



Freitag, 29.07.2011

Versicherungen gegen Hackerangriffe

Spezielle Versicherungen decken finanzielle Risiken von Hackerangriffen ab. Ohne technisches Knowhow geht aber auch hier nichts.

Die Ankündigung der US-Tochter der Zurich Financial Group (ZFS), dass der Versicherer **nicht die Umtriebe berappen** will, die nach dem **Gigahack im April** auf den japanischen Elektronikriesen Sony zukommen, wirft ein Schlaglicht auf die finanziellen Risiken durch Cyberattacken. So stellt sich die Frage, ob und wie Cyberangriffe überhaupt versichert werden können und wie es mit der Haftungsfrage oder Mitverschulden der Versicherungsnehmer aussieht.

Risiko wie jedes andere

Eines der ersten Unternehmen, die eine Cyberversicherung entwickelt haben, ist der englische Konzern Lloyds, der via seine Tochter CFC Underwriting erste Angebote bereits vor zehn Jahren lancierte. Im Fokus standen damals Dot-com Firmen, heute müsste aus der Sicht von Lloyds jede Firma, die das Internet nutzt, so eine Versicherung abschliessen.

"Datendiebstahl eröffnet eine ganz neue Welt von Haftungsrisiken und Unternehmen, gerade in Europa, müssen lernen, dass sie diese gleich abdecken müssen wie andere grosse Risiken", betonte kürzlich Graeme Newman von CFC Underwriting an einer Konferenz von Versicherungsfachleuten in Bournemouth.

Verhaltene hiesige Nachfrage

Auch in der Schweiz ist es möglich, sich gegen Cyberangriffe versichern zu lassen, allerdings sei die Nachfrage verhalten, wie Lukas Meermann, Sprecher von ZFS in der Schweiz, auf Anfrage von inside-it.ch erklärte. "Der Datenverlust aufgrund von Computerviren oder Hackerangriffen wird in der Schweiz in der Regel nicht respektive sehr restriktiv versichert."

Wie gross der Markt für Cyberversicherungen ist, scheint im Moment noch nicht klar. Obwohl das Thema seit kurzem insbesondere in den USA grössere Aufmerksamkeit erfahre, sei das Geschäft noch sehr jung und Prognosen entsprechend schwierig, so Meermann.

Aus technischer Sicht stellt sich natürlich die Frage nach dem Mitverschulden des Kunden, schliesslich erscheint es unsinnig, dass ein Versicherer bezahlen müsste, wenn Hacker eine längst bekannte Sicherheitslücke ausnützen sollten. Der ZFS-Sprecher sagt dazu: "Eine Hacker-Versicherung muss detaillierte Angaben zu den im Einzelnen gedeckten Schäden enthalten und die Sorgfaltspflichten des Versicherungsnehmers werden für den Einzelfall definiert."

Wöchentlicher Sicherheitsreport

Noch einen Schritt weiter geht Wolfgang Prentner von ZT Prentner IT in Wien: "Einzig eine permanente Überwachung macht Sinn", sagt der Geschäftsführer des Unternehmens, das seine IT-Sicherheitsdienstleistungen mit einem Versicherungsschutz kombiniert hat und dieses Paket als "Internet- Sicherheitsgurt" verkauft: Sollte ein Kunde gehackt werden, haftet Prentners Unternehmen mit 1,5 Millionen Euro pro Fall.

Zu seinen Kunden gehören Stellen der öffentlichen Hand wie die Stadt Salzburg und Spitäler, aber auch Konzerne aus den Bereichen Finanz, Industrie oder Handel. Die Kosten für den Sicherheitsgurt im virtuellen Raum belaufen sich zwischen 2000 und 100'000 Euro, so der staatlich befugte IT-Ingenieur im Gespräch.

Nach einer ersten Risikoanalyse und diversen Penetrationstests liefert das Unternehmen seinen Kunden wöchentliche Berichte zum Zustand der Systeme und meldet allfällige Schwachstellen, klassifiziert in die drei im Security-Bereich üblichen Dringlichkeitsstufen hoch, mittel und niedrig. "Wenn der Kunde das dann nicht bereinigt und es zu einem Angriff kommt, dann haften wir nicht", so Prentner. Und: "Zu einem Versicherungsfall ist es noch nie gekommen." (Philippe Kropf)

ZTPRENTNERIT
STAATLICH BEFUGT. IT-ARCHITEKTEN