

## IT-Sicherheit bei Versicherungen

# Prävention ist besser als Reaktion

**IT-Sicherheitslücken sind in Unternehmen weit verbreitet. Manch scheinbar sicheres Firmennetz entpuppt sich beim genaueren Hinsehen als ungenügend. Unternehmen tun deshalb gut daran, sich frühzeitig darum zu kümmern, wie Daten verloren gehen, wo die Gründe dafür liegen und wie ein Datenverlust verhindert werden kann.**

Priska B. Roelli

Noch nie hatten IT-Verantwortliche an so vielen Fronten zu kämpfen, um die Unternehmenssicherheit aufrechtzuerhalten, wie heute: So droht einerseits Gefahr von aussen durch professionell organisierte Cyberbanden, die ihre technischen Verfahren immer raffinierter gestalten und hoch komplexe Technologien einsetzen, um an ihr Ziel zu gelangen. Andererseits ist die Unternehmenssicherheit durch die zunehmende Mobilität der Mitarbeitenden, die mit Handhelds und Laptops von aussen auf das Unternehmensnetzwerk zugreifen, bedroht. Die rasante Weiterentwicklung und Nutzung sozialer Medien trägt ebenfalls dazu bei, dass das Risiko steigt, Opfer von Angriffen durch Cyberkriminelle zu werden. Verschärft wird die Gefahr zusätzlich durch die aufkommenden Self-Service-Strategien der Versicherungen, die sich online gegenüber bestehenden und potenziellen Kunden öffnen, ihnen ermöglichen, Transaktionen via Computer und mobilen Geräten abzuwickeln und sich so noch mehr Sicherheitsprobleme ins Unternehmen holen. Und last but not least stellen die Mitarbeiter selbst ein weiteres, nicht zu unterschätzendes Risiko dar.

## Datenschutz ja, aber wie?

Angesichts des vielfältigen und wachsenden Gefahrenpotenzials stellen sich für die IT-Verantwortlichen viele Fragen zur Informationssicherheit. Denn trotz hoher technischer Sicherheitsmassnahmen nimmt der Datenklau in Unternehmen laufend zu. Rein technische Schutzmassnahmen bieten längst keine ausreichende Sicherheit mehr vor Datenmissbrauch durch Mitarbeiter oder Hackerattacken von aussen. Doch wie können Versicherer ihre Daten wirkungsvoll schützen? Reichen eine Kombination aus organisatorischen und ethischen Massnahmen, eine Vereinfachung der IT-Architektur und eine höhere Aufmerksamkeit des Managements aus,

um einen ausreichenden Level an Datensicherheit zu erreichen? Tatsache ist, dass viele Unternehmen oft nur einzelne Sicherheitsrisiken identifizieren und isolierte Massnahmen treffen, um diese zu beheben, ohne eine ganzheitliche und langfristige Risikomanagement-Strategie zu ergreifen. Taktische Massnahmen sind sicher sinnvoll; ohne ganzheitlichen Ansatz, der sowohl die IT-Prozesse selbst, als auch infrastrukturelle, personelle und organisatorische Aspekte der gesamten IT-Umgebung berücksichtigt, bleiben die Risiken jedoch bestehen. Ein unternehmensweit einheitliches Sicherheitsmanagement, bei dem Unternehmen nicht nur die Gefahren im Blick haben sollten, die direkt vor ihnen liegen, sondern auch ein Augenmerk für andere Gefahren haben, ist deshalb unerlässlich.

