Interview mit Lutz Donnerhacke – Mitgründer des Fördervereins Informationstechnik und Gesellschaft (Fitug)

Marc Ruef, scip AG, maru-at-scip.ch
Lutz Donnerhacke, IKS GmbH, lutz-at-iks-jena.de

scip AG: Hallo Lutz. Vielen Dank, dass Du Dir die Zeit für dieses Interview nimmst. Dein Name ist seit Jahren unweigerlich mit der (deutschsprachigen) "Hacker-Kultur" verwoben. Betrachtet man in diesem Belang Deinen Werdegang, ist er sehr klassisch. Was findest Du, hat sich jedoch seit den Zeiten von C64, Zak McKracken und 5,25"-Floppy-Disks verändert?

Lutz Donnerhacke: Die Grundlagenkenntnisse sind verloren gegangen. Der Einstieg für heutige Technikinteressierte findet auf einem so hohen Niveau statt, dass nur noch in seltenen Ausnahmefällen der Interessent die relevanten Detailkenntnisse erwirbt oder erwerben will.

Dies betrifft besonders die Programmierkenntnisse, aber auch die Kenntnisse von Protokollen. Im Ergebnis sieht man heute viele Leute blind irgendwas probieren, anstatt systematisch Ursachen und Wirkungsweisen abzuklopfen. Es gipfelt darin, dass zufällig funktionierende Handlungsweisen wie Voodoo-Rituale gehandelt und in den verschiedensten Zeitschriften abgedruckt werden.

Besonders schlimm ist jedoch, dass durch das fehlende Verständnis zunehmend wieder unsichere oder schlecht performante Software erstellt wird, ja sogar unsichere Algorithmen und Protokolle neu entwickelt werden.

In Bezug auf Computersicherheit konnte vor allem im Umgang mit neuen Schwachstellen und wie diese Veröffentlicht werden eine Veränderung festgestellt werden: Bugtraq wurde zunehmends unspektakulär und spannende Diskussionen werden immer spärlicher. Hat das Genre IT-Security ein bisschen seinen Reiz verloren?

Nein, im Gegenteil. Der beobachte Rückgang öffentlicher, sicherheitsrelevanter Informationen ist in der Vermeidung der Öffentlichkeit zu suchen. Sicherheit und selbst Diskussionen darüber sind knallhartes, ökonomisches Geschäft geworden. Das macht das Thema eigentlich nur noch spannender.

Die Massenmedien pflegen den Begriff "Hakker" in anderen Zusammenhängen zu nutzen, weder er ursprünglich eingeführt wurde. Bedauerst Du dies oder ist es lediglich eine übliche Entwicklung der Popularisierung einer Subkultur? Was verstehst Du unter einem Hacker? Welches sind für Dich die "grossen Hacker"?

Die strenge Unterscheidung zwischen "Hacker", "Cracker" und "Crasher" ist ein typisch deutsches Phänomen. Das Definitionsmonopol des Chaos Computer Clubs erlaubte damals eine positive Konnotation des Wortes "Hacker" einzuführen und zeitweilig in der Sprache zu verankern. Internationales Journalistentum kann und wird eine Gleichschaltung der Bedeutungsebenen solcher Begriffe erreichen, schon allein, um überhaupt zuverlässig kommunizieren zu können.

„Die strenge Unterscheidung zwischen Hacker und Crakker ist ein typisch deutsches Phänomen."

Der Fachbegriff "Hacker" ist also dabei, sich auf einem Begriffsniveau einzupegeln. Die deutsche Sonderbehandlung führt jedoch auch international zu einer etwas besseren ethischen Einstufung des Begriffs. Viel mehr konnte man nicht erwarten.

Für mich ist ein Hack etwas, das besonders kreativ Technik zweckentfremdet. Meistens verdienen besonders elegante oder besonders effiziente Algorithmen diese Bezeichnung. Sicherheitstechnisch betrachtet sind die Zweckentfremdungen der Hacks schlichte Hintertüren durch gezielte Fehlfunktionen.

Vorbilder zu benennen ist schwer. Neben Wau ist aktuell Florian Weimer zu nennen.

Der Förderverein Informationstechnik und Gesellschaft e.V. propagiert die menschennahe "Demokratie im Netz", die auf bürokratische Regelungen verzichten möchte, um ein Höchstmass an Effizienz und Humanismus gewährleisten zu können. Wo hört für Dich aber Meinungsfreiheit auf und wo sind Regulierungen erforderlich?

