Planetenforscher sucht Leben im All Interview Seite 12 Bizzare Schnecken-Sexpraktiken S. 13



Überall in den Netzen gibt es digitale Schlupflöcher. Diese aufzuspüren versuchen Cyber-Kriminelle genauso wie Hacker im Auftrag des Staates. *Foto: fotolia*

# In der Haut des Hackers

**In der Mini-Stadt CyberCity in den USA rüsten sich IT-Experten für den Krieg der Computer. Auch hierzulande schlüpfen Sicherheitsforscher in die Rolle von Datendieben und Netzterroristen, um sich gegen großflächige Systemausfälle zu wappnen.**

*Karin Krichmayr*

Es ist eine Art Spielzimmer, in dem die USA den Cyberkrieg proben. In CyberCity – so heißt das vom Pentagon beauftragte Projekt des Sans Institute – gibt es Miets-häuser, Fabriken, Banken, ein Kraftwerk, ein Spital, ein Kaffeehaus mit Gratis-WLAN. Rundherum führt eine Modelleisenbahn. Auf knapp fünf Quadratmetern entsteht eine Kleinstadt im Puppenhausformat. Winzige Lampen erleuchten die Fenster, gesteuert von denselben Stromnetzkomponenten wie in der echten Welt. Jeder der 15.000 virtuellen Bewohner verfügt über E-Mail-Accounts, Bankkonten und Passwörter.

CyberCity ist ein Trainingsplatz für im Auftrag der Regierung stehende Hacker, die sich auf den vielbeschworenen Krieg der Computer vorbereiten. Sie sollen lernen, möglichst rasch auf digitale Attacken zu reagieren – die augenblicklich sichtbar werden, wenn etwa der Strom ausfällt. Andere Missionen klingen richtig filmreif: zum Beispiel einen mit Massenvernichtungswaffen beladenen Zug umzuleiten. Oder einen Hacker aufzuhalten, der sich ins System des Spitals eingeklinkt hat, um einen prominenten Patienten per Überdosis umzubringen.

Die Modellstadt, die ab März in Betrieb gehen soll, ist nur eine von vielen virtuellen Umgebungen, in denen Militärs und Wissenschafter die Bedrohungen aus dem Cyberspace erforschen. Im Normalfall werden die Netzwerke jedoch allein im Computer simuliert. Dass nun ein Musterstädtchen hinzukommt, steht auch für die wachsende Angst vor einem Cyberkrieg mit ganz realen Auswirkungen, die in den USA umgeht.

Noch konzentrieren sich Hackerattacken auf Datenklau und Spionage, wie zuletzt im US-Energieministerium, bei drei großen US-Zeitungen und bei Twitter. Doch Cyberangriffe können nicht nur wirtschaftlichen Schaden anrichten, sondern auch große Teile lebenswichtiger Infrastruktur lahmlegen – vom Stromnetz über Schleusentore bis hin zu Atomkraft- und Chemiewerken.

## Verwundbare Systeme

„In allen hochtechnologisierten Ländern ist die Verwundbarkeit gegenüber Cyberattacken relativ hoch, da die kritische Infrastruktur weitgehend über IT-Systeme gesteuert wird", sagt Thomas Bleier, Sicherheitsforscher vom Austrian Institute of Technology (AIT). „Dazu kommt das Risiko einer Bedrohung von außen, etwa aus politischen Gründen."

Während sich die USA mit einer eigenen Cyber-Streitkraft und martialischer Rhetorik schon für Gegenangriffe im Internetkrieg rüsten, setzt man in Europa vor allem auf Defensive. Die EU pocht auf eine Meldepflicht für Unternehmen, Behörden, Banken, Energieversorger, Verkehrsbetriebe etc., sollten sie einen Angriff auf ihre Netze registrieren. So sollen Schwachstellen und Gegenstrategien aufgespürt werden. Österreich liegt laut einem aktuellen Cyberattack-Stresstest des Brüsseler Thinktanks Security and Defence Agenda (SDA) mit dreieinhalb von fünf Sternen im weltweiten Mittelfeld.