## Risikoanalyse und Definition

Die Kernfunktion eines Sicherheitsmanagements beinhaltet die Untersuchung des nötigen Schutzes durch eine Risikoanalyse und die Definition der geeigneten Sicherheitsmassnahmen. Mögliche Gefahren können dadurch von vornherein reduziert und etwaige Störfälle eruiert werden. Der Komplexität des Informationssystems entsprechend müssen dabei Massnahmen für die Gewährleistung sämtlicher Sicherheitsaspekte festgelegt werden. Dabei gilt es, die im Einsatz stehende Hard- und Software gründlich zu analysieren und sich ein realistisches Bild über die Verwundbarkeit des eigenen Unternehmens zu machen. Fragen, die in diesem Zusammenhang gestellt und beantwortet werden müssen, wie beispielsweise:

- Welchen Wert haben unsere Informationen – sowohl aus Sicht des Unternehmens als auch von der Konkurrenz?
- Mit welchen Konsequenzen müssen wir bei einem Verlust rechnen?

- Wo befinden sich die grössten Schwachstellen?
- Wo befinden sich die geschäftskritischen Daten, wer hat Zugriff auf sie und wie sind sie derzeit geschützt?
- Ist das Identitäts- und Zugriffsmanagement geregelt und wenn ja wie?
- Ist das Thema IT-Sicherheit innerhalb der Organisation systematisch organisiert?
- Sind die Mitarbeiter im Umgang mit sensiblen Informationen geschult?
- Bestehen Sicherheitsrichtlinien und halten sich die Mitarbeiter daran?

helfen, Lücken aufzudecken und mögliche Risikoschwachstellen zu identifizieren. Die Liste ist nicht abschliessend, und es gibt eine Vielzahl weiterer Punkte, die für eine sichere IT-Infrastruktur berücksichtigt werden sollten, genauso wie die fortlaufende Entwicklung und Anpassung der Dokumentation. Denn eine nicht den aktuellen Gegebenheiten entsprechende IT-Sicherheitspolitik spiegelt nur eine scheinbare, nicht oder nur teilweise vorhandene Sicherheit wieder.

## Fazit

IT-Sicherheit ist kein Thema, das sich nebenbei erledigen lässt, sondern ein kontinuierlicher Prozess, der regelmässig analysiert und bewertet werden muss. Mit den daraus resultierenden Ergebnissen können IT-Verantwortliche Sicherheitsmassnahmen umsetzen und Vorkehrungen treffen, die nicht nur die Vertraulichkeit, Integrität und Verfügbarkeit der Unternehmensdaten gewährleisten, sondern gleichzeitig dabei helfen, mögliche Schäden, die durch unerwünschte Eindringlinge angerichtet werden, auf ein Minimum zu reduzieren. ■

Im Anschluss an diesen redaktionellen Artikel publizieren folgende Firmen ihren Publi-Forum-Beitrag:  
**SwissSign AG, Swisscom (Schweiz) AG, Norman Data Defense Systems AG**

IT-Sicherheit

# «Online Security» muss für den Kunden einfach sein

**Digitale Identität und digitale Signatur sind für die Online Security zentrale Elemente. Die SuisselD mit bereits heute verfügbaren Lösungen zu sicherer Kommunikation und Identifikation ist der richtige Ansatz.**



BILD: ZVG

**Adrian Humbel ist CEO der SwissSign AG. SwissSign erstellt Lösungen für die Schweizerische Post wie die Post SuisselD, IncaMail, Swiss Post Box und den SwissStick**

**Schweizer Versicherung: Welche Sicherheitsprobleme beschäftigen die Versicherungen in technischer und praktischer Hinsicht derzeit am meisten?**

**Adrian Humbel:** Ich denke, dass es mit den Möglichkeiten von Web 2.0 und mit der sehr guten Internet-Abdeckung in der Schweiz für Versicherungen zunehmend interessant wird, Korrespondenz oder andere Transaktionen direkt online anbieten zu können. Dabei wird die eindeutige Identifikation und die Möglichkeit der digitalen Willensbekundung (digitaler Signatur) zunehmend notwendig. Zusätzlich sehe ich Bedürfnisse in der einfachen, sicheren und nachweisbaren Kommunikation. Alles Bereiche, wo die Schweizerische Post sehr gute Lösungen anbieten kann.

