Whitepaper

Nutzen Sie die Kraft von sieben Milliarden Mobiltelefonen zur Authentifizierung

Inhaltsverzeichnis

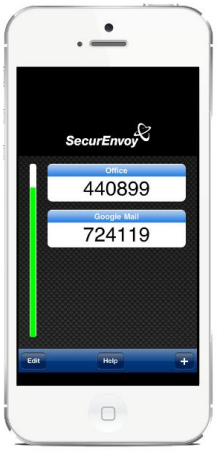
Einleitung

So viele Mobiltelefone wie Menschen auf der Erde soll es im Jahr 2014 geben, so die Prognose der Internationalen Fernmeldeunion (ITU) – das bedeutet rund sieben Milliarden Geräte. Dabei haben Smartphones zwischenzeitlich herkömmliche Mobiltelefone im internationalen Vergleich überflügelt. Die Alleskönner sind geschäftlich wie privat zum ständigen Begleiter avanciert. Dank mobilem Internet ermöglichen sie E-Mail-Abruf, Surfen oder Webtelefonie von unterwegs. Wie sich der Zugriff auf Unternehmensnetzwerke am effektivsten absichern lässt, erklärt dieses Whitepaper.

Bewährtes statt Neuinvestitionen

Wer auf Daten und Informationen zugreifen will, muss in der Regel seine Identität belegen, oftmals per Benutzername und Passwort. Mehr Sicherheit bieten Zwei-Faktor-Authentifizierungslösungen, die den Nachweis gleich doppelt erbringen: Neben den persönlichen Login-Daten gibt der Nutzer einen einmalig gültigen Passcode (One-Time-Passcode, OTP) ein. Diesen empfängt er entweder über ein spezielles Hardware-Token, das er zu diesem Zweck immer mit sich tragen muss. Nachteile für Unternehmen sind hierbei erhöhte Kosten für die Verteilung, Ausgabe und Wartung. Zudem bedeutet ein verlorenes Token auch einen „verlorenen“ Systemzugriff. Einen einfacheren Weg bieten tokenlos arbeitende Zwei-Faktor-Authentifizierungssysteme, denn sie nutzen vorhandene Mobilgeräte wie Mobiltelefone und Co. Per E-Mail, SMS oder App erhält der Nutzer den Passcode. Statt an ein zusätzliches Token denken zu müssen, setzt der User also einfach sein Mobile Device ein.

Beispiel für Hardware-Token



Passcodes in der SecurEnvoy-Lösung

Der Nutzer hat die Kontrolle

SecurEnvoy als Erfinder der tokenlosen SMS-Methode stellt dabei die Kontrolle durch den Nutzer an oberste Stelle. So können auch konventionelle Mobiltelefone, sog. Feature Phones, zur Authentifizierung eingesetzt werden. Dank SMS-Fähigkeit empfangen sie die Passcodes per Textnachricht. Allerdings ist hierbei wichtig zu bedenken, was passieren könnte, wenn der Nutzer kein Mobilfunksignal hat oder Übertragungsverzögerungen bemerkt. Diese Schwierigkeit umgeht SecurEnvoy von vornherein über sein patentiertes Vorgehen mittels vorgeladener (preload) SMS. Das bedeutet, ein eingetippter Code wird sofort ersetzt und eine neue Zahlenfolge steht für den nächsten Authentifizierungsprozess zur Verfügung. Darüber hinaus hilft ein kleiner SMS-Trick dabei, die vorhandene Nachricht mit einem neuen Passcode zu aktualisieren anstatt eine neue Nachricht senden zu müssen. Dadurch muss der Anwender keine alten SMS löschen

Alternativ können Besitzer von Smartphones auf eine Soft Token App zurückgreifen, die die Technologie One Swipe enthält. Der Vorteil ist, das die App die Passcodes in Echtzeit generiert, ohne eine Internet- oder Mobilfunkverbindung zu benötigen; alle 30 Sekunden wird eine neue Zahlenfolge ähnlich wie bei einem physischen Token bereitgestellt. Die Anwendung ist für Smartphones, Tablets sowie Laptops erhältlich und arbeitet unter den Betriebssystemen iOS, Blackberry, Android, Mac OSX, Windows XP, Vista, 7 und 8. Bei der One Swipe-Methode erstellt der Nutzer innerhalb der App einen einmalig gültigen QR-Code, der alle nötigen Authentifizierungsinformationen erhält, inklusive der User ID. Dieser QR-Code wird anschließend per Webcam am Laptop oder Tablet erfasst und ermöglicht so den unkomplizierten Identitätsnachweis. Mit Blick auf die Zukunft arbeitet SecurEnvoy auch an sicheren Authentifizierungsprozessen mittels Fingerabdruck und NFC (Near Field Communication, engl. für Nahfeldkommunikation, die den kontaktlosen Austausch von Daten per Funktechnik über kurze Strecken ermöglicht). So wie Apple Air Pay Zahlungen von Kleinbeträgen ermöglichen wird, wird One Swipe die gleiche Prozedur einsetzen, um Mitarbeitern Remote-Zugriffe auf Unternehmensressourcen zu geben.

