

COMPUTER

Bezahlter Einbruch

Ein Informatiker aus Tübingen ist berufsmäßiger Hacker: Großunternehmen beauftragen ihn damit, Sicherheitslücken in ihren Firmennetzen aufzuspüren.

Wenn Sebastian Schreiber von Computereinbrüchen redet, beginnen seine Augen zu leuchten: „Dezember“, sagt er, „war ein toller Monat, da haben wir fast jeden Tag ein anderes Firmennetz geknackt.“

Für Schreiber ist es nur eine Frage der Zeit, bis er ein Schlupfloch findet. „Manchmal ist es richtig mühsam, und wir brauchen mehrere Wochen für die Analyse. Aber meist reichen ein paar Stunden, dann sind wir drin.“

Schreiber ist Anfang dreißig und entspricht weder vom Alter noch vom Aussehen dem Klischee eines Hackers. Statt Kapuzenshirt trägt er meist Krawatte zum dunklen Anzug. Und mit seinem Topfhaarschnitt würde er auch in einem Priesterseminar nicht auffallen.



FRANCIS GEORGE

Profihacker Schreiber (in Las Vegas)
Mit „Google“ auf der Suche nach Opfern

Doch wenn Schreiber sein Notebook aufklappt, um eine Kostprobe seines Könnens zu geben, verwandelt sich der freundliche junge Mann in einen raffinierten Einbrecher. „Um ein Opfer zu finden, benutze ich einfach die Suchmaschine ‚Google‘“, sagt er und tippt ein paar Begriffe ein, um ungeschützte Server zu finden.

Etliche Web-Adressen werden angezeigt, darunter sogar das Massachusetts Institute of Technology (MIT) bei Boston, das Mekka der digitalen Revolution. „Nicht mal

die sind in der Lage, ihre vertraulichen Informationen zu schützen“, sagt Schreiber und kann ein ironisches Grinsen nicht verbergen: „Die haben zwar ein sehr gutes Passwort – aber es ist keine gute Idee, dieses Passwort im Web zu veröffentlichen.“

Er klickt weiter. „Hier drückt ein gewisser Richards an der Universität Waterloo gerade den Kostenplan für ein Symposium aus. Interessant.“ Er navigiert zum deutschen Internet-Laden pc-webstore24.de und wählt einen Flachbildschirm für 474 Euro aus. „Aber ich verhandle ein bisschen nach“, sagt er und hat nach ein paar Klicks die Preisangabe auf 4,74 Euro manipuliert. „Jetzt könnte ich den Bildschirm bestellen und dann bei Ebay verkaufen. Da wäre eine gute Gewinnmarge drin.“

Ist die Bekanntgabe dieser Sicherheitslücke nicht schon Beihilfe zu Straftaten? „Nein, das habe ich natürlich vorher mit meinem Anwalt geklärt“, sagt Schreiber: „Wenn ein Internet-Laden sein Informationssystem nicht schützt, kann er Eindringlinge nicht verklagen. Erst, wenn ich das ‚nachverhandelte‘ Schnäppchen bestellen würde, wäre das illegal. Aber so etwas tue ich natürlich nicht.“

Schreiber ist hauptberuflicher Rechnerknacker, seine Dienste sind käuflich. Sein Tagessatz: rund 1300 Euro. Doch er steht nicht im Dienst der Mafia, sondern ist unter anderem tätig für DaimlerChrysler, SAP,

IBM, den TÜV und die Europäische Kommission. Der Test von Websites ist dabei nur ein allererster banaler Einstieg in eine Analyse. Meist lautet sein Auftrag, hausintern das System daraufhin zu untersuchen, ob und wie leicht sich Unbefugte Zugang zu geheimen Daten verschaffen können.

Vor knapp sieben Jahren, als Informatikstudent, gründete Schreiber in seiner Heimatstadt Tübingen das Beratungsunternehmen Syss GmbH. Heute hat der ehemalige Zivildienstleistende elf Mitarbeiter, berät die Bundeswehr und schult Ermittler der Landeskriminalämter.

Schreibers Eltern, ein Richter und eine Lehrerin, wollten eigentlich, dass der Junge Akkordeon lernt und Musiker wird. Die Liebe zur Tastatur blieb zwar, doch als Zehnjähriger erprobte er seine Fingerfertigkeit lieber an der Klaviatur seines C-64-Rechners. Im Abenteuerspiel „Das Drachental“ fand er schnell ein paar Sicherheitslücken, die es ihm erlaubten, sich unendlich viele Leben zu erschleichen, den Drachen zu besiegen oder die Königstochter zu heiraten.

Nach einem Praktikum bei den Stadtwerken folgte das Studium der theoretischen Informatik. Im Rahmen seiner Diplomarbeit zum Thema Sicherheit erlaubte ihm sein Professor, testweise in den Uni-Rechner einzudringen – eine einfache Fingerübung.



Rechenzentrum von SAP (in Walldorf)
Gefährliche Gefahrenabwehr

Seitdem führt Schreiber für Unternehmen sogenannte Penetrationstest durch: Nach dem Unterschreiben von allerlei Verschwiegenheitsverträgen greift er die Computersysteme der Auftraggeber an – bevor es andere tun, die ohne offizielle Lizenz zum Hacken agieren. Hat er eine Schwachstelle gefunden, berät er den Kunden, wie sich die Lücke schließen lässt.

Die kalkulierten Grenzverletzungen von Schreibers Zunft sind nicht unproblematisch, sie setzen ein Höchstmaß an Vertrauen seiner Auftraggeber voraus. Schließlich könnten die Experten theoretisch ihre Insiderkenntnisse missbrauchen, um sie später einmal anonym zu erpressen.

So werfen Penetrationstests immer wieder schwierige Fragen auf. Einerseits können sie wichtig sein für die Gefahrenabwehr, andererseits könnten sie auch selbst zur Gefahr werden.

Schreibers Team ist auf einen engen Kontakt zum Untergrund angewiesen, um auf dem neuesten Stand zu bleiben. Ständig informieren sich seine Mitarbeiter in einschlägigen Internet-Foren und auf Hackertreffen.

Wie intensiv darf der Austausch mit dem Untergrund sein? Das Thema spaltet die Branche, doch in einem sind sich alle einig: „Für uns“, sagt zum Beispiel Lutz Hausmann von der Lüneburger Firma Securepoint, „ist das Know-how von Hackern wertvoll, um Einblicke in die Denkweise möglicher Angreifer zu bekommen.“

Da war es für Hausmann nur konsequent, dass er auch dem Hacker aus Wafensen, der vor einem Jahr mit dem Sasser-Virus Millionenschäden verursachte, einen Ausbildungsplatz anbot.

Schreiber dagegen würde Vorbestrafte prinzipiell nicht einstellen, um seine Kunden nicht zu beunruhigen. Zu derlei vertrauensbildenden Maßnahmen dürften auch sein Anzug und sein seriöses Auftreten zählen. Nur das Leuchten seiner Augen verrät etwas vom diebischen Spaß, den das Computerknacken ihm immer noch macht.

HILMAR SCHMUNDT