

«Besser 5 umgesetzte Massnahmen als 20 geplante»

Ein Unternehmen, das die zehn wichtigsten IT-Security-Massnahmen beherzigt, verfüge über einen guten Grundschutz, sagt Wolfgang Sidler, Mitautor des «Sicherheitshandbuches für die Praxis» und Security Consultancy Manager einer Schweizer Versicherung.

Das Jahr 2005 war von einigen Vorfällen geprägt. Welche waren Ihrer Meinung nach die grössten Herausforderungen, denen sich Security-Verantwortliche in den vergangenen zwölf Monaten stellen mussten?

Es gilt hier, die strategische und die operative IT-Security-Ebene zu unterscheiden. Auf der operativen Ebene galt es, das Unternehmen vor der Flut an Spam-Mails und Viren zu schützen. Viele Unternehmen hatten zudem enorme Herausforderungen im Bereich Business Continuity Management und Disaster Recovery. Auf der strategischen Ebene muss gewährleistet werden, dass die Gesetze und Verordnungen eingehalten werden. Die Zusammenarbeit mit dem Business wird deshalb zunehmend wichtig. Es zeigt sich der Trend, dass IT-Security und IT-Risk-Management langsam zu IT-Governance zusammengeführt werden.

Obwohl die Industrie immer bessere Produkte entwickelt und auch das Bewusstsein bezüglich der Wichtigkeit von IT-Security wächst, kommt es immer wieder zu gravierenden Sicherheitspannen. Wo sehen Sie die Ursachen für diese Entwicklung?

Die Bedrohungen und die Integration dieser neuen, angeblich sicheren Produkte in eine bestehende IT-Infrastruktur werden immer komplexer. Meist werden die Abhängigkeiten der einzelnen Applikationen und Systeme untereinander falsch eingeschätzt oder nicht erkannt. Auch ist eine gewisse Ignoranz seitens des Managements auszumachen. Es ist beruhigender, die Risiken nicht zu kennen, denn so sind keine Gegenmassnahmen notwendig, das heisst es müssen keine Ressourcen gebunden werden. Erst nach einem wirklich ernstem Vorfall werden die ersten Sicherheitsmassnahmen zaghaft ins Leben gerufen.

Immer wieder wird mangelndes Managementverständnis und die dar-

aus resultierenden knappen Finanzen als Grund für fehlende IT-Sicherheit verantwortlich gemacht. Wie können Security-Verantwortliche diesem Argument entgegenwirken?

Dies ist wirklich eine gute Frage. Es gibt keine hundertprozentige Sicherheit. Dass Sicherheit etwas kostet, ist nicht zu bestreiten. Jedoch sollte man in keine Sicherheitsmassnahmen investieren, wenn der zu erwartende Schaden kleiner sein wird, als die Investition. Fünf umgesetzte Sicherheitsmassnahmen sind besser als zwanzig geplante. Wenn sich ein Unternehmen auf die zehn wichtigsten IT-Sicherheitsmassnahmen konzentriert, hat es bereits einen guten IT-Grundschutz.

Vermehrt versuchen Unternehmen ihre IT-Sicherheit durch ein Outsourcing an spezialisierte Unternehmen zu optimieren. Wie stehen Sie zu dieser Alternative?



Wolfgang Sidler

IT-Sicherheit an einen Outsourcer auszulagern kann per se für einige Unternehmen das Richtige sein, für andere ist dies jedoch die falsche Strategie. So genannte Managed Security Services wie zum Beispiel das Administrieren von Firewalls kann für ein KMU durchaus eine sehr gute Lösung sein. IT-Probleme lassen sich aber nicht auslagern – sie müssen zuerst intern gelöst werden. Vergessen Sie nicht, dass die Verantwortung ebenfalls nicht an einen Outsourcer delegiert werden kann.

In welchen Bereichen erwarten Sie als IT-Security-Experte die grossen Herausforderungen der kommenden zwei Jahre?

In den kommenden zwei Jahren wird das Thema IT-Compliance und IT-Governance eine sehr wichtige Rolle spielen. Unternehmen, die bereits Erfahrungen mit Sarbanes-Oxley (SOX) gemacht haben, kennen das Vorgehen und den Aufwand. Basel II wird ebenfalls langsam auf die Finanzunternehmen Einfluss haben. Jedoch sind hier die Massnahmen in Bezug auf die IT-Sicherheit noch nicht so ganz klar definiert. Ein weiterer Trend ist die Speicherung von Daten auf PDAs, Smartphones, Blackberrys, USB-Memory-Sticks und Notebooks. Für die IT-Security-Spezialisten wird es eine enorme Herausforderung sein, diese Mobilität in den Griff zu bekommen und die Daten entsprechend vor unbefugtem Zugriff zu schützen. Identity Management (User Administration) mit Single-Sign-on-Lösungen ist ebenfalls ein aktuelles Thema. Computer-Forensik wird immer aktueller, um interne Missbräuche zu untersuchen und nach einem Sicherheitsvorfall Beweismittel gerichtsverwertbar zu sichern. Auch das Thema Security Awareness darf nicht vergessen werden. Das Verhalten des Mitarbeiters ist massgeblich dafür verantwortlich, ob vertrauliche Daten das Unternehmen verlassen oder nicht. ■