Schema der One Swipe-Methode

Selbst wenn der Anwender kein mobiles Endgerät besitzt, kann er sich virtuell ausweisen. Dazu hat SecurEnvoy den Voice Call entwickelt. Nach Eingabe der Login-Daten zeigt der Anmeldebildschirm einen Passcode an. Zur gleichen Zeit setzt das System einen Festnetzanruf ab, den der Nutzer entgegennimmt und über die Telefontastatur den Code eintippt. Auf diese Weise authentifiziert er sich und der Zugang wird gewährt.

Optionen für optimale Passcode-Übertragung

Neben den verschiedenen Übertragungswegen haben End User hinaus die Möglichkeit, die Aktualisierung des Passcodes entsprechend der Arbeitsbedingungen im Unternehmen anzupassen. Auf diese Weise lassen sich z.B. vorübergehende Empfangsschwierigkeiten ausgleichen. Die folgenden Varianten sind möglich:

- **SMS:**

Preload	Echtzeit, Anzeige direkt am Bildschirm	Drei Codes in einer SMS; eingegebene werden direkt durch neue ersetzt	Wiederverwendbare Codes, Aktualisierung alle 1-90 Tage (frei wählbar)

- **Soft Token, mit One Swipe-Option:**

für Smartphones

für Laptops und für Tablets

One Swipe QR-Code

- **E-Mail:**

Preload

Echtzeit

Drei Codes in einer E-Mail, eingegebene werden direkt durch neue ersetzt

Wiederverwendbare Codes, Aktualisierung alle 1-90 Tage (frei wählbar)

- **Voice Call:**

Gerätewechsel selbst vollziehen

Hinsichtlich der Benutzerfreundlichkeit für die IT-Abteilung punkten die tokenlosen Lösungen mit einem optimierten Lebenszyklus-Management. Mittlerweile weisen die meisten Mobilgeräte nur noch eine kurze Verweildauer im Unternehmen auf; nicht selten werden ganze „Flotten“ von Mobile Devices ausgetauscht, sobald ein neues Modell auf den Markt kommt. Aus diesem Grund hat SecurEnvoy auch hier dem Nutzer die Kontrolle übergeben, soll heißen: Er kann den Wechsel vom alten aufs neue Geräte einfach selbst vollziehen. Der Umstieg vollzieht sich dabei praktischerweise ebenfalls mittels Zwei-Faktor-Authentifizierung. Ein Beispiel anhand eines Wechsels vom iPhone 5 auf der aktuelle iPhone 6: Zuerst meldet sich der Anwender über die App oder per SMS vom alten Gerät am „Manage my token“-Portal mittels Zwei-Faktor-Authentifizierung an. Anschließend scannt er den angezeigten QR-Code mit dem neuen Gerät, um es mit einem neuen Seed Record (einem speziellen Algorithmus zur Erstellung der Passcodes) auszurüsten. Der Sicherheitsserver löscht

daraufhin automatisch den alten Seed Record, sodass das alte Gerät bedenkenlos weiterverwendet oder wiederverkauft werden kann. Keinerlei wiederverwendbare Codes bleiben zurück; die Nutzeridentität wird nicht über ältere Geräte verteilt. Zusätzlich nimmt das Anmelden in Eigenregie der IT-Abteilung Arbeit ab.

