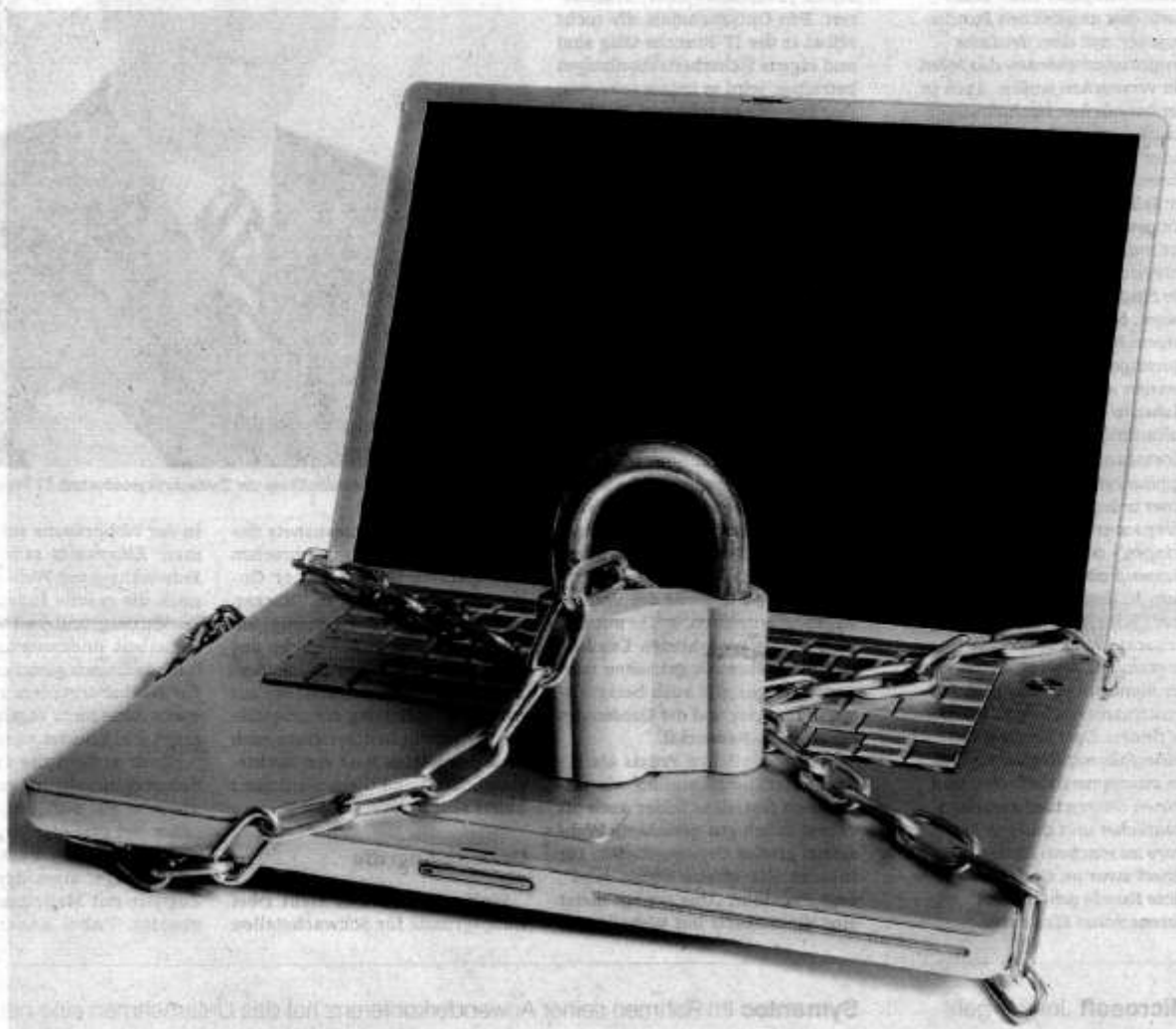




medianet

Inside Your Business. Today.

Web-Präsenzen viel zu schlecht gesichert



Der Datenklau geht um In den vergangenen Wochen haben Hacker durch spektakuläre Einbrüche in Netze von sich reden gemacht. Die Haftung für gestohlene Daten liegt aber weiterhin komplett bei den Betreibern von Websites. **Seite 54**

Die Angst der Website-Betreiber vor der Haftung

Auch bei Fehlern des Providers oder Dritten sind die Site-Betreiber für ihre verwalteten Daten verantwortlich.

