Hackerangriffe sind nicht immer kompliziert

Sicherheit in der Informationstechnik sollte jedes Unternehmen ernst nehmen – auch ein Laie kann gefährlich werden

Hacken kann jeder. Das haben IT-Sicherheitsexperten auf der Computermesse Systems in München eindrucksvoll demonstriert: Mit einfachen Mitteln kann jeder zum Internetbetrüger werden. Ein geschärftes Bewusstsein für Sicherheitsdenken ist daher gefragt.

Von Cinthia Briseño, München

Sebastian Schreiber ist ein junger, sympathischer Typ. So wie er auf der Bühne steht, im adretten Anzug, vermittelt er nicht gerade den Eindruck eines typischen Hackers, wie man ihn sich als Laie wohl vorstellen mag. Doch ganz schnell wird deutlich: Sebastian Schreiber ist ein Experte. Er weiß genau, wie sich Betrüger im Internet bewegen.

Vergangene Woche hatte Schreiber in der Sendung „Stern-TV" vorgeführt, wie man sich Musik kostenlos über das Internet ziehen kann, ohne sich dabei strafbar zu machen.

Jetzt – auf der Computermesse Systems in München – hat es der Geschäftsführer der Tübinger IT-Sicherheitsfirma Syss auf eine Webseite der Erdinger Brauerei abgesehen: Im Forum des Erdinger Bundesliga-Tippspiels können sich Mitglieder gegenseitig Nachrichten schicken. Es geht ganz schnell: Schreiber registriert sich als Nutzer des Forums, schickt sich selbst eine Nachricht, ruft diese ab und verändert dann in der Adresszeile des Webbrowsers einfach eine Zahl. „ID=40632" steht dort irgendwo. Schreiber löscht die „2", tippt stattdessen eine „1" ein, drückt die Eingabetaste und schon landet er in einer E-Mail von einem gewissen Harry, die Sebastian Schreiber eigentlich nichts angeht.

URL-Manipulation nennt sich diese recht simple Art eines Hackerangriffs. So funktionieren viele Betrügereien im Netz. Ein ähnlicher Trick genügt, und Schreiber hat eine Pizza Quattro Stagioni für einen statt 5,90 Euro in seinem virtuellen Warenkorb.

An Schreibers Seite auf der Bühne des Computermesseforums der IT-Security-Area steht der Rechtsanwalt Jyn Schulze-Melling. Bisher hat er alle Aktionen Schreibers kommentarlos beobachtet. Doch als Schreiber auf den Bestellknopf drücken möchte, schaltet er sich ein: „Wer sich durch einen solchen Vorgang im Internet einen Preisvorteil verschafft, begeht Computerbetrug." Der Strafbestandskatalog im Strafgesetzbuch sei umfassend. Mittlerweile gebe es für alle möglichen Internetdelikte einen passenden Strafbestand. So verzichtet Schreiber lieber darauf, die billige Pizza zu bestellen, und fährt mit der Demonstration seines Live-Hacks fort.

Für ein großes Aha-Erlebnis unter den Zuschauern sorgt Schneiders präparierter USB-Stick. Einmal in den Computer gesteckt, öffnet sich automatisch ein Trojaner. Es bedarf nicht viel Fantasie, um sich vorzustellen, dass sich mit dieser Methode ziemlich leicht großer Schaden anrichten lässt.

„Für Trojaner gibt es einen Markt, sie sind käuflich ohne weiteres erwerblich. Ab 1500 Euro sind schon sehr effektive Tools zu haben", sagt Schreiber und warnt davor, fremde USB-Sticks einfach in den Computer zu stecken. Neuere USB-Sticks seien in der Lage, dem Computer vorzugaukeln, ein CD-ROM-Laufwerk zu sein. Deshalb würden sich selbst startende Programme auch als solche erkannt und ausgeführt. Schreiber empfiehlt darum jedem, die „Autorun-Funktion" auf dem Rechner zu deaktivieren, selbst wenn dieser kein CD-ROM-Laufwerk habe. Dies sei der einzig wirksame Schutz vor böswilligen Absichten, sagt Schreiber, „Firewalls und Antivirensoftware helfen da gar nicht."

Sebastian Schreiber kennt die Tricks der Betrüger im Internet. Foto Syss

Mit Hilfe eines Trojaners die Rechner anderer auszuspionieren ist das eine. Mittlerweile haben Hacker aber auch Handys im Visier, weshalb trojanische Pferde auch für Mobilfunkgeräte entwickelt werden. Ein „trojanisiertes Handy", wie Schreiber es nennt, liefert dann unter Umständen ganz neue Arten privater Daten. Zum einen lässt sich darüber der Aufenthaltsort einer Person ermitteln, zum anderen kann ein Handy mit einer solchen Schnüffelsoftware auch leicht zu einer Wanze werden: Das Handy baut unbemerkt eine Verbindung zum Handy des Hackers auf, und so kann dieser alle Gespräche des Handynutzers mithören.

Und so liefern sich Hacker und Unternehmen zur IT-Sicherheit ständig ein Rennen um die neueste Sicherheitslücke und die dazu passende Schutztechnologie. Der Präsident des Bundesamts für Sicherheit in der Informationstechnik, Udo Helmbrecht, spricht nicht ohne Grund von möglichen Bedrohungsszenarien, weshalb der IT-Sicherheitsmarkt auch künftig weiterhin wachsen würde – ebenso wie der „Cybercrime".

Stuttgarter Zeitung
Mi, 24.10.2007