Bildquelle: Fotolia

DOSSIER SICHERHEIT
IN KOOPERATION MIT BOLL ENGINEERING

Benutzername und Passwort sind nicht genug

Je mehr Prozesse in die Wolke verlagert werden, umso grösser wird die Menge an schützenswerten Daten, die übers Netz zirkulieren. Deshalb werden sichere Verfahren zur Zugangskontrolle immer wichtiger. Filip Zirin

Mit der Verlagerung von Geschäftsprozessen, Dienstleistungen und Anwendungen in die Cloud wird die sichere Authentifizierung immer wichtiger. In einem solchen Szenario gilt es, den Zugriff auf Dienste und Ressourcen sauber zu regeln. Und weil mit den Anwendungen auch vertrauliche Daten ins Internet abwandern, muss der Datenschutz auf ein angemessenes Niveau gehoben werden. Der Trend zu «bring your own device» verstärkt das Bedürfnis nach einfachen und zuverlässigen Authentifizierungsverfahren noch zusätzlich.

Das Log-in mittels Benutzername und Kennwort stammt aus einer Zeit, als die Internetnutzer noch nicht viel zu verlieren hatten. Eine solche zweistufige Authentifizierung wird aber der Bedeutung des Internets für die Abwicklung von Geschäftsprozessen längst nicht mehr gerecht. Hier werden stärkere Verfahren benötigt, denn die Hacker von früher haben nichts mit den Internetkriminellen von heute zu tun, denen es bei ihren Angriffen vor allem ums grosse Geld geht. Um den heutigen Sicherheitsbedürfnissen gerecht zu werden, werden vermehrt Verfahren der «Multi Factor Authentication» eingesetzt. Dabei wird neben Benutzername und Passwort eine zusätzliche Sicherheitsschranke beispielsweise in Form eines Einmalpassworts verwendet. Das wiederum wird durch Hardware- oder Software-Tokens dynamisch und zeitbasiert generiert. Diese aus dem Onlinebanking bekannten Verfahren sind heute Stand der Technik und zu vernünftigen Kosten zu haben. Die grosse Herausforderung wird sein, die Sicherheitslösungen einfach und schnell in bestehende Umgebungen und Applikationen einzubinden. Nur wenn eine sichere Authentifizierung gewährleistet ist, werden sich Trends wie Cloud Computing durchsetzen. <

> **Seite 26**
Starke Authentisierung als Notwendigkeit

> **Seite 28**
Beat Zuberbühler, ASGA: «Für uns war schnell klar, dass wir eine Lösung mit Hardware-Token bevorzugen»

Starke Authentisierung als Notwendigkeit

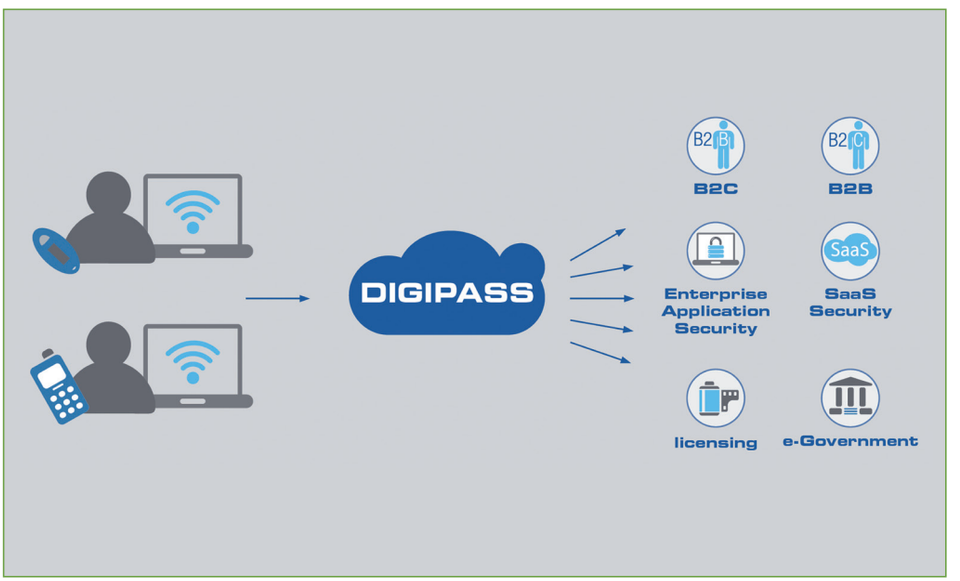
Im Bestreben, den Zugriff auf Daten und Applikationen wirksam zu schützen und zugriffsberechtigte Personen bei deren Anmeldung sicher zu authentisieren, setzen Unternehmen vermehrt auf die sogenannte «Multi Factor Authentication». Thomas Boll