Persönlich halte ich Regulierungen für erforderlich, um Einschränkungen der Meinungsfreiheit zu verhindern. Meinungsfreiheit gliedert sich dabei in zwei Teilbereiche: Meinungsäusserungsfreiheit und Rezipientenfreiheit.

Die Meinungsäusserungsfreiheit ist mit dem Internet schon weit gediehen, denn praktisch jeder kann seinen eigenen Webserver o.ä. betreiben. Leider ist zunehmend die Einschränkung dieser Meinungsfreiheit zu beobachten: Es ist schwieriger geworden, feste IP-Adressen und ungefilterte Zugänge zu bekommen. Die Access-Provider versuchen durch Einschränkung der eigenbetriebenen Server ein Zusatzgeschäft mit Webspace und co. zu generieren.

Rezipientenfreiheit wird leider zu wenig beachtet. Statt dessen versucht man mittlerweile das Recht auf freien Erhalt von Information auch auf dem Transportweg zu beschneiden. Es werden ganze Teile des Internet ausgeblendet, wenn irgendwo IP-Sperren oder gar Contentfilter zum Einsatz kommen. Bedenklich ist auch die Willkür, mit der Suchmaschinenbetreiber Informationen unterdrücken. Hier tut eine Regulierung hin zu mehr Transparenz not.

Um es platt zu sagen: Die Wiedereinführung des Feindsenderverbots ist Demokratieschädlich.

Kritiker werfen Wisschenschaftlern mit Hang zu hypothetischen Betrachtungen gerne vor, dass diese lediglich vor der Wirklichkeit und ihren reellen Problemen flüchten wollen. Wie stehst Du als Analytiker und Denker einer solchen Kritik gegenüber?

Kürzlich habe ich Joseph Weizenbaum erlebt und etwas mit ihm reden können. Er ist zu der bemerkenswerten Erkenntnis gelangt, dass die Probleme der Welt quantisiert vorgebracht werden, also in handlichen Bruchstücken ohne grossen Zusammenhang. Dadurch geht die Priorisierung der Probleme verloren, man beschäftigt sich lieber mit unwichtigen Dingen, wie z.B. mit einem Interview.

Aufgrund meiner mathematischen Ausbildung habe ich wenig Schwierigkeiten damit, Probleme gar nicht global zu priorisieren. Es gibt halt verschiedene Halbordnungen und ich benutze die, die mir momentan am besten hilft. Das ändert sich gern auch mehrfach pro Stunde.

Im aktuellen Kontext möchte ich aber anmerken, dass die Probleme der Meinungsfreiheit und des Datenschutzes sehr reale Betrachtungen darstellen.

Die Regierungen und ihre Organe sind seit jeher darum bemüht, im Falle eines Informationskriegs die Oberhand behalten zu können. Die Folgen davon sind Restriktionen im Umgang mit kryptografischen Methoden. Wie empfindest Du derlei Bestrebungen?

Ich kann derzeit keine Einschränkungen bei kryptografischen Algorithmen feststellen. Ein politischer Hack ist jedoch die französische Reglung, die Krypto verbietet und das Verbot per Durchführungsbestimmung auf irrelevant grosse Schlüssellängen beschränkt. Dies verlagert das Kryptoverbot aus dem Bereich der Legislative in den Bereich der Exekutive. Cool.

Wesentlich mehr Schwierigkeiten machen die Reglungen zum "geistigen Eigentum". Hier wird nachhaltig die Entwicklung und der Fortbestand von Informationsverarbeitungssystemen untergraben.

„Meinungsfreiheit gliedert sich dabei in zwei Teilbereiche: Meinungsäusserungsfreiheit und Rezipientenfreiheit.“

Denkst Du, dass Quantenkryptografie eine Zukunft hat?

Quantenkryptografie im Sinne der öfter besprochenen abhörsicheren Leitungen hat ein sehr begrenztes Einsatzfeld ohne Massenzukunft. Erfolge der Quantencomputer sind dagegen geeignet im Massenmarkt gravierende Umwälzungen anzustossen, ich halte diese in den nächsten zehn Jahren jedoch nicht für sonderlich praxisrelevant.

Wird bei Quantenkryptografie nicht lediglich die Abhörsicherheit gegen die Anfälligkeit von Denial of Service-Attacken mittels Abhören eingetauscht und somit das Verfahren unwirtschaftlich gemacht?

