SecurEnvoy

Whitepaper

Das Prinzip der tokenlosen Zwei-Faktor-Authentifizierung

SecurEnvoy

Inhaltsverzeichnis

Einleitung 2
Was ist Zwei-Faktor-Authentifizierung? 2
Zugriff per Hardware Token 3
Vor- und Nachteile von Token 3
Authentifizierung mittels Smartcards 4
Digitale Zertifikate sind von gestern 4
Tokenlose Zwei-Faktor-Authentifizierung: aus BYOD wird BYOT 5
Flexibilität ist Trumpf 5
Im Überblick: Vorteile der tokenlosen 2FA 6
Fazit 7

WHITEPAPER

SecurEnvoy

Einleitung

Das Thema IT-Sicherheit spielt in Zeiten der virtuellen Kriegsführung, immer komplexer werdenden Malware-Bedrohungen und Online-Spähangriffen eine noch bedeutsamere Rolle als zuvor. Insbesondere Firmen sorgen sich, denn Trends wie Bring Your Own Device (BYOD) sorgen dafür, dass Unternehmensnetzwerke angreifbarer werden. Der Zugriff findet nicht mehr nur allein in den Räumlichkeiten der Firma statt, sondern weitet sich auf Home Offices, Hotels und Flughäfen aus – Örtlichkeiten, an denen sich z.B. Außendienstmitarbeiter aufhalten und von dort Unternehmensdaten abrufen möchten.

Um sicherzustellen, dass sich auch tatsächlich Mitarbeiter XY einloggt und nicht etwa ein Cyber-Gangster Anmeldeinformationen zu seinen Zwecken missbraucht, sind verschiedene Methoden entwickelt worden. Allen voran steht das Passwort, das zusammen mit dem Benutzernamen den Login ermöglicht. Doch wie Studien ermittelt haben, sind Passwörter häufig zu einfach gewählt und lassen sich in Folge dessen in kurzer Zeit knacken: Schon ist der Account gekapert.

Für mehr Sicherheit sorgen so genannte Zwei-Faktor-Authentifizierungslösungen. Wie sie im Detail funktionieren, welche Varianten es gibt und worin die Vorteile für Unternehmen bestehen, erklärt dieses Whitepaper.

Was ist Zwei-Faktor-Authentifizierung?

Im Zuge der Entwicklung von IT-Sicherungsmaßnahmen – speziell für Identifizierungsprozesse – sind Security-Spezialisten dazu übergegangen, mehrere Mechanismen miteinander zu verknüpfen. In diese Kategorie fällt auch die Zwei-Faktor-Authentifizierung (kurz 2FA). Zur eindeutigen Identifizierung eines Anwenders sind mindestens zwei von drei möglichen Faktoren nötig:

- etwas, das nur der Nutzer selbst kennt, wie z.B. eine PIN,
- etwas Materielles, das ausschließlich der Nutzer besitzt, wie z.B. ein Token (USB-Stick etc.) und/oder
- etwas, das untrennbar zu einem Nutzer gehört, wie z.B. der Fingerabdruck.

Ein geläufiges Beispiel für eine Authentifizierung per Zwei-Faktor-Methode ist das Geldabheben am Bankautomaten: Für eine erfolgreiche Transaktion benötigt der Kunde sowohl seine persönliche Bankkarte als auch seine PIN. Fehlt eine der

WHITEPAPER

beiden Komponenten oder wird die PIN nicht korrekt eingegeben, bleibt der Zugriff auf das Konto verwehrt.

Diese doppelte Absicherung reduziert das Risiko, dass Kriminelle gestohlene Zugangsdaten umgehend für die Übernahme eines fremden Accounts missbrauchen können. Bei vielen 2FA-Lösungen wird etwas, das der Nutzer besitzt, durch eine einmalig gültige Ziffernfolge, einen sog. One-time Passcode (OTP), repräsentiert. Dieser OTP wird entweder über einen Gegenstand, den User besitzt, generiert, wie z.B. ein Security-Token. Oder ein vertrauenswürdiger Server errechnet den OTP und sendet ihn als zweiten Faktor an das entsprechende Gerät/Token. Ein Übertragungsweg ist z.B. eine SMS-Nachricht auf das Mobiltelefon des Anwenders. OTPs bieten aufgrund der ständigen Neugenerierung weitaus weniger Angriffspotenzial im Vergleich zu häufig statischen oder zu simplen Passwörtern, die darüber hinaus mittels Phishing, Keylogging oder Replay-Angriffen ausgespäht werden können.

Zugriff per Hardware Token

Der konventionelle Weg bei einer 2FA-Lösung besteht in der Nutzung eines Hardware-Tokens. Ein Token kann beispielsweise ein USB-Stick oder ein Schlüsselanhänger sein. Oftmals zeigt ein Display die Zahlenkombination an, die der Nutzer in der Anmeldemaske eintippt. Der generierte OTP identifiziert den Anwender anschließend eindeutig durch Kombination mit seinen persönlichen Login-Daten.