Damit ist diese Methode extra angeschafften Hardware Token voraus, denn sie würden an dieser Stelle nach umständlicher Neuregistrierung und Verteilung verlangen. Steht ein Wechsel der Token an, sei es aufgrund von Diebstahl, Verlust, aus Wartungsgründen oder auf Grund von Compliance-Richtlinien des IEEE (Institute of Electrical and Electronics Engineers) müssen die IT-Mitarbeiter alle alten Token einsammeln. Anschließend sind die neuen Token für jeden Nutzer einzeln zu registrieren und mit den entsprechenden Voreinstellungen zu versehen. Ggf. sind außerdem Verzögerungen bei der postalischen Zustellung der Geräte zu erwarten, falls Mitarbeiter in einem anderen Land arbeiten. Im schlechtesten Fall wird das Token beim Versand beschädigt und muss nochmals neu ausgestellt werden – dies kann derart ausufern, dass der Nutzer lange Zeit keinen speziell abgesicherten Remote-Zugang nutzen kann.

Verteilen Sie nicht wahllos Ihre Identität

Mit dem Aufkommen des BYOD-Trends verteilen mehr und mehr Nutzer ihre Arbeit auf verschiedene Geräte und Umgebungen wie Tablets, stationäre Rechner, Smartphones, Laptops, Business Lounges, etc. Der Schlüssel zur Beibehaltung der Kontrolle über all diese Geräte ist, eines von ihnen auszuwählen – normalerweise das Mobiltelefon als Software Token – und dieses zu nutzen, um sich auf allen weiteren Devices zu authentifizieren. Diese Vorgehensweise bietet deutliche Vorteile gegenüber anderen Lösungen, bei denen jedes verwendete Gerät mit digitalen Zertifikaten oder mehrfachen Soft Tokens authentifiziert wird. Der Versuch, den Lebenszyklus aller dieser Devices zu verwalten, wird unweigerlich damit enden, dass wenigstens eins der Geräte versehentlich wiederverwendet oder verkauft wird. Der Ansatz von SecurEnvoy ist der einzige, der nur ein Token-Device pro Nutzer erlaubt, es aber dem Anwender sehr einfach macht, dieses Ausgangsgerät zu wechseln, wenn er das Bedürfnis danach verspürt. Diese Vorgehensweise bedeutet schlicht und einfach, dass es unmöglich ist, die Nutzeridentität über mehrere Geräte zu verteilen.

Maximale Sicherheit durch Seed Record-Trennung

Apropos speziell gesichert: Zwei-Faktor-Authentifizierung bedeutet nicht per se „diese Lösung ist sicher“. Jeder 2FA-Entwickler, der kryptografische Schlüssel, sog. Seed Records,

erstellt und sie dann an seine Kunden verteilt birgt eine fundamentale Sicherheitslücke. Denn die Kunden müssen darauf vertrauen, dass die Kopie des Schlüssels, den der Hersteller speichert, sicher aufbewahrt wird und Hackern oder Regierungsbehörden nicht zugänglich ist. SecurEnvoy hingegen fügt eine weitere Sicherheitsstufe hinzu. Die Seed Records werden zu keiner Zeit vom Hersteller generiert oder gespeichert. Dafür sorgt die automatische Separierung des Records: Ein Teil wird lokal am Server des Klienten erzeugt, während sich der zweite aus charakteristischen Eigenschaften des Mobilgeräts ergibt, z.B. Informationen über die SIM-Karte, die CPU o.Ä. Jedes Mal, wenn die App einen Passcode generiert, entschlüsselt das Endgerät den ersten Seed Record-Part und leitet den zweiten Teil entsprechend ab. Auf diese Weise ist es außerdem unmöglich, dass ggf. vorhandene Malware auf dem Smartphone den Seed Record kapert, da ein Teil davon niemals auf dem Gerät vorhanden ist.

Fazit

Rein rechnerisch besitzt mittlerweile fast jeder Erdbewohner ein Mobiltelefon, manche aufgrund von Firmengeräten sogar noch mehr. Auch Laptops und Tablets sind durch die steigende Zahl von aus der Ferne (remote) arbeitendem Personal weit verbreitet. Diese Tatsache können sich Unternehmen, Behörden und andere Organisationen zunutze machen und die Endgeräte als Authentifizierungswerkzeuge einsetzen. Dem User die Kontrolle darüber zu geben, welches Gerät er als Authentifizierungswerkzeug einsetzt und die Möglichkeit, das Gerät jederzeit zu wechseln oder upzugraden ist eine bessere Lösung. Verglichen mit token-basierten Lösungen ist dieser Weg günstiger, weniger arbeitsaufwändig und sicherer, insbesondere dann, wenn wie bei SecurEnvoy der Seed Record getrennt wird, um Manipulationen zu verhindern.