

„Starke Authentisierung“: Schonfrist definitiv vorbei

Die Sicherheit im Internet rückt auch in Österreich immer stärker ins öffentliche Bewusstsein. Unter anderem wird in Fachkreisen unter dem Oberbegriff „Identity and Access Management“ intensiv diskutiert, ob Schutzmaßnahmen wie „Zwei-Faktor-Authentisierung“ heute noch genügen.

Urs Zurbuchen

Wenn Vertreter der IT-Security-Branche vermehrt Sicherheit anmahnen, könnte man das als Laie unter Umständen noch im Bereich Eigeninteresse ansiedeln. Doch wenn sich die Meldungen in den Medien über die Sicherheit im Internet - insbesondere beim E-Banking und bei E-Shops - häufen, das öffentlich Bewusstsein erwacht und sich sogar die Rechtsprechung vermehrt dem Thema annimmt, weiß man: Jetzt geht's ans Eingemachte.

Die Kadenz der Meldungen und das Ausmaß der Bedrohung haben allein schon in den letzten Monaten spürbar zugenommen. Metapher bieten sich geradezu an. Manche behaupten, das Internet als Kontakt-, Informations- und Shoppingparadies bekomme immer mehr den Charakter eines Dschungels. Im Gegensatz zu real existierenden Urwäldern, wo Raubtiere immer mehr unter Druck geraten, haben reißende Tiere in der freien Internet-Wildbahn ganz offensichtlich ihre „ökologischen Nischen“ gefunden. Es wimmelt von Phishing-Hyänen und Malware-Schlangen.

Oder man bemüht das Vokabular der Kriegskunst. Auf Angriff folgt Verteidigung. Und auf eine erfolgreiche Verteidigung folgt ein neuer, andersartiger Angriff. Diese auch auf dem „Internet-Schlachtfeld“ zu beobachtende Dynamik, erinnert an einen Begriff aus dem kalten Krieg, den wir eigentlich alle gerne nur noch in Werken zur Zeitgeschichte lesen würden: das Wettrüsten.

Doch wohlgemerkt: Es geht nicht um Panikmache, sondern einfach darum, den Tatsachen ins Auge zu schauen und praxisorientierte Vorbeuge- und Abwehrmaßnahmen zu entwickeln. Denn es gibt wirksame Instrumente. Entsprechendes Gewicht erhält



Authentisierungstrends: Woher weht der Wind?

der vielschichtige Bereich „Identity and Access Management“ (IAM). Die grundlegende Mission des IAM ist, einen kontrollierten Zugriff auf Informationsressourcen und Anwendungen zu ermöglichen.

Wahrnehmung in Österreich verstärkt

IAM bzw. Identity Management wird ebenfalls in einer eben erschienenen, vom Austrian Security Forum (ASF) initiierten Studie zum IT-Security-Markt Österreich als eines der drei wichtigsten Themen der Zukunft aufgeführt. Als Initiative mit Breitenwirkung darf auch die „Internetoffensive Österreich“ nicht ungenannt bleiben, insbesondere der Arbeitskreis „Sicherheit und Konsumentenschutz“.

Ohne Zweifel werden die Ausgaben für IT-Sicherheit im Allgemeinen und für Maßnahmen gegen Phishing, d. h. E-Mail-Security und Malware im Speziellen in den nächsten Jahren signifikant zunehmen. Allein für 2009 rechnet die erwähnte Studie mit einem Wachstum des IT-Security

Marktvolumens in Österreich von 16%.

Die springende Frage für die Entscheider: In welche Technologien bzw. Lösungen soll investiert werden? Oder anders gefragt: Welche Systeme genügen, und wohin geht die Entwicklung?

Online-Banking stark gefordert

Es gibt wohl kaum eine Branche, in der diese brennenden Fragen intensiver diskutiert werden als im Finanzbereich, besonders beim Online-Banking. Der Druck kommt von allen Seiten: Berichte über Identitätsdiebstahl (Phishing) oder kriminelle Umleitung von Überweisungen (z. B. mittels Trojaner) verunsichern generell die Kundschaft und fügen betroffenen Banken erheblichen Imageschaden zu - ganz zu schweigen von konkreten rechtlichen Forderungen (vermutlich ist die Dunkelziffer bei den Schadenssummen hoch). Ferner müssen Banken unter dem Stichwort „Compliance“ immer mehr und immer strengeren nationalen, europäischen und internationalen Normen ge-

nügen. Da sich das Online-Banking in der Bevölkerung zur gängigen Praxis entwickelt hat, sind die Banken gefordert, Lösungen anzubieten, die sich breit anwenden lassen. Auch hier geht es ums Abwägen - wie eigentlich immer in der IT-Security. Die Systeme haben einfach einsetzbar und bezahlbar zu sein und ein angemessenes Maß an Sicherheit zu bieten. Es können also keine Maximallösungen sein, die zu teuer sind oder die Geschäftsprozesse bzw. den Kundenkomfort behindern. Integraler Bestandteil aller Lösungen ist der Themenkomplex „Authentisierung“ oder „starke Authentisierung“.