Wirtschaftsspionage, gezielte Attacken auf IT-Ressourcen, Datenklau ... die Liste aktueller Bedrohungen liesse sich beliebig fortsetzen. Sie begründet die Anstrengungen einer wachsenden Zahl von Unternehmen, den Zugriff auf Netzwerke, Webanwendungen, Daten und Applikationen zu schützen. Dabei setzen sie vermehrt auf eine hochsichere Zwei-Faktoren-Authentisierung. Dies vor dem Hintergrund, dass für viele Anwendungen die Sicherheit, die durch die Kombination aus Benutzername und Kennwort erreicht wird, nicht ausreicht. Erst durch den Einsatz zusätzlicher Komponenten – in der Regel Hardware-OTP-Token (One Time Password) beziehungsweise elektronische TAN-Listen (Transaktionsnummer) – wird der benötigte Schutz gewährt. OTP-Token generieren auf Knopfdruck dynamische, zeitbasierende Einmalpasswörter, die zur Anmeldung an die jeweilige Applikation genutzt werden und mittels derer sich elektronische Signaturen absichern und validieren lassen. Sie machen den unerlaubten Zugriff auf Netzwerk und Applikationen durch Dritte weitgehend unmöglich, da für die Anmeldung eine Kombination aus Wissen (Zugangsdaten) und Besitz (Token) erforderlich ist.

Einen ebenso wichtigen Beitrag zur sicheren Authentisierung und zur Einbindung wirksamer Log-in-Prozeduren leisten Smart Cards, aktive und passive Proximity Cards sowie biometrische Verfahren wie etwa Fingerprint. Sie gewährleisten eine sichere und höchst komfortable Benutzer-Identifizierung.

Ganzheitliche Integration

Zur nahtlosen Einbindung einer umfassenden «Multi Factor Authentication» stellen die in diesem Bereich tätigen Lösungsanbieter entsprechende Authentisierungs- und E-Signatur-Plattformen zur Verfügung – in der Regel mit «Windows Server 2008»-Support und AD-Integration (Active Directory). Diese eignen sich für sämtliche denkbaren Applikationen, die auf eine starke Authentisierung angewiesen sind, und sorgen dafür, dass ausschliesslich befugte Personen Zugriff auf sensitive Daten und Anwendungen wie beispielsweise Onlinebanking und «Software-as-a-Service» (SaaS) oder auf ERP- und E-Health-Lösungen erhalten. Zudem bieten sie Schutz für webbasierte Anwendungen und ermöglichen eine hochgradige Sicherung von VPN-Zugängen ins Firmennetzwerk.



Auch als Cloud-Service erhältlich: «Multi Factor Authentication». Bildquelle: Boll Engineering

Trotz hoher Komplexität lassen sich fortschrittliche Enterprise-Lösungen einfach und schnell in bestehende Umgebungen und Applikationen einbinden. Die von Vasco erhältliche Plattform «Identikey» beispielsweise stellt dazu komfortable «Plug and play»-Funktionalitäten zur Verfügung und unterstützt sowohl Radius- als auch Web- und SOAP-Schnittstellen. Dabei lässt sich der Datenspeicher in Active-Directory- oder ODBC-Datenbanken integrieren. Ob als reine Softwarelösung oder als leistungsfähige Appliance – beide Varianten ermöglichen ein zentralisiertes, komfortables User-Management. So steht dem Administrator eine einheitliche Konsole für Funktionen wie Benutzerverwaltung, Token-Management, Auditing und Reports zur Verfügung.