**Versicherungen sind erfahrungsgemäss punkto IT-Sicherheit gut aufgestellt. Besteht trotzdem Verbesserungspotenzial? Wenn ja, wo?**

**Humbel:** Verbesserungspotenzial besteht immer. Wichtig dabei ist, dass die Sicherheitsmassnahmen von den Benutzern nicht als zusätzliche «Hürden» aufgenommen werden. Strong Authentication, White Listing, Black Listing, Transaktionssignatur für aussergewöhnliche Fälle usw. wird in Zu-

kunft vermehrt eingesetzt werden. Auch hier gibt es bereits heute recht gute Standardlösungen.

**Welchen Stellenwert nimmt Mobile Security ein? Gilt es für eine so ausendienstlastige Branche, spezielle Massnahmen zu ergreifen?**

**Humbel:** Es wird immer wichtiger, dass auch mobil auf nötige Daten zugegriffen werden kann. Vielfach werden dazu speziell gemanagte und konfigurierte Laptops abgegeben. Dies ist recht teuer und vom Unterhalt her auch nicht sehr trivial. Neu könnte man da mit einem USB-Stick, der sämtliche Software für den sicheren Zugriff auf die wichtigen Applikationen sowie die (Suisse) ID des Aussenmitarbeiters enthält, kostengünstig und sicher neue Lösungen schaffen. Ein Beispiel dazu ist unser SwissStick.

**Stichwort Webapplikations-Sicherheit: Wie sehen die Vorkehrungen hier aus? Besteht Nachholbedarf?**

**Humbel:** Eine erste Herausforderung bei Webapplikationen ist die eindeutige Identifikation des Benutzers, denn Benutzername und Passwort sind für die meisten kommerziellen Webapplikationen nicht sicher genug. Eine sehr gute Lösung dazu ist die soeben lancierte SuisselD, welche die sogenannte «Strong Authentication» bietet, also etwas, das ich habe (Chip/Stick), und etwas, das ich weiss (Passwort). Zugleich ist mit dieser Zugangsmethode auch die Person zu 100 Prozent identifiziert. Eine zweite Herausforderung ist die Transaktionssicherheit rund um «Man in the Middle»-Attacken. Dem kann mit entsprechender Software auf einem USB-Stick entgegnet werden. Der Vorteil dieser Lösung ist, dass sie unabhängig vom Betriebssystem und ohne spezielle Software auf jedem PC läuft.

**Welche Rolle spielen Verschlüsselungstechnologien? Sind sie die «ultimative Lösung» zum Schutz gespeicherter Daten?**

**Humbel:** Verschlüsselungstechnologien sind heute unabdingbar. Die Verschlüsselung

sollte aber nach Möglichkeit für den Benutzer transparent, d.h. unbemerkt, erfolgen. So wird zum Beispiel bei unserer Lösung zur sicheren Kommunikation (IncaMail) das E-Mail während des Transports verschlüsselt, und bei Entgegennahme durch den Empfänger automatisch entschlüsselt. Ein gegenseitiger, in der Regel nicht sehr intuitiver Austausch von «Schlüsseln» entfällt dadurch.

**Security Awareness und das Mitarbeiterverhalten nimmt neben der technischen Komponente eine wichtige Rolle ein. Greift dieses Thema bereits, und wie gehen Versicherer diese Problematik an?**

**Humbel:** Security Awareness und Schulung von entsprechendem Mitarbeiterverhalten sind nach wie vor die besten Mittel, Sicherheitsprobleme schon gar nicht entstehen zu lassen. Dazu braucht es neben der Information für den Nutzer aber auch Lösungen, die in der Realität gelebt werden können. Passwortvorgaben mit Zahlen und Sonderzeichen, die alle vier Wochen in den unterschiedlichsten Systemen gewechselt werden müssen, sind meiner Meinung nach unbrauchbar. Single-sign-on-Lösungen mit Strong Authentication oder Consistent-sign-on-Lösungen mit der SuisselD sind da sicher der richtige Weg. Zusätzliche Awareness braucht auch im Bereich E-Mail. Ist es doch vielen Nutzern nicht bekannt, dass E-Mails in der Regel «clear text» übers Internet transportiert werden. Auch hier sind «lebbare» Sicherheitslösungen, die evtl. sogar Zusatznutzen (wie z. B. Empfangsquittung), bringen der Schlüssel zum Erfolg. ■

