ISSN 1021-271X P.B.B ZUL.NR. 02Z031040M – VERLAGSORT WIEN, VERLAGSPOSTAMT 1110 WIEN
AUSGABE 3-2014. Ein Produkt der Bohmann Verlagsgruppe

EUR 5,50
www.monitor.at

Juni 2014

monitor

ÖSTERREICHS IKT-WEGWEISER FÜR KLEINE UND MITTELSTÄNDISCHE UNTERNEHMEN

Grundlagen, Lösungen & Anwendung

ENTERPRISE Content Management

36 Industrie 4.0
Wie die Produktion der Zukunft aussieht und die reelle mit der virtuellen Welt verschmilzt.

50 Ausbildung 2.0
Lernen, was Sie wissen müssen, um die aktuellen IT-Trends in Ihrem Unternehmen erfolgreich einzusetzen.

20 Boost Your Company!
Wie mit der richtigen ECM-Lösung chaotische Datenströme zur produktivitätssteigernden Quelle werden.

Zwei-Faktor-Authentifizierung

Identitätsmanagement 2.0

Wissen Sie noch, wann Sie Ihre letzte Zwei-Faktor-Authentifizierung durchgeführt haben? Vielleicht war es bei der letzten Führerscheinkontrolle, als Sie Ihren Ausweis mit Lichtbild vorzeigen mussten?

Gastkommentar von Robert Korherr, CEO, und Erich Kronfuss, Geschäftsstellenleiter Österreich bei der ProSoft Software Vertriebs GmbH

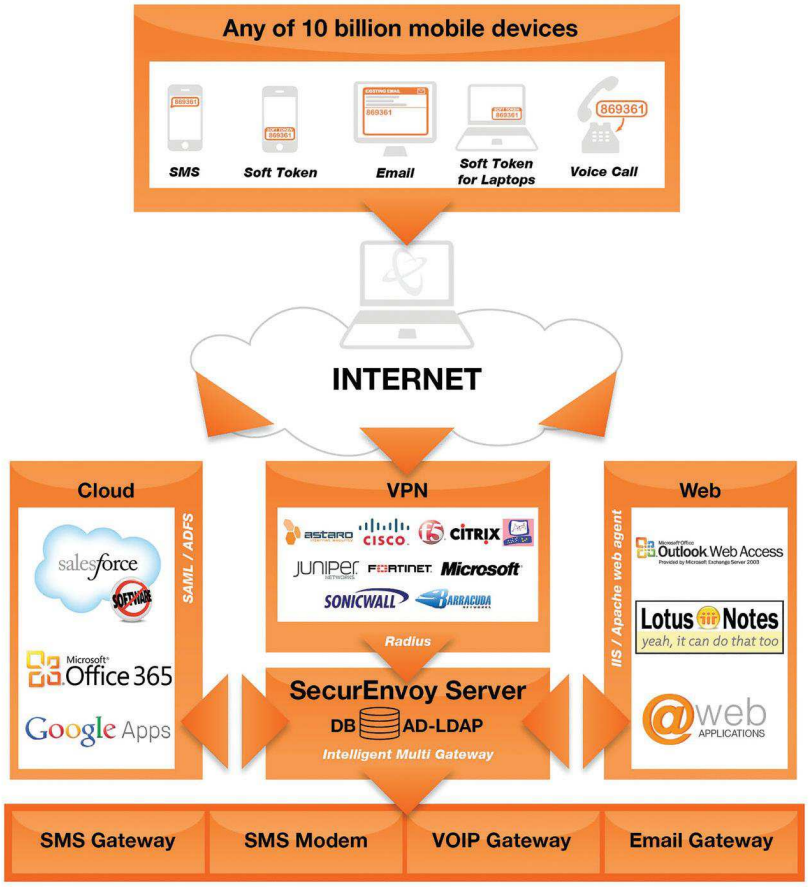

Bild: SecurEnvoy 2014

Eine moderne Zwei-Faktor Authentifizierung wie SecurAccess sollte nicht nur sicher sein, sondern auch verschiedenste Übertragungsmedien online wie offline anbieten.

Der Polizist hat hier nichts anderes getan, als Ihre Identität festzustellen und Sie anhand ihrer Ausweisdaten und des Fotos zu verifizieren. Ganz ähnlich verhält es sich mit der Identifizierung und Authentifizierung für die Zwei-Faktor-Authentifizierung in der IT.

