Whitepaper

Der Herr der Schlüssel

Wie zweigeteilte Seed Records alle Sicherheitsbedenken gegenüber Zwei-Faktor-Authentifizierung auflösen

Inhaltsverzeichnis

Einleitung

Was ein Haus für Familien ist, ist ein Netzwerk für Unternehmen – ein Ort, an dem sich das eigene Hab und Gut befindet. Oberste Prämisse ist in beiden Fällen, jederzeit für eine 100 %ige Absicherung zu sorgen. Viele Privatanwender riegeln ihre Habseligkeiten mit Vorhängeschlössern ab, weil diese als sehr sicher gelten, da nur der Hausbesitzer selbst einen Schlüssel zum Öffnen besitzt. Kaum jemand denkt beim Kauf einer solchen Verriegelungsvorrichtung daran, dass auch der Schlosser als Verkäufer bzw. bei Mietshäusern der Hausmeister einen Zweitschlüssel als Sicherheitskopie haben könnte. Doch Schlosser bzw. Schlüsseldienste könnten von Dieben bestohlen werden, die dann direkten Zugriff auf Aberhunderte von Zweitschlüsseln hätten. Einem Beutezug durch Häuser und Villen stünde nichts mehr im Wege. Somit lauert für Haus- und Wohnungsbesitzer eine stete Gefahr im Hintergrund, der sich die meisten gar nicht bewusst sind.

Dieser Fall lässt sich nahezu eins zu eins auch in der digitalen Welt wiederfinden – insbesondere bei Netzwerkzugriffen via Zwei-Faktor-Authentifizierung (2FA). Die Methode soll als Schutzschirm für sensible Firmendokumente dienen, doch manche 2FA-Anbieter setzen ihre Kunden dabei neuen, externen IT-Bedrohungen aus. Welche Schäden dadurch entstehen können und worauf Unternehmen achten sollten, erklärt dieses Whitepaper.

Passwortschutz allein reicht nicht mehr

Nicht nur Wohnungs- und Hausbesitzer verriegeln ihr Hab und Gut; auch Unternehmen schirmen interne Daten und Informationen gegenüber Hackern und anderen Cyberkriminellen ab. Immer noch am weitesten verbreitet ist der Passwortschutz. Mitarbeiter müssen daher für den Zugriff auf das Firmennetz zunächst ihre Identität belegen, was mittels Eingabe des Benutzernamens und des persönlichen Passworts geschieht. Doch der einfache Passwortschutz allein bietet nicht ausreichend Sicherheit, was aktuelle Schlagzeilen über massive Firmen-Hackings verdeutlichen: Großunternehmen wie eBay oder Dropbox waren kürzlich von millionenfach gestohlenen Passwörtern betroffen. Finanzielle und Imageschäden können hier die Folge sein. Firmen sollten daher neben Benutzername und Passwort eine zweite Sicherheitseingabe für den Netzwerkzugriff einführen – so wie bei Zwei-Faktor-Authentifizierungslösungen üblich.

2FA ja, Hardware-Token nein

Im Rahmen der Zwei-Faktor-Authentifizierung geben Mitarbeiter zusätzlich zu den persönlichen Login-Daten einen einmalig gültigen Passcode (One-Time-Passcode, OTP) ein.

Damit Angestellte diesen Code empfangen können, erhalten sie von ihren Arbeitgebern ein Hardware-Token, z.B. eine Smartcard. Dieses Gerät muss immer mitgeführt werden, um sich bei der Arbeit unmittelbar im Netzwerk authentifizieren zu können. Die Kosten der Token mögen einzeln gesehen gering sein, sind jedoch für Unternehmen ein nicht zu unterschätzender Faktor, da in der Regel jeder Mitarbeiter, der Zugriff auf das Netzwerk haben soll, ein solches Authentifizierungsgerät braucht. Je nach Mitarbeiteranzahl entstehen erhebliche Kosten, und auch der finanzielle Schaden durch Diebstahl oder Verlust der Token ist nicht zu verachten. Hinzu kommt der Wartungsaufwand, den die Hardware-Token verursachen.

Beispiel für Hardware-Token

Einfachere Login-Vorgänge bieten Zwei-Faktor-Authentifizierungssysteme, die ohne kostenintensive physische Token auskommen. Firmen nutzen stattdessen die vorhandenen Mobilgeräte der Mitarbeiter. Der zum Einloggen erforderliche zweite Passcode wird Nutzern per SMS, E-Mail oder App auf ihr Smartphone, Laptop oder Tablet zugeschickt. Somit kann sich der Nutzer mit einem Mobilgerät authentifizieren, das er ohnehin jeden Tag mit sich trägt. Da Smartphones die herkömmlichen Mobiltelefone in der Praxis längst abgelöst haben, ist für Firmen die Passcode-Zustellung via App mit Blick auf die Zukunft wohl die interessanteste.

