Gefährliche **Fallen**

IT-Kriminalität ist ein lohnendes Geschäft mit vergleichsweise niedrigem Risiko, sagt Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Ein Interview zur Lage der IT-Sicherheit in Deutschland.

Herr Dr. Helmbrecht, Anfang März hat das BSI einen Bericht zur Lage der IT-Sicherheit in Deutschland vorgestellt. Sind sich die Bürger bewusst, welche Gefahren im World Wide Web lauern?

Die Sicherheit der Privatsphäre und der persönlichen Informationen ist heute für die meisten IT-Nutzer wichtig. In Deutschland sehen wir im internationalen Vergleich sogar ein hohes Sicherheitsbedürfnis. Das wirkt sich auch auf das Verhalten der Anwender aus: In unseren Umfragen geben über 90 Prozent der Internet-Nutzer an, einen Virenschutz einzusetzen, und auch die Nutzung der Personal Firewalls steigt an. Medienwirksame Vorfälle wie der Conficker-Wurm tragen dazu bei, dass Sicherheitsmaßnahmen nicht nur als notwendig, sondern auch als nützlich angesehen werden. Diese Botschaft ist bei den Verwaltungen, in der Wirtschaft und beim Bürger gleichermaßen angekommen.

Was tut das BSI, um die Bürger vor zunehmenden Gefahren im Internet zu schützen?

Den Privatanwendern geben wir mit dem Bürger-CERT, einem kostenfreien Warn- und Informationsdienst, und mit den Internet-Seiten BSI-für-Bürger Hilfestellungen, welche aktuelle Bedrohungen bestehen und wie man sich schützen kann. Zudem engagieren wir uns im Verein Deutschland sicher im Netz und in der europäischen Initiative Klick-safe, die praktische und einfache Hilfen für Privatleute anbieten, um sich im Netz sicher bewegen zu können.

Wie sieht es mit dem IT-Sicherheitsbewusstsein der öffentlichen Verwaltung aus?

Die Sensibilität wächst auch hier, nicht zuletzt, weil die Bürger anspruchsvoller werden. Sie stellen nicht nur hohe Anforderungen an die Verfügbarkeit von Verwaltungsdienstleistungen auf elektronischer Ebene, sondern sie fordern auch zunehmend sichere Kommunikationswege und legen Wert auf Vertraulichkeit und Datensicherheit. Diese Sensibilität auf beiden Seiten führt dazu, dass die Themen E-Government und IT-Sicherheit – wie bei dem Projekt De-Mail – heute Hand in Hand gehen. Und das zu Recht, denn auch die Netze der Bundesregierung sind täglich Angriffen und illegalen Zugriffsversuchen ausgesetzt.

Wie hat sich die Bedrohungslage nach Ihrer Beobachtung in den vergangenen Jahren entwickelt?


Dr. Udo Helmbrecht

Insgesamt ist die Lage der IT-Sicherheit unverändert ernst, wobei einige Angriffsmethoden an Bedeutung verlieren, während andere immer beliebter werden. Wir haben zwar auf viele Bedrohungen mittlerweile Antworten entwickeln können. Doch durch die zunehmende Verlagerung alltäglicher Aktivitäten ins Internet ist IT-Kriminalität für Angreifer heute weiterhin ein lohnenswertes Geschäft bei vergleichsweise niedrigem Risiko. Mittlerweile nutzen über die Hälfte der Anwender das Internet um beispielsweise Einkäufe zu tätigen oder Bankgeschäfte zu erledigen. In der Folge dieser Entwicklung nehmen auch die Professionalisierung und Kommerzialisierung der Cyber-Kriminalität zu. Phishing beispielsweise, also das Entwenden persönlicher Daten durch gefälschte E-Mails oder Web-Seiten, ist so ein Phänomen, das mittlerweile ja vielen Nutzern ein Begriff ist.

Welche Angriffsmethoden würden Sie als besonders gefährlich für die IT-Sicherheit einstufen?

Der klassische Virus per E-Mail hat zwar noch nicht ausgedient, aber viele Gefahren gehen heute von infizierten Web-Seiten aus, bei denen sich der Nutzer die Schad-Software quasi selbst abholt. Diese besonders gefährlichen Fallen heißen Drive-By-Downloads und tauchen zurzeit immer häufiger auf. Dabei wird allein durch das Aufrufen einer präparierten Seite im Browser eine Schad-Software installiert. Einen anderen großen Teil der Schadprogramme stellen heute so genannte Trojanische Pferde dar. Diese werden zunehmend komplexer und mit immer mehr Funktionen ausgestattet. Die Software spioniert beispielsweise Zugangskennungen aus, lässt den Zugriff auf die Daten des Nutzers zu oder ermöglicht eine Fernsteuerung des Rechners.