Identifizierung versus Authentifizierung

Die Identität einer Person wird über Merkmale festgestellt, die auf drei Arten nachgewiesen werden:

- durch etwas, dass ich weiß (Geburtsdatum),
- durch etwas, was ich habe (Ausweis),
- und durch etwas, was ich bin (Fingerabdruck).

Die Identifizierung wird im Zusammenhang mit einer Mehr-Faktor-Authentifizierung meist zur Feststellung der Identität einer Person eingesetzt. Hierzu können die drei oben aufgeführten Merkmale genutzt werden. Bei einer Authentifizierung wird die Identität verifiziert, beispielsweise durch den Personalausweis.

Wie funktioniert eine Zwei-Faktor-Authentifizierung im Alltag?

In vielen Haushalten kommt die Zwei-Faktor- Authentifizierung bereits beim Online-Banking zum Einsatz. Hier muss der Anwender zunächst auf der Webseite seinen Benutzernamen und sein Passwort eingeben, um daraufhin eine SMS auf sein Mobilfunkgerät gesendet zu bekommen. Mit diesem Einmal-Passwort findet dann die Verifizierung des sich einloggenden Anwenders statt. Banken verhindern damit, dass sich Cyber-Kriminelle in den Anmeldeprozess einschalten, die personenbezogenen Daten kopieren und ungewollte Transaktionen starten.

Zwei-Faktor Authentifizierung im Unternehmenseinsatz

Im Unternehmen findet die Zwei-Faktor-Authentifizierung ebenfalls weite Verbreitung, z. B. bei der morgendlichen Anmeldung am PC. Der Mitarbeiter identifiziert sich über seinen Firmenausweis, um seine Arbeitsstätte zu betreten (1. Faktor, Haben), danach muss er am PC noch ein Passwort eingeben (2. Faktor, Wissen) und erst dann kann er mit der Arbeit beginnen. Müssen sich Mitarbeiter von unterwegs am Firmennetzwerk anmelden, dann ist eine Zwei-Faktor-Authentifizierung noch viel wichtiger, um Datendiebstahl zu verhindern.

Hierbei kann das Identitätsmanagement ähnlich sicher und ebenso komfortabel funktionieren. Aktuelle Lösungen nutzen vorhandene Geräte wie das Handy oder Tablets zur Authentifizierung. Die „tokenlose" Zwei-Faktor-Authentifizierung, verzichtet auf den Einsatz von zusätzlichen Hardware-Token, was das IT-Budget entlastet und den administrativen Aufwand deutlich reduziert.

Anwendungsfall Außendienst

In vielen Unternehmen hat sich der Vertrieb den geänderten Anforderungen des Marktes angepasst und erfordert mehr Flexibilität und Mobilität. Dazu gehört auch, dass Vertriebsmitarbeiter sich von unterwegs sicher ins Unternehmensnetzwerk einwählen müssen, um Daten abzurufen oder zu synchronisieren. Dabei werden auch fast immer sensible Daten ausgetauscht, und das entweder über offene und damit unsichere WLAN-Hot-Spots oder ungesicherte Internetverbindungen. Bei diesem Vorgang sorgt eine Zwei-Faktor-Authentifizierung für mehr Sicherheit, wenn das Einmal-Kennwort als SMS geliefert wird. Hacker, die Daten abfangen wollen, müssten sich Zugriff auf das Mobilfunkgerät und auf den Laptop verschaffen, mit dem sich gerade ins Unternehmensnetzwerk eingewählt wird. Cyber-Kriminelle müssten dann etwas „Haben" und zugleich etwas „Wissen".

Anwendungsfall Mitarbeiter im IT-Service

Wie wichtig Flexibilität bei einer Zwei-Faktor-Authentifizierung ist, zeigt ein anderes Beispiel: Mitarbeiter im IT-Service arbeiten häufig an Standorten oder in Räumen, wie zum Beispiel einem abgeschotteten Serverraum, ohne eine stabile Funkverbindung. Trotzdem ist der Remote-Zugriff auf Kundendaten oder auf Anleitungen notwendig. Hier ist eine flexible Zwei-Faktor-Authentifizierung gefragt. Die Flexibilität besteht darin, dass mehrere Authentifizierungsmöglichkeiten zur Verfügung stehen und bedarfsgerecht zum Beispiel über ein Webportal ausgewählt werden können. Ist die Funknetzverbindung meist nur kurzfristig unterbrochen, können vorab gelieferte SMS-Einmal-Passwörter ausreichend sein. Bei der Lösung SecurAccess beispielsweise kann der Nutzer zwischen einer und drei vorab gelieferten SMS-Passcodes wählen. Bei einer erneuten GSM-Verbindung werden genutzte Passcodes automatisch aktualisiert. Bei Terminen im Ausland kann der User auf die Soft-Token-App wechseln und damit über sein Smartphone oder Tablet das Einmal-Passwort sicher generieren, ohne zusätzlich Kosten zu verursachen. Genau wie beim Beispiel zuvor müssen Cyber-Kriminelle sowohl etwas „Haben" als auch etwas „Wissen", um Einwahldaten abzufangen und sensible Daten stehlen zu können.

