

Vertrauliche Daten müssen durch geeignete IT-Security **vor Angriffen geschützt werden.**



BILD: ISTOCKPHOTO

VERSICHERUNGS-IT

Gemeinsames Verständnis

Neue Endgeräte schaffen auch hier neue Herausforderungen für die **Datensicherheit.**

MATTHIAS NIKLOWITZ

Die Kollegen der Abteilungen sehen uns morgens arbeiten, sie sehen uns abends arbeiten und sie sehen uns nachts arbeiten», sagt ein IT-Verantwortlicher einer Versicherung im vertraulichen Gespräch, «aber wir schlagen uns nur mit den allerwichtigsten Sachen herum, zumal die Applikationsentwickler keinen ihrer Schritte dokumentieren».

Versicherungen zählen laut dem Lagebericht 2010 der Melde- und Analysestelle Informationssicherung MELANI zur «kritischen Infrastruktur». Ein Ausfall der Versicherungs-IT würde in der Schweiz «massive Auswirkungen auf die nationale Sicherheit oder die ökonomische und/oder soziale Wohlfahrt» haben, wie es in dem Bericht heisst.

Heikle Insider-Informationen

Über die konkreten Schritte zur Sicherheitssteigerung bei der IT schweigen sich Versicherungen – wie auch

Banken – aus. Etliche Hinweise kommen aus den MELANI-Berichten. So haben viele Versicherungen ihre Zugänge auf Social-Webseiten wie Facebook gesperrt, um Social-Engineering-Angriffe zu vermeiden. Solche Massnahmen sind umstritten, weil hier Fragen wie die positiven Auswirkungen auf Arbeitsmoral und Ressourcenverwendung gegen Gefahren wie den Diebstahl von Identitäten oder sensiblen Firmeninformationen gegenübergestellt werden müssen.

Etliche Experten an der RSA-IT-Securitykonferenz, dem grössten Branchenanlass in den USA, wiesen auf die zahlreichen Umgehungsmöglichkeiten solcher Regelungen durch Netbooks oder Tablet-Computer hin. Diese beziehen ihre Daten über Mobilnetze und

umgehen die Firmen-IT vollständig. Zudem sind laut Experten auch Übersetzungsservices heikel. So kam es in etlichen Ländern immer wieder vor, dass Angestellte ganze Vertragspassagen zu Übernahmen, Firmenverkäufen und weiteren Transaktionen einfach rasch abschnittsweise über entsprechende Web-Systeme «übersetzen» liessen.

Auch die US-Börsenaufsicht SEC prüft jetzt Regelungen, um diese Form des Umgangs mit Insider-Informationen zu «handhaben» – und das heisst in der Praxis: Zu unterbinden und im Klagefall mit Geldstrafen belegen zu können. Aber auch kleine Online-Dienste wie der Terminplaner Doodle gelten als heikel und wurden in der Schweiz von einigen Firmen gesperrt, weil Aussenstehende aus bestimmten Einträgen wie «CEO Zurich F.S. trifft CEO Helvetia, 19 Uhr, grosser Sitzungsraum» gewisse Schlüsse ziehen könnten.

Kreis des Vertrauens

Versicherungen sind auch deshalb gefährdet, weil sie laut einer Studie von Accenture zu den grossen Kunden der Outsourcing-Spezialisten zählen und jetzt mit hohen Investitionen ihre Vertriebsmodelle verbessern. Hinzu kommt die Ablösung teilweise veralteter Versicherungs-Software durch Standardprodukte, wie sie sich bei Banken in den letzten zehn Jahren durchgesetzt haben. Solche Ablösungen und die Installation von modernen und effizienten Produkten von Anbietern wie Adcubum, SAP oder Ebaotech können Risiken

Ein Ausfall der Versicherungs-IT würde in der Schweiz massive Auswirkungen haben.

laut Experten eher noch vergrössern, wenn sie nicht durch entsprechende Verbesserungen auf der IT-Security-Seite begleitet werden,

weil die uralten Softwarecodes dank der praktisch geschlossenen Systeme und der für heutige Hacker unverständlichen alten Programmiersprachen wie Cobol als einigermassen sicher gelten.

Mit Sicherheitslösungen vertreten sind Firmen wie RSA, Symantec, Trend Micro oder CA. Die grossen Konzerne wie IBM, HP oder Accenture bieten noch die entsprechenden Services für die Implementierung

und Wartung an. Grosse Projekte sind hier meistens Teamwork. So führte die US-Lebensversicherung MetLife ihre «SecurID»-Lösung ein, die sie von RSA einkaufte. Diese wird auch in der Schweiz von Finanzdienstleistern verwendet, stets in Zusammenarbeit mit den Experten der Gotham Technology Group, einem IT-Servicounternehmen.