Unterschiedlich die Bedürfnisse – variantenreich die Lösungen

Der Bedarf an einer starken «Multi Factor Authentication» ist in unterschiedlichsten Anwendungsbereichen manifest. Dazu gehören Windows-Log-on und Remote-Zugriffe aufs Firmennetzwerk via VPN ebenso wie die Einbindung mobiler Devices, die Absicherung von Webanwendungen oder der wirksame Schutz von Cloud-Services. Neben den etablierten, «klassischen» OTP-Anmeldeverfahren machen vermehrt auch folgende Methoden von sich reden:

- **Offline-Authentisierung**
  Ob Kundendaten oder Preislisten, Projektunterlagen oder Finanzzahlen – der Speicherung vertraulicher Informationen auf Notebooks sind kaum Grenzen gesetzt. Folglich gilt es, die Daten selbst sowie den Informationszugriff im Offlinemodus zu sichern. Entsprechende Lösungen erlauben einerseits, Computer zu sperren sowie einzelne Dateien oder ganze Festplatten zu verschlüsseln. Andererseits

Thomas Boll ist Geschäftsführer der Boll Engineering.

bieten sie die Möglichkeit, One-Time-Passwörter offline einzusetzen und über dieselbe Plattform PKI-Funktionen zu nutzen – beispielsweise für digitale Signaturen oder Datei-Verschlüsselungen. Werden dabei OTP- und PKI-Funktionen über dieselbe Oberfläche gesteuert und nutzen sie dieselbe Authentisierungshardware (Token), lassen sich komplett umfassende Authentisierungs- und Signaturlösungen realisieren, die sowohl den Online- als auch den Offlinebetrieb unterstützen.

- **Einbindung mobiler Devices**
  Um den Zugang zum Firmennetzwerk mit einer zeitgemässen Zwei-Wege-Authentisierung abzusichern, sind nicht mehr zwingend spezifische Hardware-Token oder Programme auf den Endgeräten notwendig. Stattdessen stehen heute für Smartphones (zum Beispiel iPhone oder Blackberry) sowie für javabasierte Mobile-Phones entsprechende Softwarelösungen zur Verfügung. Deren Einbindung ist denkbar einfach. So stehen für den Rollout beziehungsweise Download der schlanken Applikationen komfortable «Application Provisioning Services» zur Verfügung. Übermittelt die berechtigte Person ihre Handynummer an den Server, erhält sie anschliessend eine SMS, mit deren Hilfe sie die Authentisierungssoftware verschlüsselt downloaden kann. Nach erfolgtem Download und der Installation der Applikation kann deren Aktivierung bei der IT-Abteilung angefordert werden.
- **Cloud-Services mit «virtuellen» Token**
  Obwohl der Bedarf erkannt wird, scheuen vereinzelte Firmen die Einführung einer sicheren Zwei-Faktoren-Authentifizierung. Dies kann sowohl durch die anfallenden Kosten als auch durch installationstechnische Fragen begründet sein. Um diesen Umständen Rechnung zu tragen, bieten einzelne Lösungsanbieter entsprechende auf Cloud basierende Authentifizierungsservices für Internetapplikationen an. Sie kümmern sich um den gesamten Authentifizierungsprozess, während sich der B-to-B- oder B-to-C-Provider ganz seinem Kerngeschäft widmen kann.

«Digipass Nano» macht aus jedem Mobile-Phone eine hoch sichere OTP-Plattform. Bildquelle: Boll Engineering

Von noch grösserer Relevanz sind die Aufwendungen, um die Authentisierungshardware (Token) an die Endanwender zu verteilen. Dies ist namentlich bei Webanwendungen der Fall, die sich an eine weit gefächerte Kundschaft richten. Vor diesem Hintergrund ist die Einbindung «virtueller Token» von besonderer Bedeutung. Diese machen das Vorhandensein eines physischen Tokens für eine sichere «Multi Factor Authentication» überflüssig. Demnach übermittelt der Authentifizierungsserver das für den Log-in-Prozess benötigte zeitabhängige Einmalpasswort via SMS an den User. Dank der Verwendung eines zweiten Kommunikationskanals wird ein Höchstmass an Sicherheit erreicht. Die Einbindung virtueller Token ermöglicht die Absicherung von Webanwendungen, die bisher aus logistischen und Kostengründen auf eine starke Authentisierung verzichten mussten. <