Anforderungen an eine moderne Zwei-Faktor-Authentifizierung

Die hier aufgeführten Beispiele zeigen, dass eine moderne Zwei-Faktor-Authentifizierung nicht nur Sicherheit bieten, sondern sich an die jeweiligen Situationen anpassen muss. Daraus lassen sich verschiedene Anforderungen ableiten: Lösungen, die unter dem Motto „Bring your own Token (BYOT)" arbeiten, benötigen keine zusätzliche Hardware, sondern nutzen vorhandene Formfaktoren, z. B. die Smartphones der Mitarbeiter. Außerdem sollten mehrere Online- oder Offline-Verfahren vorgehalten und vom User bedarfsgerecht ausgewählt werden können. Der zeitnahe Empfang einer SMS ist zwar ziemlich sicher, aber es gibt immer wieder Situationen, in denen eine Alternative zum SMS-Empfang notwendig oder gewünscht ist. Lösungen, die keine Alternativen anbieten, sind im Alltag nicht sinnvoll. Neben einem SMS-One-Time-Password (OTP) gibt es Soft-Token, die Nutzung normaler Telefone zum Beispiel für Home-Offices sowie Photo-Passcodes, die ähnlich wie beim Online-Banking einen QR-Code abfotografieren und daraus das Einmal-Passwort generieren. Vor Brute-Force-Attacken, Phishing oder Man-in-the-Middle-Angriffen schützt das Verfahren, wenn zum einen die Übertragung verschlüsselt wird und zum anderen die Einmal-Passwörter sitzungsbasiert sind. Dieses Kennwort ist dann nur für die ursprüngliche Sitzungs-ID gültig.

Fazit

Die Sicherheit beim Remote-Access beginnt nicht erst beim Aufbau einer gesicherten Verbindung, zum Beispiel über VPN. Bereits die „Tür" gilt es zu sichern, also Verbindungen in Firmennetzwerke, Web- oder Cloud-Applikationen und die dort gespeicherten Daten müssen ausreichend abgesichert sein. Hierbei geht es nicht nur um die Verhinderung von Spionage bzw. Wirtschaftsspionage ausländischer Geheimdienste. Für jedes Unternehmen, auch für KMU ist der Schutz von digitalen Identitäten, die zunehmend von Cyberkriminellen kommerziell genutzt werden, immer wichtiger.

Auf keinen Fall sollte man bei der IT-Sicherheit resignieren. Bei Fernzugriffen auf Firmendaten gibt es mit der „tokenlosen" Zwei-Faktor-Authentifizierung eine sichere Lösung, die für 1–2 Euro pro Monat ungebetene Zugriffe wirkungsvoll unterbindet. Außerdem integriert sie sich nahtlos in alle gängigen Remote-Access-Plattformen, kann meist flexibel eingesetzt werden und erzeugt nur minimalen Administrationsaufwand, gewährt dafür aber hohe Sicherheit und Schutz vor Datendiebstahl.

Datensicherheit in der Cloud mit Dextra Data

Die Dextra Data Solutions GmbH setzt im Bereich Cloud-Services für den sicheren Login und die Einhaltung von Compliance auf die Zwei-Faktor-Authentifizierung „SecurAccess" von SecurEnvoy. Gegründet im Jahr 2012 von CEO Ing. Günter Handl bietet das Unternehmen seinen vor allem mittelständischen Kunden Cloud-Lösungen und Managed Services und plant, installiert und wartet IT-Solutions. Entschieden hat sich der Dienstleister für die Zwei-Faktor Authentifizierung, um seinen Kunden ein unkompliziertes und zukunftssicheres Cloud-Computing-System zur Datensicherung zur Verfügung zu stellen. Die größere Sicherheit stellt eine klare Differenzierung zu anderen Anbietern im Markt dar und gleichzeitig erfüllt der Dienstleister damit seine Sorgfaltspflicht gegenüber seinen Kunden.

www.dextra-data.at