„Die Themen E-Government und IT-Sicherheit gehen heute Hand in Hand."

Der neue elektronische Personalausweis soll auch die Sicherheit von Internet-Transaktionen erhöhen. Wie beurteilen Sie dies?

Der elektronische Personalausweis ist definitiv nicht nur ein Sicherheitsgewinn bei der Identifizierung auf Reisen oder gegenüber Behörden. Die Informationen, die optisch auf dem Ausweis zu sehen sind, werden künftig auch auf einem berührungslosen Funk-Chip gespeichert sein. Damit ist im Internet eine verlässliche Online-Authentisierung möglich. Gegenüber E-Business- und E-Government-Dienstleistern kann sich der Nutzer damit ausweisen und stellt dabei seinem Gegenüber nur die im konkreten Fall erforderlichen Informationen zur Verfügung. Diese eID-Funktionen sind im Online-Geschäft ein großer Sicherheitsgewinn und werden kriminelle Online-Aktivitäten wie zum Beispiel Phishing deutlich erschweren. Darüber hinaus ist beim neuen Personalausweis auch eine Signaturfunktion möglich. Sie ist optional und kann vom Karteninhaber separat aktiviert werden. Das geht auch noch im Nachhinein. Diese Funktion bietet ebenfalls zusätzliche Sicherheit bei Online-Geschäften und im E-Government und auch einen gewissen Komfort für den Nutzer.

Im Oktober wechseln Sie als Direktor zur European Network and Information Security Agency. Welche Aufgaben hat diese Organisation?

Die ENISA ist die europäische Anlauf- und Beratungsstelle bei Fragen der Netz- und Informationssicherheit für alle EU-Mitgliedsstaaten und die EU-Organe. Ihre Aufgabe ist es, diese Institutionen dabei zu unterstützen, IT- und Informationssicherheit zu gewährleisten und Sicherheitslücken zu bewältigen. Schwerpunkte der Tätigkeit der ENISA sind zum Beispiel die Beratung und Unterstützung der Kommission und der Mitgliedsstaaten in ihrem Dialog mit der Industrie, um sicherheitsrelevante Probleme bei Hardware- und Software-Produkten anzugehen.

Moderne Gesellschaften sind von funktionierenden IT-Infrastrukturen abhängig. Wo sehen Sie die wesentlichen Herausforderungen für Staat und Kommunen, um Vertrauen in der vernetzten Welt zu gewährleisten?

Für Staat und Kommunen gilt dasselbe wie für Unternehmen oder Privatpersonen in der heutigen vernetzten Welt: Je mehr wir die Informationstechnik einsetzen, umso wichtiger ist es, sie sicher zu gestalten. Um das zu erreichen, müssen alle Beteiligten in ihrem Verantwortungsbereich für Sicherheit sorgen, vom Hersteller bis zum Nutzer. Der staatliche Bereich hat dabei zum einen die Pflicht, die eigene Kommunikation mit den Bürgern und mit Unternehmen sicher zu gestalten. Zum anderen sollte er auf regulierender Ebene dazu beitragen, die Voraussetzungen für eine sichere vernetzte Welt zu schaffen. Was auf Bundesebene getan werden kann – beispielsweise mit dem BSI-Gesetz oder dem IT-Investitionsprogramm – ist dabei ein wichtiger Teil. Sicher ebenso wichtig ist aber die internationale Zusammenarbeit, sei es in der EU oder darüber hinaus. Kriminalität in einer vernetzten Welt kann letzten Endes nur in internationaler Zusammenarbeit erfolgreich bekämpft werden.

Interview: Alexander Schaeff

Link-Tipp

Weitere Informationen über das Projekt Bürger-CERT, das Sicherheitsportal des BSI sowie die Initiativen Deutschland sicher im Netz und Klick-safe:

- **www.buerger-cert.de**
- **www.bsi-fuer-buerger.de**
- **www.sicher-im-netz.de**
- **www.klicksafe.de**

Weitere Links finden Sie unter www.kommune21.de.