DIGIPASS NANO – HANDY WIRD ZUM NICHT KNACKBAREN AUTHENTISIERUNGSGERÄT

Mit ihrer kürzlich vorgestellten Lösung «Digipass Nano» lanciert der europäische Security-Spezialist Vasco einen neuen Sicherheits-Layer, der Mobiltelefone zum Authentisierungsgerät wandelt. Die Lösung besteht aus einer dünnen Folie mit integriertem Sicherheits-Chip. Sie wird auf die SIM-Karte des Mobiltelefons beziehungsweise PDAs gelegt und gemeinsam ins Handy eingeschoben. Dadurch wird das Mobiltelefon in die Lage versetzt, Einmal-Passwörter (OTPs) und digitale Signaturen zu erzeugen. Endanwender können sich damit zuverlässig authentisieren und Dokumente oder Transaktionen digital signieren. Ohne dass dazu kundenseitig spezifische Token notwendig wären, lassen sich Anwendungen wie Zugangskontrolle auf Daten und Applikationen, sicheres Log-in für Remote-Arbeitsplätze, Absicherung elektronischer Finanztransaktionen oder Signatur und Verschlüsselung anderer vertraulicher Transaktionen absichern. Da es sich bei Digipass Nano um eine SIM-Anwendung handelt, ist die dazu eingesetzte Sicherheitshardware für Hacker unangreifbar. Sie bietet folglich einen Sicherheitsstandard, wie er bei softwarebasierten Lösungen nicht möglich ist. Digipass Nano ist unabhängig vom jeweiligen Provider einsetzbar, benötigt keine Anmeldung und tangiert die übrigen Funktionen des Mobiltelefons nicht. Zudem lässt sich die Lösung unabhängig von Hardware und Betriebssystem des Mobiltelefons einsetzen.

«Für uns war schnell klar, dass wir eine Lösung mit Hardware-Token bevorzugen»

Die unabhängige Pensionskasse ASGA hat für ihre Mitgliedfirmen eine Onlineplattform eingerichtet, über die sie Daten der Versicherten einsehen und mutieren können. Die Netzwoche sprach mit dem Informatikchef Beat Zuberbühler über die Vorteile eines solchen Angebots, über Datensicherheit und Umsetzung. Interview: René Mosbacher

Herr Zuberbühler, was hat die ASGA bewogen, ein Onlineportal für ihre Kunden anzubieten?
Mit «ASGAonline» wollen wir den Kunden eine zusätzliche Dienstleistung anbieten und auch unsere internen Prozesse optimieren. Zudem glauben wir, dass wir mit einem solchen Angebot unsere Stellung im Markt stärken können. Damit ermöglichen wir den Kunden unter anderem, Mutationen direkt am Bildschirm statt auf Papier über den Postweg zu erledigen. Das geht viel schneller und spart Kosten. Um Ihnen eine Grössenordnung zu geben: Wir haben 9200 Mitgliedfirmen mit insgesamt 70 000 Versicherten. Pro Jahr kommen so 120 000 bis 130 000 Mutationen zusammen. Wir hatten zwar schon PDF-Formulare auf der Website, die man am Bildschirm ausfüllen, ausdrucken und uns zuschicken konnte. Solche Papierdokumente müssen jeweils unterschrieben werden, damit sie gültig sind. Das ist umständlich und der Wunsch nach einer medienbruchfreien Verarbeitung nur logisch. Eine Voraussetzung hierfür ist natürlich eine sichere Authentifizierungslösung.

Wie ist das Portal bei Ihren Kunden angekommen?
Seit der Lancierung im September 2010 haben sich 2300 der 9200 Mitgliedfirmen für die Nutzung des Portals entschieden. Die Feedbacks waren mehrheitlich positiv – aber klar, das Angebot ist noch verbesserungs- und ausbaufähig. Wir sammeln die Anregungen von Kunden und wollen sie in den kommenden Versionen, so weit möglich, einfliessen lassen.

Kommen die Kunden mit der Authentifizierung zurecht?
Der Umgang mit dem Token ist den meisten Kunden ja schon vom Internetbanking her bekannt – entsprechend problemlos gestaltete sich die Einführung.