**swiss sign**  
Ein Unternehmen  
der Schweizerischen Post

SwissSign AG  
Sägereistrasse 25  
8152 Glattbrugg  
T: +41 44 838 36 00  
F: +41 43 344 88 10  
www.swissign.com

## IT-Sicherheit

# Lifecycle der Sicherheitsinfrastruktur aktiv managen

**Durch den schnellen Technologiewandel und die sich ständig verändernde Bedrohungslage ist es wichtig, beim Thema Sicherheit «am Ball» zu bleiben.**



BILD: ZVG

**Remo Viscardi, Head of ICT Security Services bei Swisscom (Schweiz) AG, Bereich Grossunternehmen**

**Schweizer Versicherung: Welche Sicherheitsprobleme beschäftigen die Versicherungen in technischer und praktischer Hinsicht derzeit am meisten?**

**Remo Viscardi:** Für Versicherungsunternehmen wird es immer anspruchsvoller, die Datensicherheit zu gewährleisten. Das elektronische Geschäft weitet sich aus, Mobile Working und Cloud Computing sind zum Normalfall geworden – Daten werden über das Internet bearbeitet und gespeichert. Hinzu kommen neue und verschärfte gesetzliche und regulatorische Vorschriften. Seit letztem Jahr beschäftigt auch das Thema «Pandemie» die Versicherungen relativ stark. Damit im Ernstfall von heute auf morgen der Grossteil der Mitarbeitenden sofort von zu Hause aus arbeiten und den Versicherungsbetrieb aufrechterhalten kann, sind Konzepte und entsprechende Services nötig. Flexible Remote-Access-Lösungen und starke Benutzerauthentisierung sind in diesem Zusammenhang wichtige Security-Themen.

**Versicherungen sind erfahrungsgemäss punkto IT-Sicherheit gut aufgestellt. Besteht trotzdem Verbesserungspotenzial? Wenn ja, wo?**

**Viscardi:** Durch den schnellen Technologiewandel und die sich ständig verändernde

Bedrohungslage ist es wichtig, beim Thema Sicherheit «am Ball» zu bleiben. Gerade das aktive Lifecycle Management bei der Sicherheitsinfrastruktur ist eine Aufgabe, die kontinuierlich getätigt werden muss. Die Sicherheitsinfrastruktur sollte topaktuell sein, und neue Softwareversionen müssen umgehend eingespielt werden. In diesen Bereichen gibt es sehr oft Verbesserungspotenzial, da Lifecycle-Themen nicht selten vernachlässigt werden – obwohl sie zu den wichtigsten Aufgaben überhaupt gehören.

**Welchen Stellenwert nimmt Mobile Security ein? Gilt es für eine so aussendienstlastige Branche, spezielle Massnahmen zu ergreifen?**

**Viscardi:** Versicherungen setzen bereits heute viele mobile Aussendienstmitarbeiter ein – mit zunehmender Tendenz. Für diese mobilen Arbeitsplätze und vor allem für die damit exponierten Datenbestände und Informationen müssen Schutzmassnahmen ergriffen werden. Wichtig sind starke Authentisierungen, Verschlüsselungen und Integrität der Daten – sowohl auf dem Transportweg, wie auch in der Ablage. Eine weitere Herausforderung ist: Wie werden die Mobile Devices sicherheitsmässig verwaltet? Welche Konzepte und Technologien sind wirkungsvoll?

