

# Eine Nacht lang Internet-Hacker sein

**DATENSCHUTZ** Studenten schlüpfen in einem internationalen Wettbewerb in die Rolle krimineller Datenjäger – und lernen dabei, wie man IT-Systeme sicher macht.

VON MARA MERTIN, MZ

**REGENSBURG.** Im Computerraum herrscht angespannte Stille. Kaum die Hälfte der Plätze ist besetzt. Die Beleuchtung ist schummrig. Zwischen den Monitoren flackert das Licht einzelner Laptop-Bildschirme. Immer wieder klackert eine Tastatur. Das Team ist ungeduldig: Irgendetwas scheint schiefzulaufen.

Heute Nacht kämpfen Studierende, Doktoranden und wissenschaftliche Mitarbeiter des Lehrstuhls für Wirtschaftsinformatik Seite an Seite: Für die Regensburger Universität messen sie sich im IT-Sicherheits-Wettbewerb „International Capture The Flag“ (ICTF) mit Mannschaften aus aller Welt. Seit 2006 nehmen die Regensburger an solchen sogenannten „Hacker-Wettbewerben“ teil. „Defender of the Flag“ (Verteidiger der Flagge) nennen sie ihre 15-köpfige, in diesem Jahr ausschließlich männliche, Truppe.

In den Wettbewerben geht es traditionell darum, auf speziell präparierten Websites der anderen Teams versteckte Informationen (die Flags) zu stehlen. Zugleich gilt es, die Flags auf der eigenen Website vor gegnerischen Angriffen zu schützen. „Aber beim ICTF ist immer alles anders“, sagt Florian Scheuer, der die Regensburger Teilnahme koordiniert. Niemand könne heute einschätzen, welche Aufgabe die Spieler erwarten. Dann, endlich: Mit



**Konzentration im Regensburg-Team: Es gilt, Kontodaten zu klauen. Natürlich nur im Planspiel.**

Foto: Mertin

einer Stunde Verspätung trifft die Aufgabenbeschreibung vom Veranstalter aus dem kalifornischen Santa Barbara ein. Nervös öffnet ein Spieler die Datei. Die Defender drängen sich um ihn.

Diesmal schlüpfen die Wissenschaftler in die Rolle eines Kriminellen. Sie sollen Kontodaten fiktiver Netz-Nutzer stehlen. Das Spiel findet in einem virtuellen privaten Netz statt. Dieses ähnelt in seiner Funktionsweise dem Internet, ist aber nicht mit ihm verbunden. Die fiktiven Nutzer, ein Programm des Veranstalters, tätigen zunächst ihre Bankgeschäfte

und surfen dann im Spiel-Internet. Um die Kontodaten stehlen zu können, müssen die Teams möglichst viele Nutzer auf ihre eigene, manipulierte Website locken. Erst dann können die Daten-Jäger im System der Nutzer nach Sicherheitslücken suchen und ihnen Schadcodes unterschieben – die lesen auf dem Rechner der Nutzer dann Kontodaten aus.

„Auf diese Weise erkennen wir Angriffsmöglichkeiten, die wir in zukünftigen Projekten und Arbeiten verhindern werden“, sagt Scheuer. Bei den Wettbewerben ist es an der Tagesord-

nung, sich mit unbekanntem Tools und Programmiersprachen auseinanderzusetzen. Um das erworbene Wissen weiterzugeben, haben die Regensburger Studierenden die „Arbeitsgruppe IT-Sicherheit“ gegründet.

Um halb drei Uhr nachts verlassen die letzten Kämpfer müde das Schlachtfeld. Unter 51 Mannschaften haben sie Platz 17 errungen. Die Defender sind stolz auf sich. Schließlich seien sie keine echten Informatiker. „Und für eine Außenseitermannschaft“, sagt Scheuer, „ist das doch Klasse, oder?“

## Nutzer müssen sich selbst schützen

Den Wettbewerb der „Hacker“ tragen Studenten von Prof. Hannes Federrath aus, Inhaber des Lehrstuhls für Wirtschaftsinformatik an der Universität Regensburg. Ein Studienschwerpunkt hier ist die Informationssicherheit im Internet und in IT-Systemen.

*Beim diesjährigen ICTF haben die Studenten als Hacker fiktive User angegriffen. Welchen Sinn hat dieser Rollentausch?*

Die Studenten haben sich in die Rolle des Hackers versetzt, um zu überlegen, wie dieser vorgehen würde. Wenn ich weiß, wie ein System angegriffen werden kann, bin ich in der Lage, es besser

abzusichern und zu schützen.

*Wie kann ich mich als Nutzer vor Daten-Jägern schützen?*

Keine aus dem Internet geladenen Raubkopien von Programmen verwenden und das System aktuell halten. Programm-Updates beseitigen Fehler und Sicherheitslücken, die Kriminelle nutzen könnten. Bei Freeware und Shareware sollte man

den Empfehlungen von PC-Zeitschriften folgen und nicht

### INTERVIEW



**PROF. HANNES FEDERRATH**

Wirtschaftsinformatiker

Foto: Privat

folgen und nicht wahllos Programme ausprobieren.

*Woran erkenne ich eine Website, die versucht, Daten abzugreifen?*

Äußerlich an gar nichts. Moderne Browser wie Firefox können den Nutzer warnen, wenn er bekannte, unsichere Seiten aufruft.

*Gibt es überhaupt sichere Websites?*

Websites, die über https abgerufen wer-

den, also verschlüsselt sind, bieten einen gewissen Schutz. In diesem Fall kann der Urheber bestimmt werden und dieser legt sicherlich Wert darauf, nur gefahrlose Inhalte auf seiner Seite zu haben. Etwaige Sicherheitswarnungen, beispielsweise Zertifikatsfehler, sollten aber auf jeden Fall ernst genommen werden. Generell gilt: Das Erscheinungsbild ist auch hier keine Garantie.

*Können uns Gesetze vor Kriminalität im Internet schützen?*

Nur begrenzt. Das Internet ist ein internationaler Raum, für den es noch keine internationalen Gesetze gibt. Wichtig ist, sich selbst zu schützen. (mme)