Was brauchte es auf Ihrer Seite für Anpassungen, um das Portal zu realisieren?
Wir hatten das Ziel, dass die mutierten Datensätze nahtlos in die Kernapplikation einfliessen sollen. Bis zu einem gewissen Grad wurden Abläufe auch automatisiert. Das erforderte selbstverständlich grössere Anpassungen bei den Geschäftsprozessen.


Beat Zuberbühler ist Leiter Informatik bei der unabhängigen Pensionskasse ASGA.

Was haben Sie selbst gemacht und was an Partner delegiert?
Die Softwareentwicklung lag bei unserem Partner, von dem auch die Kernapplikation stammt. Für die Implementierung der Security-Lösung war die 4net AG zuständig. Unsere Aufgaben waren im Wesentlichen die Koordination zwischen den Partnern, die Modellierung der Geschäftsprozesse und -vorfälle, das Layout des Portals und der Aufbau der Testumgebung. Auch die Kommunikation mit unseren Mitgliedern haben wir selbst gemacht.

Läuft das Portal auf Ihren Servern oder ist es ausgelagert?
Die Kernapplikation läuft inhouse. Die Webapplikation und die Security-Lösung haben wir zu 4net ausgelagert.

Es gibt ja verschiedene Lösungen für eine sichere Authentifizierung – warum haben Sie sich für ein System mit Hardware-Token entschieden?
Für uns war schnell klar, dass wir eine Lösung mit Hardware-Token bevorzugen, schon allein deshalb, weil wir vermeiden wollten, dass die Kunden zusätzliche Software installieren müssen, um das Portal nutzen zu können. Wir haben verschiedene Security-Anbieter evaluiert und sind am Ende beim Hersteller Vasco gelandet, weil uns die Produkte bezüglich Technik, Integration und Betriebskosten überzeugt haben. Im Übrigen wollten wir einfach eine stabile und bewährte Lösung.

Was haben Sie aus dem Projekt gelernt, was würden Sie anders machen?
Wir haben sehr viel gelernt – beispielsweise, dass der zeitliche Aufwand für ein solches Projekt nicht unterschätzt werden sollte. So war die Umsetzung des Portals auf der Basis von Silverlight einiges aufwendiger als ursprünglich erwartet. Das führte zu Zeitdruck und belastete einzelne Mitwirkende wohl eher etwas über Gebühr. Technisch hingegen würden wir aber alles wieder so machen. Die Integration der Security-Lösung ging zügig und ohne grössere Probleme vonstatten. Was wir nicht erwartet hatten, war das enorme Interesse unserer Kunden. Wir konnten den Ansturm nur bewältigen, indem wir für die ganze Anmeldeprozedur samt Versand des Token deutlich mehr Personal einsetzten als geplant.

Was empfehlen Sie anderen Pensionskassen?
Wer ein Kundenportal lancieren will, sollte daran denken, dass es sich bei der zweiten Säule um eine etwas abstrakte Materie handelt. Speziell Sachbearbeiter von KMUs befassen sich meist nur ein- bis zweimal im Jahr damit. Da entsteht natürlich keine Routine. Deshalb sollte die Bedienung einfach und logisch sein. Hinsichtlich der Sicherheit empfehle ich unbedingt eine dreistufige Authentifizierung. Das ist Stand der Technik, hat sich bewährt und ist heute durchaus bezahlbar. Selbstverständlich müssen die Daten, die übers öffentliche Netz geschickt werden, verschlüsselt sein.

Können Sie noch etwas über Aufwand und Ertrag aus Sicht der ASGA sagen?
Eigentlich lässt sich darüber nichts Konkretes sagen. Wir bieten das Portal unseren Kunden als kostenlose Zusatzleistung an und generieren keine Erlöse damit. Deshalb gliche eine Kosten-Nutzen-Rechnung einer Zahlenspielerei. Je nach Anzahl Mutationen beispielsweise, die zugrunde liegen, bekommt man völlig andere Amortisationszeiten. Selbstverständlich profitieren wir intern auch von der effizienteren Verarbeitung, aber bis zu einem gewissen Grad handelt es sich bei der Plattform um eine strategische Investition. <