Ein Hacker zaubert am Computer

Der Wettinger Marc Ruef ist mit 24 Jahren bereits eine bekannte Grösse in Fragen der Computer-Sicherheit. Als Co-Autor des Buches «Hacking intern» versucht er die Internet-Gesellschaft für die Fragen der IT-Sicherheit zu sensiblisieren.

Mar Ruef: Der Wettinger versucht mit seinem Engagement die Sensibilität der Internet-Nutzer für Sicherheitsfragen zu stärken *Foto: zVg*

Dave Witassek

Wann und weshalb hast Du begonnen, Dich für Computer zu interessieren?

Schon sehr früh, mit ungefähr neun Jahren, habe ich die ersten Gehversuche auf dem 386er meines Vaters gemacht. Meine eigenen Basic-Programme habe ich oft auf meiner alten Schreibmaschine vorbereitet und dann bei Gelegenheit auf seinem Rechner abgetippt. Nachdem ich mit zwölf, wegen guter schulischer Leistungen, einen eigenen XT/AT bekommen habe, begann ich mich ebenfalls für die Telefonie zu begeistern.

Bevor Du begonnen hast, Dich im Bereich IT-Sicherheit zu engagieren, warst Du ein Hacker…?

Das kommt ganz auf die Definition des Begriffs «Hacker» an. Die klassische Umschreibung versteht darunter einen der Technik aufgeschlossenen und sich für diese interessierenden Menschen. Zu dieser Gattung zähle ich mich nach wie vor, auch wenn ich längst nicht mehr jede Mode-Erscheinung mitmache. Ich kann mir durchaus vorstellen, dass ich in 30 Jahren irgendwo abgeschieden an einem kleinen See wohne und gänzlich auf E-Mails und Co. verzichten kann.

Wie kamst Du darauf, in andere Systeme einzudringen?

Ich bin erst relativ spät, nämlich 1996, wirklich mit dem Internet in Kontakt gekommen. Für Kryptografie und Computerviren habe ich mich aber schon lange davor interessiert. Der Einbruch in fremde Systeme war und ist für mich ohne Einverständnis des Besitzers ein Tabu. Die Wahrung und Achtung der Privatsphäre gilt seit jeher als einer meiner wichtigsten Grundsätze. Einen bösartigen Vorteil aus dem Unwissen anderer zu ziehen, halte ich für eine verwerfliche Vorgehensweise.

Aber das Einbrechen hast Du gelernt…?

Ich pflege zu Hause ein eigenes autonomes Netzwerk, in dem ich Angriffsszenarien durchspielen kann. Dieses Praxis-Wissen ist für meine berufliche Tätigkeit unabdingbar. Meine ersten Gehversuche ohne Internet musste ich halt damals noch auf meinem eigenen MS-DOS-Rechner umsetzen.

Was hat sich seit damals in der Hacker-Szene verändert?

Dank dem Zugang zum Internet konnte ich sehr schnell zwecks Informationsaustausch Kontakte mit Gleichgesinnten knüpfen. Damals wie heute waren es kleine Kreise von Leuten, die sich für die gleichen Themen interessiert haben. Schwachstellen in Telefon-Systemen, Chipkarten-Hacking, Kryptoanalyse, usw. Skeptizismus und Zurückhaltung schwang stets mit, vor allem aber zu Beginn einer Bekanntschaft. Heute sind die Zustände etwas «popularisiert». Begriffe wie «Computerviren» oder «Firewalls» sind in aller Munde und allgemeine Informationen dazu nicht mehr so exklusiv wie früher. In gewissem Sinne hat das Metier Computersicherheit seinen Mythos zu Gunsten einer löblichen Liberalität eingetauscht. Vermeintlich brisante Informationen — zum Beispiel die zielgerichtete Planung einschneidender Limitierungen der Privatsphäre eines jeden Schweizer Bürgers — sind heute ebenfalls der breiten Öffentlichkeit zugänglich.

Wie würdest Du heute einen Hacker definieren?

Die Definition eines Begriffs orientiert sich meines Erachtens in erster Linie nach den Personen, die diesen nutzen wollen sowie den gegebenen Kontext. Für einen Laien ist ein Hacker etwas total anderes, als für einen professionellen Security Consultant. Ich halte gerne an dem klassischen Begriff fest, da er nicht negativ ausfällt und für mich eine gewisse Nostalgie in sich birgt. Jemand, der aufgrund seiner Beharrlichkeit und Kreativität einen «Zaubertrick» mit einem Computer vollbringt — zum Beispiel eine besonders elegante Lösung eines mathematischen Problems —, das ist für mich ein Hacker.