Begriffsvielfalt

Wie so oft werden auch hier die Begriffe nicht immer einheitlich verwendet. Es wird von Authentisierung, Authentifizierung oder gar Authentikation gesprochen. Für manche Fachleute haben die Begriffe sehr wohl unterschiedliche Bedeutungen. Streng genommen verwenden sie die Authentisierung als Vorlage eines Nachweises zur Identifikation und die Authentifizierung als Überprüfung dieses Nachweises. Glücklicherweise sind da die Englischsprachigen: In ihrer Sprache kennt man keine Unterscheidung, man spricht einfach von „authentication“ oder eben „strong authentication“.

Der weit verbreiteten Praxis entsprechend wird an dieser Stelle der Begriff Authentisierung im weitesten Sinne als Verifikation der Identität einer Person (oder eines Objekts) eingesetzt. Die methodischen Grundlagen der Authentisierung sind allgemein bekannt und bewegen sich in den Bereichen Wissen (das Subjekt weiß etwas, z. B. ein Passwort), Besitz (das Subjekt hat etwas, z. B. einen Schlüssel) und Biometrie (das Subjekt bzw. eines seiner Merkmale ist anwesend, z. B. Fingerabdruck). Bei einer Kombination von zwei Methoden spricht man von Zwei-Faktor-Authentisierung, was zum Teil auch mit „starker Authentisierung“ gleichgesetzt

wird, was aber irreführend sein kann, da man auch die Drei-Faktor-Authentisierung kennt.

Die Frage der Authentisierungsstärke

Die „Stärke“ einer Authentisierung bezieht sich auf den Grad der Sicherheit in der Identitätsfeststellung. Sie wird über spezielle Authentisierungssysteme wie Identity Management Server, Authentication Server oder Web Application Firewall erreicht.

Starke Authentisierung ist heute im Banking ein unbestrittenes Muss. Weil sich aber die Bedrohungslage durch die Verbreitung von Malware verschärft hat, vertreten viele die Meinung, dass eine Zwei-Faktor-Authentisierung nicht mehr ausreicht.

In diesem Zusammenhang ist kürzlich eine Schweizer Bank dazu übergegangen, das bisherige zweistufige Login-Verfahren durch den Einsatz einer Chipkarte mit PIN-Code und einem USB-Stick zu ersetzen. Der USB-Stick enthält einen eigens konzipierten Browser als Alternative zum Browser, der fest auf dem Computer des Benutzers installiert ist. Das ist immerhin eine Erhöhung der Sicherheit, doch auch diese Lösung kann grundsätzlich vom Angreifer, der sich be-

Magr. **Urs Zurbuchen** ist Business Engineer bei der Schweizer United Security Providers AG. Das Unternehmen ist auch in Österreich aktiv und offen für Partnerschaften.
www.united-security-providers.ch



reits im Computer eingestiegen hat, umgangen werden. Das Grundproblem liegt in der Natur der Malware, das an zwei Fronten angreift:

Einerseits werden via E-Mail Sicherheitslücken auf Betriebssystem- oder Applikationsebene genutzt, um infizierte Attachments oder Links zu präparierten Webseiten auf dem Kundenrechner einzunisten. Andererseits zielt die Malware auf den Browser. Dabei verändern Angreifer Kontonummer, Empfängername und Betrag noch bevor die eigentlichen Transaktionsangaben des Benutzers verschlüsselt an die Bank gelangen. Selbst die Bestätigung der Bank wird mit der Malware abgefangen und im Browser manipuliert angezeigt.



WIR SORGEN FÜR SICHERHEIT

Ein Stromausfall oder Schwankungen in der Netzversorgung können zu Systemstörungen, Datenverlusten oder zu noch schlimmeren Schäden führen. Die einfachste und effektivste Möglichkeit diese Störungen zu vermeiden, ist der Einsatz einer USV-Anlage (**Unterbrechungsfreie Stromversorgung**). Wir gewährleisten mit USV-Anlagen von Aros Ihre sichere Stromversorgung. **Jetzt neu:** Sentinel XR 3,3 – 10kVA als Stand- oder 19" Zoll Gerät einsetzbar. **Weil Systemwissen entscheidet.**

SCHMACHTL
A-1230 Wien, Kolpingstraße 15 Tel.: (01) 6162180-23
Fax: (01) 6162180-99 E-Mail: usv@schmachtl.at
www.schmachtl.at/usv

Neue Wege gehen

Da sich diese Trojaner weder durch SSL-Verschlüsselung noch durch starke Authentisierung blockieren lassen, verfolgt die Transaktionsverifikation einen anderen Ansatz. Vereinfacht ausgedrückt werden dabei dem Benutzer sensible Transaktionen über ein zweites, unabhängiges Medium vorgelegt. Das kann (kostengünstig) über das Mobile Phone mittels SMS oder über ein spezielles Stand-alone Token geschehen.

Abgesehen von konkreten Systemevaluations müssen heute Banken und E-Commerce-Anwender wie E-Shops beim Thema Authentisierung Grundsätzliches berücksichtigen. Zum Beispiel die Entwicklung umfassender, in die übergeordneten Security-Richtlinien eingeordnete IAM-Konzepte sowie Web Application Server, die eine offene Basis bieten für neue Wege wie die Transaktionsverifikation. □