

Promotion: Versicherungsschutz

# Wer schaut sich Ihre Daten an, ohne dass Sie es wissen?



Die Hiobsbotschaften über Datenklau und Internetattacken reißen nicht ab. Dabei sind Unternehmen und öffentliche Organisationen gleichermaßen betroffen. Eine bedenkliche Entwicklung der Cyberkrieg-Aktivitäten bereitet den Verantwortlichen großes Kopfzerbrechen. Sie suchen nach Wegen, wie sie ihr Unternehmen schützen und in eine sichere Zukunft investieren können.

Sony meldete einen Hackerangriff auf ein weltweites Netzwerk, Werbekunden konnten über Jahre auf die Profile von Facebook-Anwendern zugreifen, eklatante Sicherheitslücke bei der Volkszählung Zensus 2011. Dies sind nur drei bekannte Datenpannen aus dem Jahr 2011, die die Schlagzeilen füllten. Dabei kann ein gezielter Hackerangriff oder auch ein verlorener Laptop immense Kosten verursachen.

## Die Bedrohungen nehmen weiter zu.

Die Entwicklung von Schadprogrammen ist fast so alt wie die des Computers. Wurden in den siebziger Jahren die ersten Viren entwickelt, so hatten diese eher den Sinn, Schwachstellen in den Programmen aufzuzeigen. Die Situation änderte sich allerdings in den achtziger und neunziger Jahren. Schnell lernte man aus ursprünglich sportlich motivierten Entwicklungen von Viren und Würmern, dass damit auch Zwecke verfolgt werden können, die über das »Verstopfen« von Servern oder Netzwerken hinausgingen. Das Ziel: die Manipulation von Rechnern und Daten. In den letzten zehn Jahren entstand so ein Markt mit Milliarden an Umsatz.

Als Folge entwickelte sich eine IT-Security-Industrie, die in den ersten Jahren eher auf das Geschehen reagierte als es vorauszuahnen. Mittlerweile ist jedoch eine Industrie entstanden, ohne die man gegen die Vielfältigkeit heutiger Bedrohungen und die rasche Evolution technologischer Entwicklungen des Internetzeitalters nicht mehr ankommen könnte.

Trotz mächtiger Schutzschilde durch moderne Sicherheitstechnologien treten aber nach wie vor immer Störfälle in großen und kleinen Unternehmen auf. So sehen laut der jüngsten IDC-Studie »IT Security in Deutschland 2011« beispielsweise 42 Prozent der 202 befragten Unternehmen die Abwehr neuer Angriffsszenarien als wichtigste Herausforderung. Angesichts der ständig zunehmenden Zahl an mobilen Kommunikationsgeräten, komplexeren IT-Infrastrukturen und Geschäftsprozessen, die auch Plattformen sozialer Netzwerke in ihre Kommunikation mit einbeziehen, sind die spezifischen Her-

ausforderungen an die Sicherheit nicht nur immens, sondern auch einem stetigen Wandel unterworfen. Gemäß der Studie sind es aber neben den externen Bedrohungen auch die Mitarbeiter, die ein großes Sicherheitsrisiko in einem Unternehmen darstellen können. So gab die Hälfte der Befragten an, dass die Mitarbeiter das schwächste Glied in der IT-Security-Kette darstellen, dicht gefolgt von Smartphones (31%), Laptops (21%) und PC-Arbeitsplätzen (20%).

**Spezialversicherer hilft.** Über 10 Jahre Erfahrung besitzt die Oskar Schunck AG & Co. KG für Versicherungslösungen für IT-Unternehmen. So hat sich die Oskar Schunck AG & Co. KG auch mit dem Bereich der Cyberrisiken vertraut gemacht und baut auf entsprechende Experten und Risikoträger. Daher versteht sich der Versicherungsexperte darauf, erstklassigen, unkomplizierten und flexiblen Service anzubieten, der für Kunden aller Branchen den vollen Nutzen bringt. Schunck arbeitet eng mit dem Spezialversicherer Hiscox AG aus München zusammen, der seit Mai diesen Jahres ein Spezialprodukt anbietet. Hervorragender Versicherungsschutz in Kombination mit Service ermöglicht es zahlreiche Zusatzleistungen anbieten zu können. Das aus frei wählbaren Modulen bestehende Produkt bietet die nötige Flexibilität, um für Unternehmen die passende Absicherung von Cyberrisiken zu erzielen. Ein globales Expertennetzwerk für Datenrisiken bestehend aus Anwälten und Experten stellen sicher, dass jederzeit bestmögliche Unterstützung zu Teil wird.

### **Diese Kosten werden übernommen.**

So gewährt das Data-Breach-Cost-Modul forensische Untersuchungen, bei denen der Versicherer die Kosten für die nötigen Untersuchungen trägt, um genau zu validieren, was vorgefallen ist und wessen Daten in Gefahr sind. Des Weiteren kommt der Versicherer für die Kosten der Benachrichtigungen von Kreditkartenunternehmen oder Regulierungsbehörden auf. Auch für den Kundenservice trägt der Versicherer die Kosten, beispielsweise falls ein Call Center eingerichtet, oder eine Kredit-

» Die spezifischen Herausforderungen an die Sicherheit sind nicht nur immens, sondern auch einem stetigen Wandel unterworfen. «

überwachungsservice angeboten werden muss. Versicherungsschutz besteht für Vermögensschäden – inklusive eines etwaigen immateriellen Schadens – wegen einer vom Versicherungsnehmer zu verantwortenden Datenrechtsverletzung. Dies gilt auch für alle elektronischen oder nicht elektronischen Störungen wie Phishing oder Social Engineering, sowie für Schäden durch Übertragung von Schadprogrammen. Auch für Untersuchungen durch Regulierungsbehörden oder durch die Payment card industry (Pci) sowie Schadenersatzforderungen, die sehr kostspielig sind, werden vom Risikoträger übernommen.

Der Inhalt einer Website oder einer E-Mail kann schnell missverstanden werden oder sogar ein Urheberrecht verletzen. Im Rahmen des »Cyber-Liability-Moduls«, unterstützt der Versicherer bei der Reaktion auf durch Onlineinhalte entstehende Forderungen. Fügt ein Hacker ihrer Website, ihren Programmen oder ihren elektronischen Daten Schaden zu, oder werden ein elektronisches Programm oder Daten

gestohlen, übernimmt der Versicherer im Rahmen seines »Cyber-Business-Interruption-Modules« jegliche Kosten für Reparatur, Ersatz oder Wiederherstellung. Zudem wird ein Sicherheitsberater zur Seite gestellt, der das Firmensystem überprüft und forensische Untersuchungen durchführt.

Es kann vorkommen, dass ein Hacker ihre Firma erpresst. In diesem Fall beauftragt Schunck gemeinsam mit einem Versicherer im Rahmen des »Data-Extortion-Moduls« zunächst eine der führenden Sicherheitsfirmen, um den Kunden beim richtigen Handling dieser Situation zu unterstützen. Außerdem wird ihnen die Summe erstattet, welche sie an den Erpresser bezahlen mussten, um den Schaden so gering wie möglich zu halten.

---

Konkrete Anfragen oder weitere Produktinformationen erhalten Sie bei Peter Janson, Leiter Competence Center Informationstechnologie (jansonp@schunck.de)

[www.schunck.de](http://www.schunck.de)