Heute bist Du als Security Consultant bei der Zürcher Firma «scip AG» tätig. Was sind dort Deine Aufgaben und wie bist Du dorthin gelangt?

Ich betreue vorwiegend Finanzinstitute in der Umsetzung sicherer Computersysteme und -netzwerke. Meine Hauptaufgabe besteht dabei im Überprüfen entsprechender Installationen zur Determinierung potentieller oder existierender Schwachstellen. Können solche frühzeitig entdeckt werden, lassen sie sich ebenso frühzeitig beheben. Das hilft, die Angriffsfläche und das Zeitfenster für Attacken zu minimieren. Eine Arbeit, die sowohl technisches Verständnis als auch wirtschaftliches Fingerspitzengefühl erfordert. Diese Tätigkeit führe ich seit meinem Eintritt in die Arbeitswelt durch. Für eine erste Anstellung konnte ich mich durch eine Reihe von Publikationen relativ brisanter Informationen — zum Beispiel die Sicherheit von Chipkarten — empfehlen.

Andere mit Deinen Interessen hätten erst Informatik studiert…

Es wäre durchaus eine Option gewesen. Meinem Wesen nach hat mir die Wahl eines autodidakten Weges aber besser entsprochen. Schon während des Geografie-Unterrichts steckte ich lieber meine Nase in ein Buch über TCP/IP-Netzwerkadministration, als mich mit dem Verlauf von Schweizer Flüssen auseinander zu setzen. Aber wer weiss: Ich bin noch jung und vielleicht hole ich das Versäumte irgendwann nach...

Muss man als Sicherheits-Spezialist zwangsweise auch ein guter Einbrecher, in deinem Falle also Hacker sein?

Das Wissen, wie ein Angriff funktioniert, kann natürlich nur Förderlich für das Umsetzen von Gegenmassnahmen sein, es ist aber nicht immer eine Pflicht. Ich kenne eine Vielzahl hervorragender Consultants, die sich vorwiegend auf organisatorischer oder konzeptioneller Ebene mit IT-Sicherheit auseinandersetzen. Das Fehlen von technischem Verständnis kann so gewisser Weise wieder wett gemacht werden.

Und wie stellst Du Dir Deine berufliche Zukunft vor?

Mit meinem aktuellen Arbeitgeber und den mir zugetragenen Arbeiten bin ich sehr zufrieden. Ich könnte mir vorstellen, dass ich in den kommenden Jahren keine Änderung anstrebe.

Wie beschäftigst Du Dich heute im Privaten mit dem Computer? Unter anderem betreust Du ja die Website «computec.ch»…

Mit der Erfüllung meines Traums im Bereich der IT-Security zu arbeiten, ist auch mein Drang nach Abwechslung gewachsen. Komme ich nach Hause, will ich mich eher weniger mit Netzwerken und Codezeilen herumm ühen. Zurzeit gibt es nur wenige Projekte, denen ich effektiv meine Freizeit widme. Meine Webseite ist seit Jahren mein kleines Steckenpferd, das pro Monat über 120 000 verschiedene Besucher anlockt — Meine eigene kleine Plattform, um ein bisschen etwas zu bewegen. Immer mehr in den Mittelpunkt gerückt sind bei mir in den letzten Jahren die soziologischen und politischen Probleme der Computersicherheit. Die Einführung biometrischer Daten in Pässen, die Installation von Überwachungskameras durch die SBB oder das Anstreben von Trivial-Patenten in der Software- Industrie sind für mich die nicht zu unterschätzenden Gefahren des echten Lebens. Aufklärungsarbeit in dieser Hinsicht tut zwingend und dringend not.

Auf Dich aufmerksam gemacht hast Du auch als Co-Autor des bei «Data Becker» erschienenen Buches «Hacking intern». Wie bist Du zum Schreiben gekommen?

Ich habe schon immer gern geschrieben. Habe ich mich mit einem Thema — egal ob Computer oder Philosophie — auseinandergesetzt, habe ich stets für mich die wichtigsten Punkte zusammengefasst, primär, weil ich viele Dinge schnell wieder vergesse. Irgendwann dachte ich, anstatt meine Zeilen bei mir verstauben zu lassen, könnte ich diese auch der Öffentlichkeit zugänglich zu machen. Vielleicht können auch andere davon profitieren.

