Special Innovation

A Min Tjoa: „Viele Unternehmer sind der Meinung, ihre Firmen seien für Angriffe von außen uninteressant. Die Netzwerke solcher Firmen sind dann zumeist in geradezu abenteuerlicher Weise ungeschützt und damit hervorragende Ziele für Hacker-Angriffe“, erklärt der Obmann von Secure Business Austria.

Grob unterschätzte Gefahr

Sonja Gerstl

economy: ***Secure Business Austria arbeitet nun seit fast zwei Jahren im akademisch-industriellen Umfeld von Informationstechnologie (IT)-Sicherheit. Wie sind Ihre bisherigen Erfahrungen mit österreichischen Unternehmen? Wird die Bedeutung der IT-Sicherheit erkannt?***

A Min Tjoa: Das ist leider immer noch sehr unterschiedlich. Im Bereich der Großunternehmen ist das Bewusstsein diesbezüglich sehr ausgeprägt – hier wird entsprechend investiert und Informationssicherheit als „Business Enabler“ verstanden. Bei vielen Unternehmen aus dem Segment der KMU *(kleine und mittlere Unternehmen, Anm.)* wird IT-Sicherheit bestenfalls als notwendiges Übel, schlechtestenfalls als sinnlose Geldverschwendung gebrandmarkt. Viele Unternehmer sind der Meinung, ihre Firmen seien aufgrund ihrer überschaubaren Größe für Angriffe von außen „uninteressant“. Die Netzwerke solcher Firmen sind zumeist in geradezu abenteuerlicher Weise ungeschützt und damit hervorragende Ziele für Hacker-Angriffe. Hier ist viel Aufklärungsarbeit notwendig, obwohl etwa die Wirtschaftskammer mit ihrer „IT-Safe“-Initiative durchaus bereits viel geleistet hat.

Schätzen Sie die Gefahren für Unternehmen heute für gefährlicher ein als etwa vor zehn Jahren?

Auf jeden Fall. Auch kleinere Unternehmen verlagern immer mehr ihrer existenziellen Kernprozesse auf IT-Basis. Vor zehn Jahren waren die meisten Firmen noch via Wählleitungen mit dem Internet verbunden – falls es überhaupt einen Internet-Anschluss gab. Heute hat praktisch jeder einen Breitbandzugang, in vielen Unternehmen ist ein Ausfall der EDV mittlerweile mit administrativem Stillstand gleichzusetzen.

Wo setzt hier nun Secure Business Austria an?

Über ein duales Forschungskonzept: Auf der einen Seite behandeln wir äußerst aktiv die technische Seite. Die Stichworte dabei sind Malicious Code Detection, also die Erkennung von bösartigem Programmcode, oder Penetration Testing, das heißt die Erforschung neuartiger Methoden zum Eindringen in fremde Rechensysteme. Auf der anderen Seite beschäftigen wir uns intensiv mit den organisatorischen Aspekten. Dazu gehören die Bewusstseinsbildung bei Mitarbeitern und Geschäftsführung, die Erarbeitung sicherer, robuster Geschäftsprozesse und die Einbettung der EDV in einen vernünftig geregelten organisatorischen Rahmen.

Was? Sie bilden Hacker aus?

Im technischen Bereich werden natürlich die dafür erforderlichen Technologien sehr genau analysiert. Wir müssen forschen, wie Hacker und andere Angreifer arbeiten und welche Gegenmaßnahmen möglich sind. Das ist ein ständiger Wissenskampf, wenn Sie so wollen. Anders ist ein Schutz doch gar nicht möglich! Sicherheit durch Ignoranz ist in diesem Bereich sicherlich nicht zu erreichen.

Apropos Ignoranz: Wie stehen Sie zum deutschen „Hacker-Paragrafen“, mit dem die deutsche Bundesregierung den Gefahren durch das Internet Einhalt zu gebieten versucht?

Das ist meiner Meinung nach ein völlig falscher Ansatz. Damit werden legalen Experten die Werkzeuge entzogen, die in der Illegalität natürlich weiter massiv genutzt werden. Ich hoffe, dass sich Österreich nicht zu einer ähnlichen Verschärfung des Strafrechts hinreißen lässt.