Etwas mehr Punkte könnte die Cyber-Sicherheitsstrategie bringen. Sie soll bis zum Frühjahr unter Dach und Fach sein, um die auch hierzulande grassierende IT-Kriminalität in den Griff zu bekommen und Schutz gegen terroristisch motivierte Computerinfarkte zu bieten. Die wissenschaftliche Basis dafür wird in mehreren Forschungsprojekten erarbeitet, darunter auch jene des Sicherheitsforschungsprogramms „Kiras", das vom Verkehrsministerium initiiert wurde.

„Auf staatlicher Ebene fällt es oft schwer, die aktuelle Bedrohungslage zu eruieren, weil so viele Abhängigkeiten bestehen", sagt der AIT-Experte Thomas Bleier. Er leitet das Kiras-Projekt „Cyber Attack Information System (CAIS)", an dem auch das Bundeskanzleramt sowie Innen- und Verteidigungsministerium beteiligt sind. „Wir modellieren diese Abhängigkeiten, also etwa welche Auswirkungen eine Störung des Telekommunikationssystems auf die Strom- und Bahnnetze hat."

Die IT-Security-Forscher testen an diesen Modellen verschiedene Cyberangriffe – von sogenannten „Denial of Service"-Attacken, die zum totalen Systemausfall führen, bis hin zu gezielt eingeschleusten Trojanern und Würmern –, um Schwachstellen und kritische Punkte ausfindig zu machen. Zudem wird mit T-Mobile und T-Systems ein Tool entwickelt, das erlauben soll, verdächtige Datenaktivitäten schneller zu identifizieren, auch wenn sie einem unbekannten Muster folgen.

Dem Katz-und-Maus-Spiel, in dem sich Hacker und Cyber-Cops gegenseitig zu überlisten versuchen, begegnet ein anderes Forscherteam gleich mit der Spieltheorie – mit der Entscheidungssituationen modelliert werden, in denen sich mehrere Beteiligte gegenseitig beeinflussen. „Wir wollen den Konflikt zwischen Angreifer und Verteidiger mathematisch darstellen, um das System möglichst optimal gegen Ausfälle oder Lauschangriffe abzusichern", sagt Stefan Rass von der Universität Klagenfurt.

## Simultane Bedrohungen

Rass ist Mitarbeiter beim Kiras-Projekt „Risikomanagement für simultane Bedrohungen", das ebenfalls von Innen- und Verteidigungsministerium begleitet wird. Dabei sollen mehrere, oft konkurrierende Aspekte berücksichtigt werden – wie etwa die Vertraulichkeit von sensiblen Daten auf der einen und die möglichst schnelle Verfügbarkeit auf der anderen Seite. „Am Ende soll ein Risikomanagement-Prozess herauskommen, der individuell auf verschiedene Netzwerke angewendet werden kann", sagt Rass.

Auch wenn Österreich bisher von umfassenden Attacken aus den Weiten des Cyberspace verschont blieb – mit gezielten Angriffen muss gerechnet werden. „Besonders riskant ist die schleichende Evolution der Systeme", sagt Thomas Bleier. „Die Stromnetze etwa werden nicht von heute auf morgen zu Smart Grids. Es kommen ständig neue Funktionen dazu, und die Auswirkungen werden nicht immer mitgedacht." Digitale Schlupflöcher gibt es überall, und so gilt es für die Sicherheitsforscher, ständig Schritt zu halten mit neuen Technologien wie dem Cloud-Computing. Bleier ist überzeugt: „Da kann noch einiges auf uns zukommen."

TERMIN

## Sicherheit als Risiko

Wie es dazu kommt, dass Sicherheitsversprechen zum Risiko für den Frieden, für die Lebensumstände, das Ökosystem oder das Klima werden können – das steht im Zentrum des Symposions Dürnstein zum Thema „Risiko Sicherheit", das von 14. bis 16. 2. im Stift Dürnstein stattfindet. Die von Wachau Kultur Melk und der Donau-Uni Krems veranstaltete Tagung widmet sich zum zweiten Mal einem gesellschaftspolitischen Brennpunkt, und zwar aus dem Blickwinkel von Theologie und Philosophie.

Den Auftakt macht die US-Soziologin und Globalisierungsforscherin Saskia Sassen mit einem Vortrag zur Sicherheitspolitik als Bedrohung für die persönliche Freiheit. Weiters diskutieren internationale Experten über sicheres Wachstum, Ernährungssicherheit und Sicherheitstechnologien. Vertreter aller Religionen werden zudem über den sicheren Tod und das Jenseits sprechen. (kri)