Um was geht es in eurem Buch?

Es ist ein allgemeines Buch zur Einführung in den Bereich der Computersicherheit. Wir haben dabei versucht grundlegende Vorgehensweisen praxisorientiert zu vermitteln und uns nicht auf vergängliche Inhalte (zum Beispiel aktuelle Computerviren) zu stützen. Ein gutes Informatik-Buch sollte auch nach vielen Jahren kein Stück seiner Aktualität eingebüsst haben. Meine liebsten Computerbücher stammen mitunter aus einer Zeit, in der Ronald Reagan noch die grösste Streitmacht dieses Planeten dirigiert hat.

Macht man sich unter Hackern nicht unbeliebt, wenn man ihre Kniffe an die Öffentlichkeit trägt? Zauberer verraten ihre Tricks ja auch nicht…

Vor allem zu Beginn meines Schaffens als freier Autor habe ich die eine oder andere Rüge aus einschlägigen Kreisen einstecken müssen. Allgemeine Informationen sollten jedoch frei und jedem, der sich für sie interessiert, zugänglich sein. Ich mag Computer und ich mag das Internet. Kann ich durch einen Artikel das Verständnis dafür bei meinen Lesern verbessern, verhelfe ich gleichzeitig dem neuen Medium zu einer besseren Qualität. Diese positive Entwicklung ist für alle Nutzer desselben von Vorteil.

Und Deine nächsten Projekte?

Seit etwas über einem Jahr arbeite ich an der Entwicklung eines offenen Security Scanners und Exploiting Frameworks namens «Attack Tool Kit» *(Infos unter ATK, www.computec.ch/ projekte/atk/)*. Dieses Projekt stösst aufgrund seiner Brisanz und den hoch gesteckten Zielen auf ein enormes internationales Interesse. Da ich mit meiner freien Lösung an den Stühlen alteingesessener Branchengrössen rütteln will, werde ich wohl noch die eine oder andere Nacht vor meiner abgenutzten Tastatur verbringen.

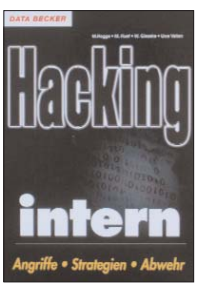
Was glaubst Du, wie sich die Computer-Branche bezüglich der Sicherheits-Aspekte entwickeln wird?

Das Verständnis für Sicherheitsprobleme wächst unter dem Strich sowohl bei den Entwicklern als auch bei den Nutzern. Ich meine aber festzustellen, dass der Trend immer mehr zu einer Kluft zwischen Wissenden und Unwissenden führt. Die einen Leute wissen sehr viel über die neuen Technologien, andere verweigern sich diesen gänzlich. Diese Entwicklung wird zwangsweise zu einer Ausgrenzung, quasi zu einer Zweiklassengesellschaft in unserer technokratischen Zeit führen. Wie der Satz «Wissen ist Macht» so schön sagt, werden die Unwissenden wohl das Nachsehen haben. Und damit stellen sie ebenfalls indirekt eine Gefahr für das System und sämtliche Benutzer dar. Denn ein System ist nur so sicher, wie sein schwächstes Glied.

Vor welchen Gefahren müssen sich Computer-Anwender deiner Meinung nach in naher Zukunft am meisten hüten?

Die grösste Gefahr für ein System ist mitunter seine Komplexität. Die Entwickler von Software müssen noch viel lernen, um den Anwendern das Leben so leicht wie möglich — und damit auch sicher — zu machen, ohne dabei die Transparenz aus den Augen zu verlieren. Weniger ist oftmals mehr. Die grösste Gefahr für unsere moderne Gesellschaft ist hingegen die Abhängigkeit von der Technik. Können wir uns in der Hinsicht nicht wieder ein bisschen los reissen, machen wir uns zwangsweise verwundbar. Aber zu diesem Schritt wird wohl frühestens, wenn überhaupt, die Generation nach uns fähig sein.

Das Buch



Hacker-Tricks

Immer häufiger geraten auch private Rechner ins Visier skrupelloser Hacker. Viren, Würmer und Attacken machen den Usern zu schaffen. «Hacking intern» verrät die Tricks der Cyber-Rowdies und gibt Tipps, wie man sich schützen kann. Auch für den Normalanwender verständlich, hat das Buch Potential, zu einem Standardwerk auf diesem Gebiet zu werden.

Marc Ruef u.a., Hacking intern, Data Becker, 880 Seiten