Wenn der Hersteller den Zweitschlüssel verliert

Mitarbeiter installieren die sogenannten Soft Token Apps für iOS, Android etc. auf ihrem privaten Smartphone. Die App generiert das für den zweiten Authentifizierungsschritt benötigte OTP. Mit Eingabe von PIN und OTP erhalten Angestellte über die Applikation Zugriff auf geschützte Ressourcen im Netzwerk. Doch Unternehmen sollten dabei eine Sache beachten: Die meisten 2FA-Anbieter erstellen mit der Verbreitung der OTPs auch kryptografische Schlüssel, sogenannte Seed Records, und genau diese Schlüssel bergen

fundamentale Sicherheitslücken: Die Kunden müssen darauf vertrauen, dass die Kopie des Schlüssels, die der Hersteller speichert, sicher aufbewahrt wird und Hackern oder Regierungsbehörden nicht zugänglich ist. Somit haben die Hersteller eine ähnliche Verantwortung wie Schlosser oder Hausmeister, die Zweitschlüssel im Falle eines Falles sicher archivieren müssen.

Dem US-amerikanischen 2FA-Anbieter RSA Security Inc. sind jedoch im Zuge eines Hackerangriffs im Jahr 2011 sensible Seeds von den Unternehmensservern gestohlen worden. Da sich aus den Seeds Millionen von OTPs ableiten lassen, verloren alle Software Token wie auch die Soft Token Apps enorm an Sicherheit und Vertrauenswürdigkeit. Somit stellen sich viele 2FA-Nutzer die Frage, ob sie den entsprechenden Anbietern überhaupt noch vertrauen können. Sind die Transportwege sowie die Art und Weise der Erstellung von OTPs überhaupt noch sicher? Können sich auch Regierungen Zugang zu Seeds von Unternehmensservern verschaffen, um Wirtschaftsspionage zu betreiben? Anhand des RSA-Hacks sind diese Bedenken absolut berechtigt. Wie können 2FA-Anbieter die Seeds absichern und vor Dritten schützen?

Doppelter Schutz vor Passwortdieben

SecurEnvoy hat als Erfinder der tokenlosen Zwei-Faktor-Authentifizierung im Gegensatz zu RSA eine weitere Sicherheitsstufe hinzugefügt. Allerdings werden anders als üblich die Seed Records zu keiner Zeit vom Hersteller selbst generiert oder gespeichert. Dies gewährleistet SecurEnvoy durch eine automatische Separierung des Record: Ein Teil wird lokal am Server des Clients erzeugt, während sich der zweite aus charakteristischen Eigenschaften des Mobilgeräts ergibt, z.B. Informationen über die SIM-Karte, die CPU o.Ä. Generiert die App einen Passcode, entschlüsselt das Mobilgerät die erste Seed Record-Hälfte und leitet die zweite Hälfte entsprechend ab. Da also ein Part der beiden Seed Records niemals auf einem Mobilgerät des Mitarbeiters vorhanden ist, schließt SecurEnvoy aus, das angreifende Malware einen Seed Record erbeuten kann. Auch wenn ein Teil des Seed Record vom sogenannten „Hardware-Fingerabdruck“ des Smartphones abgeleitet werden kann, besitzt SecurEnvoy dennoch keinerlei Kopien des Seed.

Passcodes in der SecurEnvoy-Lösung

Auch offline authentifizieren

Die Soft Token App dient den Mitarbeitern somit als sichere Authentifizierungshilfe im Firmenalltag. Für den Fall, dass das Mobilfunksignal plötzlich ausfällt und die OTPs mit der App nicht empfangen werden können, hat SecurEnvoy die Technologie One Swipe entwickelt. Sie generiert die sicheren OTPs in Echtzeit, ohne eine Internet- oder Mobilfunkverbindung zu benötigen. Ähnlich wie bei einem physischen Token wird hierbei alle 30 Sekunden eine neue Zahlenfolge für die Passcodes bereitgestellt. Mitarbeiter können die Anwendung One Swipe auf Smartphones, Tablets und Laptops unter den Betriebssystemen iOS, Blackberry, Android, Mac OSX sowie Windows XP, Vista, 7 und 8 nutzen.