Zum einen ist die Abhörsicherheit entgegen der ursprünglichen Versprechungen nicht zu halten. Zum anderen ist der Einsatzbereich so speziell, dass die betroffenen Strecken ausreichend überwacht werden können, d.h. das Erkennen des Lauschers zu einer schnellen Ergreifung führt.

Zu DDR Zeiten hatte die Rote Armee Kabel in Druckluftrohren verlegt. Beim Anbohren eines solchen Rohres konnte man durch Frequenzmessung der auftretenden stehenden Wellen (wie bei einer Flöte) den Ort des Angriffs sofort ermitteln und den Zugriff organisieren. Sehr effektiv, ziemlich teuer und nur für Spezialfälle geeignet. Wie Quantenkryptografie.

IPv6 schimmert seit Jahren am Horizont. Was denkst Du, welche Auswirkungen wird die Einführung der neuen Protokollgeneration auf die Welt und ihre digitale Sicherheit haben?

IPv6 ist ein wesentlicher Beitrag zur Meinungsäusserungsfreiheit. Damit wird es möglich, Informationen direkt und ungefiltert anzubieten. Wir (als ISP) haben sehr positive Erfahrungen mit IPv6 im Backbone, für Server und Arbeitsplätze gemacht.

Seitens der Sicherheit ist hervorzuheben, dass man deutlich leichter das verwurmte Endgerät ermitteln kann, als im klassischen PAT Fall. Dies ermöglicht schnellere und genauere Reaktionen. Ebenso sind Filterlisten deutlich besser gerätebezogen definierbar, insbesondere für Laptops.

RFID ist in aller Munde. Über Risiken wird jedoch, wie gewohnt, in den Massenmedien wenig debattiert. Wird sich das Wardriving in Zukunft nicht mehr nur auf WLANs beschränken, sondern vorwiegend auf die kontaktlosen Chipkarten abzielen? Ist es dann wohl schon zu spät?

Es ist zu spät. RFID ist allerdings nur eines von vielen Trackingsystemen, die die Privatsphäre der Bürger ausspionieren. Solange jedoch die Bürger selbst immer weiter ausspioniert werden wollen (siehe Payback), ist ein Aufbegehren gegen die Industrie sinnfrei. Mündigen Bürgern folgt die Industrie von allein: Man sehe sich nur an, dass UnCDs in England kein Thema sind, weil sie nicht akzeptiert werden.

Computerkritiker wie Joseph Weizenbaum postulieren, dass sich der moderne Mensch kritisch mit der Technik, den Medien und Informationen auseinanderzusetzen hat, um damit quasi die Mündigkeit in einem technokratischen Zeitalter zu erreichen. Denkst Du, dass dies überhaupt von einer Konsumgesellschaft wie der unseren verlangt werden kann? Falls ja, bleibt dieses Ziel überhaupt erreichbar?

Es kann und muss verlangt werden. Medienkompetenz ist gerade im Rahmen der Meinungsfreiheit wichtig. Menschen, die nicht in der Lage sind, Informationen abzuwägen, ziehen ein redaktionell bearbeitetes "Internet" vor, also befürworten Einschränkungen der Rezipientenfreiheit.

Und zum Schluss noch die etwas andere Frage: Wenn Du einen eigenen Staat gründen würdest, welche drei Dinge würdest Du dem Volk frei oder möglichst billig zur Verfügung stellen wollen?

Wir (Thüringen Netz e.V.) hatten vor nunmehr 10 Jahren mal einen Staatsgründung des Internets mit den entsprechenden Juristen durchdiskutiert. Es geht. Es würde Spass machen. Es macht unheimlich viel Arbeit. Man muss vielzuviel "unwichtigen" Kram erledigen. Es macht keinen Spass.

„Medienkompetenz ist gerade im Rahmen der Meinungsfreiheit wichtig.“

Das, was an der Staatsgründung keinen Spass macht, ist die umfassende Verantwortung für den Bürger. Deswegen hat Vatikanstadt keine Staatsangehörigen. Ohne Bürger ist die Frage jedoch auch wieder sinnfrei. (*lacht*)

Vielen Dank für Deine Zeit sowie das interessante Interview. Und viel Glück für die Zukunft Deiner interessanten Projekte.

Danke.

Herausgeber

scip AG
Technoparkstrasse 1
CH-8005 Zürich
+41 44 445 1818
mailto:info@scip.ch
http://www.scip.ch

Zuständige Person:
Marc Ruef
Security Consultant
+41 44 445 1812
mailto:maru@scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.