Welche anderen Themen halten Sie in den nächsten Jahren für sicherheitsrelevant?

Einen wichtigen Schwerpunkt in unserer Forschung stellt die Datensicherheit für besonders sensible personenbezogene Daten dar – etwa im Gesundheitsbereich. Hier arbeiten wir an Methoden, die den strengen österreichischen Datenschutzbestimmungen entsprechen sollen und dennoch die Vorzüge der Informationstechnologie in der Medizin voll ermöglichen. Ein weiterer wichtiger Schwerpunkt ist die Frage der Organisationssicherheit in kleineren Unternehmen. Hier müssen noch die richtigen Ansätze entwickelt werden, die den Unternehmen tatsächlich helfen, ohne dabei zu viel administrativen Überbau zu erzeugen.

www.securityresearch.at

Vor allem in KMU wird Sicherheit bezüglich Informationstechnologie mitunter stiefmütterlich behandelt. Ihre Firmennetzwerke bieten eine hervorragende Angriffsfläche für Hacker. F.: Bilderbox.com

Zur Person

A Min Tjoa ist Obmann von Secure Business Austria und Leiter des Instituts für Softwaretechnik und Interaktive Systeme an der Technischen Universität Wien. Foto: M. Fuchs

Die nächste Generation

Neue wissenschaftliche Direktorin für das Gregor Mendel-Institut.

Ende November dieses Jahres hat sich Gründungsdirektor Dieter Schweizer (69) von der operativen Geschäftsführung des Gregor Mendel-Instituts (GMI) zurückgezogen. Das von Schweizer im Auftrag der Österreichischen Akademie der Wissenschaften (ÖAW) konzeptionell entwickelte, seit 2000 erfolgreich aufgebaute GMI am Campus Vienna Biocenter ist eine von drei neuen Forschungsgesellschaften der ÖAW im Rahmen der Exzellenzinitiative 2000. Das GMI ist die einzige außeruniversitäre Einrichtung in Österreich, die Grundlagenforschung in molekularer Pflanzenbiologie betreibt. Es bereichert den Campus Vienna Biocenter und spielt in der österreichischen Forschungslandschaft eine bedeutende Rolle.

Dem Erbgut auf der Spur

Nun hat die Österreichische Akademie der Wissenschaften GMI-Senior Scientist Ortrun Mittelsten Scheid zur interimistischen wissenschaftlichen Direktorin des Pflanzenforschungsinstituts bestellt. Mittelsten Scheid, seit 2004 am GMI, studierte in Hamburg Biologie, gefolgt von post-doktoraler Ausbildung am Max Planck-Institut für Zellbiologie in Ladenburg bei Hans-Georg Schweiger und an der ETH Zürich bei Ingo Potrykus. Von 1992 bis 2003 war sie im Team von Jerzy Paszkowski am Friedrich Miescher-Institut für Biomedizinische Forschung der Novartis Research Foundation in Basel maßgeblich an den dortigen bahnbrechenden Untersuchungen zur Epigenetik bei Pflanzen beteiligt. Ihr Hauptinteresse gilt epigenetischen Phänomenen in polyploiden Pflanzen. *sog*

www.gmi.oeaw.ac.at

Wechsel im GMI: Ortrun Mittelsten Scheid folgt Gründungsdirektor Dieter Schweizer. Foto: GMI

„Hacker-Paragraf“

Die deutsche Bundesregierung hat zur Bekämpfung des Terrorismus im Sommer 2007 den neuen Paragrafen 202 c StGB in Kraft gesetzt, der die Vorbereitung einer Straftat durch Herstellung, Beschaffung, Verkauf, Überlassung, Verbreitung oder Zugänglichmachen von Passwörtern oder sonstigen Sicherheitscodes für den Datenzugang sowie von geeigneten Computerprogrammen künftig mit Geldstrafe oder Freiheitsentzug bis zu einem Jahr unter Strafe stellt. Die damit kriminalisierten „Hacker-Tools“ dienen jedoch auch Netzwerkadministratoren, Software-Entwicklern und Experten aus dem IT-Sicherheitsumfeld dazu, Netzwerke und Endgeräte auf Sicherheitslücken hin zu prüfen.