**Stichwort Web-Applikations-Sicherheit: Wie sehen die Vorkehrungen hier aus? Besteht Nachholbedarf?**

**Viscardi:** Web-basierte Applikationen sind grundsätzlich sehr gut für mobile Arbeitsumgebungen geeignet, da sensitive Daten normalerweise nur zentral im Netz gespeichert werden. Die Web-Anwendungen sind aber in jedem Fall einem detaillierten Risk Assessment zu unterziehen.

**Welche Rolle spielen Verschlüsselungstechnologien? Sind sie die «ultimative Lösung» zum Schutz gespeicherter Daten?**

**Viscardi:** Moderne Verschlüsselungstechnologien bieten einen sehr guten Schutz für gespeicherte Daten – sofern sie (a) richtig eingesetzt werden (Prozesse, Leute) und (b)

die Schlüssel gut gewählt und absolut sicher aufbewahrt sind. Zusätzlich muss man sicherstellen, dass Daten auch auf dem Transportweg und während der Bearbeitung angemessen geschützt werden.

**Security Awareness und das Mitarbeiterverhalten nimmt neben der technischen Komponente eine wichtige Rolle ein. Greift dieses Thema bereits, und wie gehen Versicherer diese Problematik an?**

**Viscardi:** Der Mensch ist noch immer bei weitem die grösste Quelle von Unsicherheiten und Zwischenfällen (unbewusst und bewusst). Der stufengerechten Schulung der Benutzer ist deshalb höchste Aufmerksamkeit zu widmen. Wichtig sind auch – als Motivation für die Ausbildung – die praktische Demonstration von Risikoverhalten und gezielte, aber kontrollierte Versuche durch Dritte, das Sicherheitssystem auszuhebeln. Dies, um Schwachstellen aufzuzeigen und danach die Lehren daraus zu ziehen.

**Was gibt es aus Ihrer Sicht zu diesem Thema noch zu sagen?**

**Viscardi:** In den meisten Fällen geht man von einer Bedrohung von aussen aus. Oftmals kommt die Bedrohung von innen dazu. Deshalb ist für eine hohe Grundsicherheit, das Prinzip des «Need to know» konsequent anzuwenden: Der Mitarbeiter erhält nur Zugriff auf die Informationen, die er zur Ausübung seiner aktuellen Funktion braucht. ■



**swisscom**

Swisscom (Schweiz) AG  
Grossunternehmen  
Postfach, CH-8021 Zürich  
Telefon: 0800 800 900  
[www.swisscom.ch/security](http://www.swisscom.ch/security)

## IT-Security

# «Die ultimative Lösung zum Schutz von Daten gibt es nicht»

**IT-Sicherheit erfordert individuelle Strategien. Werden verfügbare Technologien mit organisatorischen Bedingungen etabliert, lassen sich Risiken auf ein Minimum reduzieren.**



BILD: ZVG

**Mike Gasser, General Manager,  
Norman Data Defense Systems AG**

## **Schweizer Versicherung: Welche Sicherheitsprobleme beschäftigen die Versicherungen in technischer und praktischer Hinsicht derzeit am meisten?**

**Mike Gasser:** Die meisten Unternehmensdaten gehen durch falsches Verhalten der Mitarbeiter verloren. Security-Awareness ist deshalb ein grosses Thema. Web-2.0-Anwendungen und der zunehmende Einsatz von Multi-Channel-Architekturen, Data-Leakage-Prevention- sowie Identity- und Access-Managementlösungen, neue Technologien wie Cloud Computing und auch Compliance-Richtlinien sind Themen, die jetzt und auch in Zukunft die Versicherer sicher beschäftigen werden.

## **Versicherungen sind erfahrungsgemäss punkto IT-Sicherheit gut aufgestellt. Besteht trotzdem Verbesserungspotenzial? Wenn ja, wo?**

**Gasser:** Fehlendes Identitäts- und Zugriffsmanagement von Seiten des Unternehmens, zu späte Einspielung von Software-Patches, fehlende Sicherheitssperren bei mobilen Geräten, unzureichende Datensicherung, «schwache» Passwörter, offene drahtlose Zugänge, fehlende Verschlüsselungstechnologien und Antiviren-Scanner sowie die Unachtsamkeit der Mit-

arbeiter stufen wir als die grössten Probleme ein.