Vor- und Nachteile von Token

Diese Art von Token kann jederzeit und überall zur Nutzererkennung verwendet werden. Zudem ist der User nicht auf zusätzliche Hardware oder Programminstallationen angewiesen. Die Mängel dieser Vorgehensweise betreffen jedoch insbesondere die Handhabung, Sicherheit und Kosten. So ist die Zuweisung eines Tokens an einen speziellen Nutzer unumgänglich. Damit erwarten die IT-Abteilung aufwändige Zuweisungsarbeiten: Je mehr Mitarbeiter ein Token erhalten, desto mehr individuelle Konfigurationen sind nötig.

Zusatzkosten ergeben sich aus der begrenzten Lebensdauer der Geräte (etwa drei bis vier Jahre) sowie bei Verlust oder Diebstahl. Sind weltweit Mitarbeiter ansässig,

entfallen ebenfalls Kosten auf den Versand der Geräte. Hinzu kommt die Abhängigkeit des Nutzers, denn er muss sein Token jederzeit mit sich führen, um sich authentifizieren zu können. Verliert oder vergisst er seinen Token, bleibt ihm der Zugang versperrt. Auf die Dauer könnte der Mitarbeiter das ständige Mitführen, auch auf „Verdacht“, als lästig empfinden. Ein weiterer Schwachpunkt ist, dass der User sein Token nicht immer dabei hat. Doch wenn er es nicht hat, wo ist es dann? Diese Schwachstelle mag bedingt gegebenenfalls, dass der Nutzer gleich mehrere Token mit sich führt.

Authentifizierung mittels Smartcards

Eine andere Methode sind Smartcards, die ebenso wie Hardware Token personengebundene Zugangsprozesse unterstützen. Der wesentliche Vorteil von Chipkarten ist die mehrfache Verwendung der Karte für den Zugang zu Gebäuden und zum Speichern mehrerer Zertifikate in einem Ort. Der Nachteil ist der Einsatz der Chipkarten sowie die Lieferung und die Sicherheit der Zertifikate, mit denen sie arbeiten. Auch hat ein Zertifikat nur eine geringe „Lebenszeit“ und das ist das größte Problem, das Administratoren hinsichtlich des Zertifikat-Managements zu lösen haben: das Ersetzen und Widerrufen von Zertifikaten. Neben dem Einsatz der Chipkarte benötigt der Nutzer zusätzlich am jeweiligen Endgerät einen Smartcard-Reader, der oftmals nicht integriert ist. Dementsprechend muss die passende Hardware nachgerüstet bzw. Software installiert werden. Daraus resultiert meist ein erhöhter Support-Bedarf seitens der Mitarbeiter, die den Umgang mit Smartcards und der dazugehörigen Hard- und Software erst erlernen müssen. Ein weiterer Minuspunkt: Mit mobilen Endgeräten lassen sich Smartcards nicht nutzen, da eine spezifische Lesevorrichtung weder integriert ist, noch auf Grund der meist schlanken Bauweise nachträglich eingebaut oder angebunden werden kann.

Digitale Zertifikate sind von gestern

Mittlerweile eher überholt ist die Nutzung digitaler Zertifikate, da sie sich nur unzureichend für flexible, ortsunabhängige Logins eignen undrechnergebunden sind. Daraus folgt ein weiteres Manko, denn jeder, der den entsprechenden Rechner verwendet, kann sich einloggen, weil das Zertifikat keiner spezifischen Person zugeordnet ist. Sollte der PC re-formatiert oder die Festplatte zerstört werden, ist der Zugang mittels Zertifikat ohnehin unwiderruflich blockiert.

Tokenlose Zwei-Faktor-Authentifizierung: aus BYOD wird BYOT

Eine flexiblere Vorgehensweise bieten tokenlose Zwei-Faktor-Authentifizierungsmethoden. Sie beruhen nicht auf gesonderten Hardware-Lösungen, sondern nutzen stattdessen Geräte, die der User bereits besitzt. Das kann z.B. ein Mobiltelefon, ein Smartphone oder ein Tablet-PC sein – unabhängig davon, ob von der Firma zur Verfügung gestellt oder als Privatgerät genutzt. Derartige tokenlose 2FA-Lösungen erfüllen alle Sicherheitsfunktionen von Hardware-Token, zusätzliche Hardware-Anschaffungen sind aber obsolet. Damit wird aus BYOD kurzerhand BYOT: Bring your own Token.

Bislang können sich Nutzer auf zwei unterschiedliche Arten tokenlos authentifizieren: Entweder generiert eine auf dem Gerät installierte Software auf Anfrage neue Passcodes, oder der User erhält seine Zugangsdaten in Echtzeit per SMS. Der Fallstrick der Software-Lösung sind allerdings die vielen verschiedene Mobiltelefontypen und die damit verbundene Vielfalt der Betriebssysteme. In diesem Fall ist nicht nur die Anschaffung kostenintensiv, auch müsste die IT-Abteilung für alle drei Software-Typen geschult sein.

