

Bericht in TagesAnzeiger Digital (www.hacker.tagesanzeiger.ch)

«Wargames» in der Schweiz: Informatiker üben für den Cyber-Krieg

Von Anatol Heib. Aktualisiert am 21.04.2009

In Rapperswil hackten Informatiker an einem Kongress Passwörter und E-Banking-Daten – zu Übungszwecken. Ein Spam-Jäger informierte die Teilnehmer über die immer raffinierteren Methoden der Cyber-Mafia.



Teilnehmer am «Swiss Cyber Storm 2».

Links [Hacking Lab](#) / [Abuse-Blog](#)

Hacken für die gute Sache

Sicherheitsunternehmen wie Compass Security verdienen mit dem Knacken von Netzwerken ihr Geld: «Ethical Hacking» nennen sie ihre Tätigkeit. Unter diesem Begriff wird in der Regel eine Hacker-Tätigkeit verstanden, die innerhalb der geltenden Gesetze stattfindet. An ein entsprechendes Zertifikat kommt man nur über den Besuch eines spezifischen Kurses heran. Dieser ist in der Regel mit relativ hohen Kosten verbunden und an bestimmte Bedingungen geknüpft.

Diese so genannten White Hacker wie jene von Compass Security greifen im Auftrag von Firmen deren Netzwerke und Server an – und zeigen Schwachstellen auf. Sie sind das moralische Gegenüber zu den bösen Black-Hat-Hackern.

IT-Sicherheitsleute, Studenten und andere Interessierte schlüpfen am 18. und 19. April an der «Swiss Cyber Storm 2» in die Rolle von Hackern. Der Anlass wurde vom Schweizer Sicherheitsunternehmen Compass Security und der Hochschule für Technik in Rapperswil organisiert. In der Aula der Schule lösten die über 100 Teilnehmer an Laptops sogenannte «Wargames»: Aufgaben, in denen sie typische Hackerangriffe durchspielten. Besucher konnten ihnen über die Schulter blicken und erhielten an Vorträgen Tipps für die eigene PC-Sicherheit.

Cyberstorm-Teilnehmer knackten Passwörter, täuschten eine falsche Identität vor, hackten Daten fürs Online-Banking oder versuchten mit einem Link im E-Mail, jemanden auf eine präparierte Seite zu locken. «Nur wer in die Rolle der Hacker schlüpft, kennt ihre Methoden und kann sie mit den eigenen Waffen schlagen», sagt Ivan Bütler von Compass Security. Er vergleicht die Wargames mit Manövern der Armee, die so den Ernstfall probt. Für gelöste Rätsel erhielten die Teilnehmer Punkte, die Veranstalter führten eine Rangliste. Die Attacken übten die Informatiker mithilfe einer speziellen Website, die Umgebungen für Angriffe simuliert. «Hier können sie auf legale Weise Neues dazulernen», sagt Bütler. Um zu üben könnten sie ja nicht einfach eine richtige Seite hacken.

«Trainieren und weiterbilden»

«Ich bin hier, um vor allem zu trainieren und mich weiterzubilden», sagt Christian Schinnerl, der gerade ein Wargame löst. Er ist IT-Security-Manager aus St. Gallen. «Die Jugendlichen hier sind sehr gut. Ich war vorübergehend auf Platz 1 der Rangliste, jetzt bin ich abgerutscht.» Mit 37 ist Schinnerl unter den Teilnehmern schon fast ein Senior. Aus Deutschland angereist ist Hendrik Hilken (20). «Die Wargames zeigen mir mögliche Lücken auf meinem eigenen Computer – schliesslich will ich ihn ja sauber halten.» Wenig später versucht er bei einer Aufgabe zwei bekannte Sicherheitslücken zu nutzen. «Die sind schon gestopft», stellt er fest. Nun googelt er im Web nach Informationen über weitere Lücken.

Unter den Teilnehmern fällt Simone Obernöder auf. Sie ist eine von zwei Frauen, die den Anlass als Wargame-Spielerinnen besuchen. «Viele Frauen haben beim Thema Informatik noch Berührungsängste», sagt sie. Die Aufgaben löst sie mit vier Kollegen. «Das macht einfach mehr Spass.» Obernöder hat Wirtschaftsinformatik studiert, «Cyberstorm 2» ist ihr erster Hackeranlass überhaupt.

Spionage-Kit mit Support-Garantie

Während den Wargames, die nur auf den kleinen Laptop-Bildschirmen stattfinden, traten in der Aula diverse Referenten auf. Sie berichteten über Gefahren im Internet und sicheres E-Banking. Wie ausgeklügelt die Werkzeuge der Kriminellen sind, erklärte Roman Hüsey in seinem Vortrag über Hackerangriffe. Der Betreiber des Sicherheits-Blogs Abuse.ch sorgte im vergangenen Jahr für Schlagzeilen. Weil er die Arbeit von Cyber-Kriminellen störte, verschickten sie an Schweizer Mailboxen ein gefälschtes Massen-Mail. Darin wurde in seinem Namen ein Amoklauf angekündigt. Mitten in der Nacht wurde Hüsey von der Polizei abgeholt. Die Sache klärte sich danach schnell auf.

Der Informatiker beschrieb in Rapperswil ein sogenanntes Crimeware-Kit - ein Softwarepaket für Spionageattacken. Dieses ist auf dem Schwarzmarkt für ein paar Dollar erhältlich und erlaubt Kriminellen, auf einfachste Weise infizierte Computer zu überwachen - so gelangen sie an Passwörter von E-Mails oder an die Zugangsdaten von E-Banking. Eine simpel zu bedienende Benutzeroberfläche zeigt auf einen Blick die infizierten Computer. Die Cyber-Kriminellen sehen zum Beispiel, wann infizierte PCs online waren und was aus ihnen rausgeholt wurde. Auch Live-Screenshots des Desktops seien möglich.

«Die Anwendung hört sogar mit, wenn man sich über eine sichere https-Verbindung in seinen Facebook-Account einloggt», weiss Hüsey. Für ihn erreicht die Software eine neue Qualität: «Der Verkäufer bietet beim Kauf Support und eine Anleitung an. Genau so, als ob man im Laden eine Software kaufen würde.» Wer hinter dem Crimeware-Kit steckt, ist unbekannt.

Im Vorbeisurfen infiziert

Zugang zu fremden PC verschafft sich die Hacker-Software über einen Trojaner, den Kriminelle mit Spam-Mails oder einem Link einschleusen. Das File nistet sich mit unscheinbaren Dateinamen in die Systemdateien ein. «Sich dagegen zu schützen ist schwierig. Grundsätzlich gilt, neben dem System und Virenschutz auch den Adobe Reader und zum Beispiel den Flashplayer aktuell zu halten.»

Für die Cyber-Kriminellen sei zurzeit vor allem das sogenannte Drive-By-Infektionen Trojaner attraktiv: Hacker verstecken auf Websites die Malware, die sich schon auf den eigenen Rechner installiert, wenn man nur die Seite ansurft. (Tagesanzeiger.ch/Newsnetz)

Erstellt: 19.04.2009, 22:23 Uhr