

## Der "Internet-Sicherheitsgurt" von ZT-Prentner-IT kombiniert technischen Schutz und volle Haftungsübernahme im Schadensfall durch staatlich befugte IT-Ziviltechniker.



Datenverlust und Internetsicherheit sind für die Versicherungsmathematik schwer greifbar. Bis dato gibt es im deutschsprachigen Raum keine regulären Versicherungen gegen Internet-Hacking und Datendiebstahl. "Teilweise ist es möglich, die Kosten für Daten- oder Systemwiederherstellung versicherungstechnisch abzudecken. Die eigentliche Gefahr sind aber Schadenersatzklagen und Imageschäden, die Millionenbeträge ausmachen können", erklärt IT-Security-Experte Hans-Jürgen Pollirer, Obmann der WKÖ-Bundessparte Information und Consulting.

Gemäß der aktuellen Verizon-Studie "2011 Data Breach Report" greifen Hacker neben Großunternehmen und Banken vermehrt auch Handels- oder Tourismusbetriebe an, weil kritische Personendaten wie Kreditkartennummern aufgrund geringerer Sicherheitssperren dort leichter zu erbeuten seien. Von den insgesamt 1.700 untersuchten Datenklau-Fällen sind 50 Prozent der Schäden durch Internet-Hacking entstanden und immerhin 17 Prozent wurden durch eigene System-Fehler ermöglicht.

### INTERNET-SICHERHEITSGURT

Zur Absicherung von Web-Systemen hat die Ziviltechnikergesellschaft ZT-Prentner-IT aus Wien den "Internet-Sicherheitsgurt" entwickelt: Das Service kombiniert technische Checks - professionelles Internet-Hacking zum Aufzeigen von Sicherheitslücken - mit der vollen Haftungsübernahme bei Datenpannen, Datendiebstahl oder Systemblockaden wie Denial of Services bis zu Schadenssummen von 1,5 Millionen Euro, je nach Anforderung auch mehr. Konzerne wie REWE, Unternehmen des Raiffeisen-Sektors oder das Amt der Vorarlberger Landesregierung nutzen bereits diesen Rettungsring für ihre Webportale.

"Im Rahmen des Internet-Sicherheitsgurt führen staatlich geprüfte IT-Sachverständige regelmäßige Kontrollen durch. Sprich: Sie versuchen, die Webseiten von außen zu knacken. Und zwar mit jenen Technologien, die Hacker und Angreifer aktuell einsetzen könnten", erklärt Geschäftsführer Wolfgang Prentner. Die neuesten Angriffsmethoden sind für Insider über Web-Communities und einschlägige Plattformen relativ leicht aufzuspüren.

Zu Projektbeginn führt [ZT-Prentner-IT](#) eine E-Spionage nur auf Basis einer Visitenkarte oder E-Mail Adresse durch. Ergebnis ist der gesamte Netzwerkplan all jener IT-Systeme eines Unternehmens, die Online sind. "Kunden staunen immer darüber, wie viel von außen einsehbar ist", berichtet Prentner. Anschließend folgen eine Initialprüfung mit Verwundbarkeitsanalyse sowie ein Maßnahmenkatalog. Nach der Umsetzung sollen regelmäßige Checks gewährleisten, dass die Internet-Systeme stets nach dem aktuellen Stand der Technik abgesichert sind. Die Überprüfung wird mit einem staatlich anerkannten Zertifikat besiegelt: "Der Prüfbericht eines Ziviltechnikers entspricht einer öffentlichen Urkunde - ähnlich einer notariellen Bestätigung", erläutert der auf IKT spezialisierte Rechtsanwalt Johannes Juranek von der Wiener Kanzlei CMS und führt aus: "Sollte es bei geprüften Systemen zu Attacken kommen, haften Ziviltechniker aufgrund ihrer staatlichen Prüfbefugnis für entstandene Schäden. Da die Ziviltechnikergesellschaft ihre Projekte jeweils gegen berufliche Schadensfälle versichert, profitieren die geprüften Unternehmen de facto von diesem Versicherungsschutz." (pi/rnf)