Schema der One Swipe-Methode

Bei der One Swipe-Methode erstellt der Nutzer mit der App einen einmalig gültigen QR-Code. Dieser enthält alle nötigen Authentifizierungsinformationen, inklusive der User ID. Den QR-Code scannen Nutzer anschließend per Webcam am Laptop oder via Tablet ein und erlangen so einen unkomplizierten Identitätsnachweis für den Netzwerkzugriff.

Lebenszyklus eines Tokens

Im Laufe des Lebenszyklus eines Mobilgerätes erhält dieses in der Regel mehrfach Upgrades oder wird repariert. Anwender ersetzen Smartphones und Co. zudem im Schadensfall oder verkaufen die als Token genutzten Geräte unbedarft weiter. SecurEnvoys Ansatz verhindert, dass der neue Besitzer des Mobilgerätes plötzlich ein fremdes Token besitzt. Der 2FA-Anbieter erlaubt nur ein Token Device pro Nutzer, dennoch wird erlaubt, dass Mitarbeiter schnell und sicher z.B. zwischen Smartphone und Tablet als Token wechseln können: Das bedeutet, es ist schlichtweg unmöglich, eine User-Identität über mehrere Mobilgeräte zu verteilen. Alle alten Seed Records werden automatisch vom SecurEnvoy-Sicherheitsserver gelöscht, so dass Nutzer das alte Mobilgerät bedenkenlos weiterverwenden oder wiederverkaufen können.

Kein Mobilgerät? Kein Problem

Wenn ein Mitarbeiter sein mobiles Endgerät vergessen hat oder schlichtweg keines besitzt, kann er sich trotzdem virtuell legitimieren. Dies ermöglicht SecurEnvoy durch eine Voice Call-Funktion. Dabei gibt der Anwender wie gewohnt seine Login-Daten im Anmeldebildschirm ein. Zur gleichen Zeit erhält er den Passcode über einen Festnetzanruf des SecurEnvoy-Systems. Das entgegengenommene OTP gibt der Angestellte über die Telefontastatur ein. Auf diese Weise authentifiziert er sich und erhält Zugriff auf das Netzwerk. SecurEnvoy arbeitet darüber hinaus bereits an zukunftsweisenden sicheren Authentifizierungsprozessen mittels Fingerabdruck und NFC (Near Field Communication). Die letztgenannte Methode ermöglicht sogar den kontaktlosen Austausch von Daten per Funktechnik über kurze Strecken.

SMS noch nicht ausgestorben

Doch nun wieder zurück in die Gegenwart, wo viele Unternehmen nach wie vor auf die klassische SMS-Methode zur Authentifizierung zurückgreifen. SecurEnvoy als Erfinder der tokenlosen SMS-Variante ermöglicht nicht nur Smartphones, sondern auch konventionellen Mobiltelefonen, sogenannten Feature Phones, als Token genutzt zu werden. Dank SMS-Fähigkeit empfangen sie die Passcodes einfach per Textnachricht. Doch was passiert, wenn der Nutzer kein Mobilfunksignal hat oder Übertragungsverzögerungen entstehen? Um diese Schwierigkeit von vornherein zu umschiffen, hat SecurEnvoy ein patentiertes Verfahren mittels vorgeladener (preload) SMS entwickelt. Dabei wird ein eingetippter Code sofort ersetzt, und für den nächsten Authentifizierungsprozess steht schon eine neue Zahlenfolge

zur Verfügung. Ein kleiner SMS-Trick hilft dabei, die vorhandene Nachricht mit einem neuen Passcode zu aktualisieren. Dadurch muss weder stets eine neue Nachricht gesendet werden, noch müssen Anwender ihre alten SMS löschen.

Fazit

Die Anbieter von Zwei-Faktor-Authentifizierungslösungen tragen die große Verantwortung, dass ihre Kunden einen zum sicheren Login notwendigen, zweiten Passcode (OTP) erhalten – ohne das Dritte diesen einsehen oder zurückverfolgen können. Wenn 2FA-Hersteller wie RSA beim Versand der OTPs kryptografische Schlüssel (Seed Records) verlieren, können Hacker alle Passcodes von Unternehmen ausspionieren. Entwickler SecurEnvoy räumt diese eklatante Sicherheitslücke aus, indem man Seed Records teilt. Ein Teil wird lokal am Server des Clients erzeugt, die Charakteristiken des Mobilgeräts des Angestellten bilden den zweiten Teil. Da sich niemals beide Teile des Seed Record auf Smartphones, Tablets etc. befinden, werden Malware-Angriffe zu 100 % ausgeschlossen: Die tokenlose Zwei-Faktor-Authentifizierung von SecurEnvoy schützt somit das Hab und Gut im Firmennetzwerk zu jeder Zeit.