CHRIS HADERER

Wien. IT-Security-Fachleute haben es zurzeit nicht leicht: Auf der einen Seite sorgen Cracker-Gruppen wie „Anonymus“ für Wellen im Datenteich, auf der anderen Seite wird die Datenschutz-Szene durch „kleine“ Skandale wie den deutschen „Bundestrojaner“ erschüttert. Für Unternehmen, die nicht selbst in der IT-Branche tätig sind und eigene Sicherheitsabteilungen betreiben, wird es immer schwerer, ihre Systeme zu schützen. Das liegt nicht unbedingt an fehlenden technischen Möglichkeiten als vielmehr an einer unübersichtlichen Auswahl an Produkten, die alle mit der gleichen Prämisse auf Klientel warten: Alle bieten sie den optimalen Schutz der Unternehmens-IT.

Haftung für Daten

Aufrütteln will auf jeden Fall Wolfgang Prentner, Geschäftsführer der Ziviltechnikergesellschaft ZT Prentner IT. Er möchte Website-Betreiber darauf aufmerksam machen, dass jeder Betreiber selbst für die Sicherheit seiner Daten haftet, auch bei Fehlern von Providern oder Dritten (so kann sich beispielsweise die ORF-Gebühreneintreibestelle GIS nicht der Verantwortung entziehen, sollte mit den im Sommer gestohlenen Kundendaten Missbrauch getrieben werden; selbiges gilt auch beispielsweise für Sony und die Kunden des Playstation-Networks).

„In der täglichen Praxis als IT-Sachverständige stellen wir tatsächlich fest, dass leider auch oft vermeintlich gut gesicherte Webseiten großer Organisationen für Insider wie offene Türen sind“, sagt Prentner, „Uns genügt meist eine Visitenkarte mit Webadresse,



Wolfgang Prentner, Geschäftsführer der Ziviltechnikergesellschaft ZT Prentner IT.

um in das Unternehmensnetz des verblüfften Kunden einzubrechen und Netzwerkpläne seiner Online-Systeme vorzulegen.“ Hacker, die guten Kräfte der Branche, tun das, um auf eine Schwäche des Systems aufmerksam zu machen; „bad guys“ wie Anonymus, um mit der Veröffentlichung der gestohlenen Daten von Drittpersonen auch noch den letzten Rest von Rechtsstaatlichkeit und Glaubwürdigkeit hinter sich zu lassen.

Gezielte Angriffe

Wolfgang Prentner sieht zwei Hauptgründe für Schwachstellen

in der Webpräsenz von Unternehmen: Einerseits stünde bei der Entwicklung von Webseiten immer noch die rasche Inbetriebnahme im Vordergrund und weniger die Sicherheit. Andererseits seien aber auch technisch gesicherte Systeme für Hacker trotzdem zu knacken, wenn diese nicht regelmäßig optimiert und getestet werden.

„Zwar spüren die technischen Schutzeinrichtungen Massenangriffe gut auf“, sagt Prentner. „Aber bei gezielten Angriffen auf ein bestimmtes Portal werden nur wenige, etwa drei bis zehn Zugriffe mit Malicious Code eingesetzt. Dabei haben unzurei-

chend optimierte Systeme keine Chance.“

Dramatische Konsequenzen kann eine schwach gesicherte Website vor allem hinsichtlich der Haftung haben. Laut Datenschutzgesetz und laut ABGB haftet ein Webseiten-Betreiber für die Sicherheit verwalteter Daten, auch wenn Fehler beim Provider passieren. Das ABGB definiert das folgendermaßen: „Jeder, der sich zur Erfüllung seiner Aufgaben eines Dritten – Erfüllungsgehilfe – bedient, ist für dessen Fehlverhalten wie für sein eigenes verantwortlich“, sagt Rechtsanwalt Johannes Juranek von der Wiener Kanzlei CMS.

Schutz für Unternehmen

Um Unternehmen Schutz vor Datendiebstahl zu bieten, hat ZT Prentner IT einen „Internet-Sicherheitsgurt“ entwickelt, mit dem sich bereits Unternehmen wie Rewe oder Raiffeisen ‚anschnallen‘. „Mit dem Servicepaket wird ein Websystem technisch wasserdicht gemacht und gleichzeitig die Haftung für Attacken bis zu 1,5 Mio. Euro Schaden übernommen“, sagt Juranek. „Sollte es bei geprüften Systemen zu Attacken kommen, haften Ziviltechniker aufgrund ihrer staatlichen Prüfbefugnis.“

Die Methoden der Angreifer werden allerdings immer raffinierter: Beim RSA-Hack im Frühjahr (RSA ist die Security-Abteilung des Lösungsanbieters EMC) wurde beispielsweise eine Kombination aus Phishing, einer modifizierten Excel-Tabelle und einem Zero-Day-Exploit verwendet sowie neue Verschlüsselungsalgorithmen. Deshalb müssen auch die Systeme immer intelligenter werden, mit denen sich Anwender zu schützen versuchen. www.zt-prentner.it.at

Wien, 14.10.2011