In der Schweiz gilt die gemeinsame «Circle-of-Trust» Identity-Plattform der Interessengemeinschaft IG B2B für die Broker von 20 unterschiedlichen Versicherungen als eines der Vorzeigeprojekte im Bereich IT-Security. Die rund 1000 in der Schweiz registrierten Broker können sich mit einem einzigen Token und Login bei den Portalen der Versicherungen anmelden. Auf der Seite der Versicherungen sind praktisch alle grossen Adressen von Allianz und AXA Winterthur bis Vaudoise, Visana und Zurich vertreten. «Es braucht eine Community und eine treibende Kraft, welche die Partner zusammenhält», sagt Ergon-Experte Adrian Berger (siehe «nachgefragt»). «Es braucht zudem ein gemeinsames Verständnis vom Nutzen einer solchen Plattform, wie beispielsweise die Vereinfachung oder Beschleunigung des Geschäfts. Spannend ist, wenn so ein konsolidierter Datenpool mit anderen Communities interagieren kann und sich daraus neue Geschäftsmöglichkeiten ergeben.»

Anzeige

NACHGEFRAGT

«Noch nicht ganz so wie Banken»



Adrian Berger (37), Leiter der Abteilung für Finance und Security Solutions bei Ergon

Wie stark sind Versicherungen grundsätzlich hinsichtlich IT-Security sensibilisiert?

Adrian Berger: Noch nicht ganz so intensiv wie bei den Banken, aber sie sind gut sensibilisiert und haben das richtige Bewusstsein für den Umgang mit personenbezogenen Daten, die richtig geschützt werden müssen.

Was war die grösste Herausforderung beim IG B2B-Projekt?

Berger: Viele Versicherungen haben eine sehr heterogene Applikationslandschaft und bedienen sowohl den B2C- wie auch den B2B-Kanal, wobei dieser ein grosses Gewicht hat. Einen Web Single Sign-on, also eine einmalige Anmeldung für alle Plattformen über die verschiedenen Kanäle und Applikationen zu machen, ist eine Herausforderung.

Wie sieht die Kosten-Nutzen-Rechnung aus?

Berger: Eine zentralisierte Infrastruktur bringt viele Vorteile: Policies sind besser durchzusetzen, alles wird besser handhabbar, man löst die Probleme einmal richtig, Fehlerquellen werden reduziert etc. Wie die konkrete Kosten-Nutzen-Rech-

nung aussieht, können wir nicht ausführen. Wenn man E-Services anbieten will, braucht man dazu zwingend eine professionelle Infrastruktur.

Die vielen beteiligten Partner machen die Verwendung einer einheitlichen Plattform schwierig – wie wurde diese Herausforderung gelöst?

Berger: Der Verein IG B2B war der treibende Faktor mit der Vision und dem Willen, das Projekt durchzuziehen. Ein ganz wichtiger Aspekt war, auf offene Standards zu setzen und ein Lock-in-Effekt bezüglich Technologien und Lieferanten zu vermeiden. Die offenen Standards ermöglichen eine klare Trennung zwischen der zentralen IG B2B-Infrastruktur und derjenigen der Firmen. Andere Anbieter können partizipieren bzw. müssen sogar partizipieren können, um keine marktbeherrschende Situation zu schaffen.

Lässt sich das Modell einheitlicher Identity-Plattformen auch auf andere Branchen übertragen?

Berger: Eine solche Plattform zu bauen, ist sicher eine Schweizerische Eigenschaft, die auf unseren föderalistischen Grundgedanken aufbaut. Es könnte auf weitere Geschäftsfälle übertragen werden, in denen Broker eine wichtige Rolle spielen, beispielsweise die externen Vermögensverwalter.

INTERVIEW: MATTHIAS NIKLOWITZ

Warum evaluieren intelligente Broker die PKRück?

- Gleich und Gleich gesellt sich halt gern.
- Hat die PKRück nicht ein ganzes Produkt- und Beratungsangebot speziell für Broker?
- Weil sie genau wissen, wo Aufwand und Ertrag stimmen.

Die PKRück bietet Vorsorgeeinrichtungen eine echte Alternative für die Deckung der Risiken Invalidität und Tod. Wir sind im Schweizer Vorsorgemarkt bestens positioniert und bieten ein attraktives Produkt- und Beratungsangebot speziell für Broker. Können wir sonst noch etwas für Sie tun? Kommen Sie mit uns ins Gespräch (044 360 50 70)!