

# IT-Sicherheit zu locker gesehen

9. Oktober 2011 | 17:55 | | Gerald Stoiber (SN). |

[Teilen](#)

[Teilen](#)

**Daten.** Firmen nehmen oft die Sicherheit ihrer IT-Systeme nicht wichtig genug. „Der Mensch bleibt die größte Schwachstelle“, sagen Experten.

Namen und Adressen von 25.000 Polizisten landeten im Internet, die Patientendaten der Tiroler Gebietskrankenkasse ebenfalls und Teile der Server des Bundesrechenzentrums wurden gehackt – alle paar Tage gab es in jüngster Zeit derartige Meldungen. Die SN erkundigten sich, wie es um das Sicherheitsbewusstsein der heimischen Unternehmen bei deren Computersystemen steht.

In den Einschätzungen darüber gibt es durchaus Unterschiede, doch einig waren sich die von den SN befragten Fachleute in einem Punkt: „Die größte Schwachstelle bleibt der Mensch.“ Bei Problemen gebe es oft nicht so sehr technische Lücken, sondern Fehler von Benutzern, sagt Gerhard Laga, Leiter des E-Centers in der Wirtschaftskammer Österreich (WKO). Etwa, dass Daten auf weniger gesicherten Servern gelagert und dann nicht wie vorgesehen wieder gelöscht würden. Das sei auch bei den Attacken der Gruppe Anonymous bei einem polizeinahen Verein und der Tiroler Gebietskrankenkasse der Fall gewesen. „Anonymous hat in wenigen Monaten das geschafft, was den IT-Security-Abteilungen in 20 Jahren nicht gelungen ist“, sagte ein Kenner der Branche den SN, der in diesem Zusammenhang nicht genannt werden will. Die jüngsten Vorfälle zeigten, „dass unsere Infrastruktur angreifbarer ist, als uns lieb ist“, sagt Josef Pichlmayr, Geschäftsführer der auf Antivirensoftware spezialisierten Firma Ikarus.

Insgesamt sei für viele Unternehmen IT-Sicherheit „seit Jahren das wichtigste Thema“, sagt Laga. Laut Umfragen hätten 95 Prozent der Unternehmen bereits in IT-Sicherheit investiert, also etwa in Virenschutz oder Firewalls. Vier von fünf Firmen benützten Datensicherung und Archivsysteme.

Die WKO bietet seit 1997 eine Roadshow zur IT-Sicherheit. „Telefit“ ist nächste Woche im Bundesland Salzburg zu Gast (17. 10. Zell am See, 18. 10. Wifi Salzburg, 19. 10. St. Johann/Pg.). Im Internet ([www.it-safe.at](http://www.it-safe.at)) gibt es ein Handbuch, das den eigenen Bedürfnissen angepasst werden kann. Kritischer sieht der Sprecher der IT-Security Expert Group in der WKO, Martin Prager, die Lage: „Das Bewusstsein ist viel zu gering, schon einfachste Probleme werden vernachlässigt“, sagt er. Wenn ein Server im Schauraum stehe, sei das, wie wenn man bei einem Haus die Tür versperre, aber die Dachluke offen lasse.

„Bei der Wartung und der Überprüfung gibt es Lücken“, sagt auch Pragers Stellvertreter, Gerald Kortschak aus Graz. Oft reagierten Kunden nach dem Motto, sie hätten eh einmal in die IT-Sicherheit investiert und das müsse reichen. Bei Problemen wollten sie dann oft rasch ihr Geld zurück. Das Minimum sei eine jährliche Überprüfung. Externe Fachleute seien zu bevorzugen: „Der Externe hat eine unbedarfte Vogelperspektive.“ Zu den Aufträgen gehört es laut Kortschak auch immer wieder, „über die Putzkolonne Leute einzuschleusen“. Diese müssten etwa überprüfen, ob Rechner oder Laptops ungesichert zugänglich seien. So liege die „Erfolgsquote“ – dass etwas nachjustieren ist – bei 70 bis 80 Prozent. Etwa die Hälfte der Firmen nehmen die Vorschläge an.

Pichlmayr betont, bei IT-Sicherheit komme das Florianiprinzip voll zum Tragen, da Hacker dort ansetzten, wo es am leichtesten möglich sei. „Bin ich besser geschützt als die meisten, passiert mir nichts.“ Der Ikarus-Chef sieht steigenden Leistungs- und Kostendruck sowie häufige Personalwechsel als Probleme. Zudem würden Verstöße gegen Datenschutzvorschriften in Österreich kaum geahndet. Schließlich könne die Datenschutzkommission nur Empfehlungen abgeben, habe selbst aber keine Exekutivgewalt.

Der Datenschutzrat wolle sich mit dem Problem demnächst befassen, erklärte Vorsitzender NAbg. Johann Maier (SPÖ). Im EU-Parlament will ÖVP-Mandatar Hubert Pirker auf eine EU-weite Harmonisierung der Straftatbestände im Bereich Datensicherheit drängen.

© SN/SW