Eine Alternative stellt die Passcode-Zusendung per SMS dar, da die Textnachrichten keinen Übergriff auf persönliches Eigentum darstellen. Die Kehrseite dieser Lösung sind aber die gewünschten Mobilnetzverbindungen in Echtzeit. Ist das Netz gerade in diesem Moment überlastet oder es existiert im schlimmsten Fall aktuell gar keine Mobilfunkverbindung, kommt die SMS nicht an.

Flexibilität ist Trumpf

Für mehr Unabhängigkeit sorgen 2FA-Lösungen wie z.B. SecurAccess flexible Übertragungsmöglichkeiten für Passcodes:

- Vorgeladene (pre-load) SMS: Jede Nutzung eines OTP löst den Versand eines neuen aus, sodass immer ein aktueller Code vorhanden ist.
- Echtzeit-SMS;
- SMS mit drei Codes: Eine SMS erhält drei OTP, genutzte Codes werden innerhalb der gleichen Nachricht dynamisch ersetzt.
- Periodisch gesendete SMS: Die OTPs werden zu einer festgelegten Zeit in einem bestimmten Tagesintervall verschickt. Der aktuelle Code kann mehrfach verwendet werden.

- Soft Token-App für Smartphones: Erhältlich für Geräte mit iOS-, Android-, Windows (7)- oder Blackberry-Betriebssystem. Der Nutzer scannt einen Seed Record mittels eines QR-Codes und erhält daraufhin einen OTP, der alle 30 Sekunden wechselt.
- Soft Token für Laptops (Microsoft/Mac): Die Software generiert beim Anklicken einen OTP, der sich alle 30 Sekunden verändert.
- Voice Call: Der Nutzer gibt zunächst seine PIN oder seinen Passcode ein, anschließend wird ihm ein sechsstelliger Passcode angezeigt. Zur gleichen Zeit wird automatisch ein Anruf initialisiert. Der Nutzer nimmt den Anruf an und gibt den Passcode über die Telefontastatur ein.
- Vorgeladene (pre-load) E-Mail: Funktioniert wie die vorgeladene SMS, Ähnliches gilt für die folgenden drei Varianten
- Echtzeit-E-Mail;
- E-Mail mit drei Codes und
- periodisch gesendete E-Mail.

Auf diese Weise ist der Nutzer besonders flexibel und kann sich an die Gegebenheiten anpassen. Im Falle eines Außendienstmitarbeiters, der immer mal wieder aus der Ferne Unternehmensdaten einsehen muss, lohnt sich z.B. die periodisch gesendete SMS oder E-Mail, da er hier wiederverwendbare Codes zur Verfügung hat. Personal, das sich nur selten remote einloggt oder kein Mobiltelefon besitzt, kann die Voice Call-Methode nutzen. Wer bereits im Voraus weiß, dass er in einer bestimmten Region nur schlechten und keinen Mobilfunkempfang haben wird, kann auf die Drei-Codes-Variante ausweichen, um OTPs auf Vorrat zu haben. Ein Alleinstallungsmerkmal der SecurEnvoy-Technologie ist die Fähigkeit, unter zwei Geräten zu kommunizieren, selbst wenn nur ein Gerät „live“ geschaltet ist.

Im Überblick: Vorteile der tokenlosen 2FA

- Finanzielle Entlastung: 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

- Flexible Übertragungsmöglichkeiten, beispielsweise mittels SMS, E-Mail, Soft Token und Voice Call
- Der Nutzer hat die Wahl und die Kontrolle, was die IT-Abteilung maßgeblich entlastet. Sie legt lediglich die Rahmenbedingungen fest, wie z.B. die Dauer der periodischen Passcode-Aktualisierung u.Ä.
- Die persönliche Konfiguration, wie bei Token nötig, entfällt, was wiederum den Arbeitsaufwand senkt.

Fazit

Mit Hilfe der 2FA können Unternehmen sicherstellen, dass sich ihr Personal eindeutig identifiziert, da nur die korrekte Kombination aus Benutzerdaten und OTP den Login ermöglicht. Das tokenlose Verfahren bietet zudem weitere Vorteile wie z.B. Kostenersparnis, da nicht in gesonderte Token investiert werden muss. Außerdem muss das Personal kein zusätzliches Gerät bei sich tragen, sondern setzt einfach das vorhandene mobile Endgerät ein. Dadurch, dass eine Komponente dem User bekannt sein muss und die andere auf ein Gerät gesendet wird, das nur er besitzt, ist das Authentifizierungsverfahren besonders sicher. Selbst wenn der Mitarbeiter sein Smartphone oder seine Login-Daten verliert oder sie gestohlen werden – alleine sind die jeweiligen Faktoren nutzlos für den Dieb. Unterschiedliche Übertragungsmöglichkeiten sorgen des Weiteren für Flexibilität und ermöglichen die Anpassung an unterschiedliche Arbeitsbedingungen.