht ausgereift, um vollständigen Schutz zu bieten. Die Technologie hat sich weiterentwickelt hin zu 2FA. Damit stellen Unternehmen sicher, dass sich ihr Personal eindeutig identifiziert, da nur die korrekte Kombination aus Benutzerdaten und OTP den Login ermöglicht. Wird eine tokenlose 2FA-Software gewählt, ergeben sich weitere Vorteile wie z.B. Kostenersparnis und einfache Implementierung. Des Weiteren setzen die Mitarbeiter einfach die meist ohnehin vorhandenen Mobilgeräte ein, die sie zudem in der Regel bei sich tragen. In puncto Life Cycle Management kann das Personal zudem Endgeräte selbst updaten, ohne einen Anruf beim Help Desk tätigen zu müssen oder seine Identität auf dem vorherigen Gerät zu hinterlassen. Weitere Sicherheit gewährleisten zweigeteilte Seed Records, der geregelte Einsatz von nur einem Endgerät je Login sowie die übergreifende Authentifizierung bei Gerätewechsel.