## **Welchen Stellenwert nimmt Mobile Security ein? Gilt es für eine so aussendienstlastige Branche, spezielle Massnahmen ergreifen?**

**Gasser:** Die Möglichkeit, mit verschiedensten Geräten und von überall auf Geschäftsdaten zuzugreifen, erhöht das Risiko, dass Viren und Würmer den Weg ins Netzwerk finden und mobile Geräte auch verloren gehen. Damit die Betriebsstabilität und die Datenintegrität gewährleistet werden können, müssen alle mobilen Endgeräte und Wechselträger in die Sicherheitsstrategie mit einbezogen werden: Notebooks, Smartphones, PDAs, aber auch MP3-Player, iPods und USB-Sticks. Der Einsatz von Verschlüsselungstechnologien zur Datenübertragung und ein Identitäts- und Zugriffsmanagement stehen dabei an vorderster Stelle.

## **Stichwort Web-Applikations-Sicherheit: Wie sehen die Vorkehrungen hier aus? Besteht Nachholbedarf?**

**Gasser:** Drei Viertel aller Hackerattacken erfolgen über offene Webapplikationen. Werden sie nicht geschützt, sind nicht nur die Applikationen selbst, sondern auch die involvierten Backend-Systeme und die gesamte interne IT gefährdet. Web-Applikationen müssen deshalb unbedingt ins Sicherheitskonzept aufgenommen, auf Schwachstellen überprüft und gegebenenfalls nachträglich mit geeigneten Massnahmen wie beispielsweise Security-Gateways abgesichert werden.

## **Welche Rolle spielen Verschlüsselungstechnologien? Sind sie die «ultimative Lösung» zum Schutz gespeicherter Daten?**

**Gasser:** Die ultimative Lösung zum Schutz gespeicherter Daten gibt es nicht. Verschlüsselungstechnologien sind aber ein unverzichtbares Glied in der gesamten Sicherheitskette, durch die ein Angriff aufs

Netzwerk bzw. der Zugang auf Unternehmensdaten zusätzlich erschwert wird.

## **Security Awareness und das Mitarbeiterverhalten nehmen eine wichtige Rolle ein. Greift dieses Thema bereits und wie gehen Versicherer diese Problematik an?**

**Gasser:** Viele Versicherer sensibilisieren ihre Mitarbeiter bereits mit Trainings, haben Richtlinien definiert und geben vor, welche Hardware eingesetzt und genutzt werden darf. Damit IT-Sicherheit aber greift, muss sie auch gelebt werden. Die Vorbildfunktion des Managements, die den Umgang mit sensiblen Daten und die Nutzung der IT-Infrastruktur vorlebt, spielt dabei eine wesentliche Rolle.

## **Was gibt es aus Ihrer Sicht zu diesem Thema noch zu sagen?**

**Gasser:** Der Schlüssel zur effektiven Bekämpfung von Bedrohungen liegt im Einsatz von Sicherheitstechnologien im gesamten Unternehmen – in Form von mehrstufigen Lösungskomponenten. Überwindet ein Angreifer eine dieser Ebenen, dann scheitert er an der nächsten. Damit die Abwehr nach innen und aussen gewährleistet ist, muss ein Sicherheitskonzept den gesamten End-to-End-Kommunikationsprozess berücksichtigen: Dazu zählen die komplette Infrastruktur, die Server inklusive Daten und Applikationen im Rechenzentrum, TK-Systeme, LAN und WAN, die Verschlüsselung aller Sprach-, Daten- und Videoanbindungen sowie alle mobilen Endgeräte und Anwender. ■



Norman Data Defense Systems AG  
Münchenerstrasse 43  
4052 Basel  
Tel. 061 317 25 25  
norman@norman.ch  
www.norman.ch