Die Entwicklung der Hacker-Szene

Marc Ruef, scip AG, maru-at-scip.ch

Der IT-Bereich und die Sicherheit dessen ansich haben in den letzten Jahren regelrechte Quantensprünge gemacht. In diesem Artikel werden die letzten Jahre der Entwicklung der (deutschsprachigen) Hacker-Szene besprochen. Der Leser wird so in den Sog von Zeitabschnitten wie New Economy oder das fortwährende Aufkommen neuer Hacker-Gruppierungen gezogen. Neben der individuellen Sichtweise von Marc Ruef werden kulturell und wirtschaftliche Aspekte dieses Zeitalters betrachtet. Es liest sich, als wäre man dabei gewesen...

Das erste Mal richtig mit dem Internet in Berührung kam ich im Jahr 1996, als ich an der Orbit in Basel endlich einen der von den Ausstellern zur Verfügung gestellten Internet-PCs für mich in Anspruch nehmen konnte (http://www.orbit-iex.ch). Mein Vater und ich standen wie gebannt vor einer Applikation, die sich später als Webbrowser – eine aus heutiger Sicht schon längst archaisch anmutende Version des Microsoft Internet Explorers - herausstellen sollten. Der Cursor blinkte herausfordernd, schon fast neckisch - Wir sollten also etwas in das Textfeld einer Webseite namens Yahoo schreiben. Gesagt getan. Als die ersten Suchresultate aufgelistet wurden, habe ich mich unweigerlich in das neue Medium verliebt. Es vergingen keine zwei Monate, bis ich dann endlich als Beta-Tester der damals brandneuen Kabel-Modems in der Schweiz einen Internet-Anschluss mein Eigen nennen konnte.

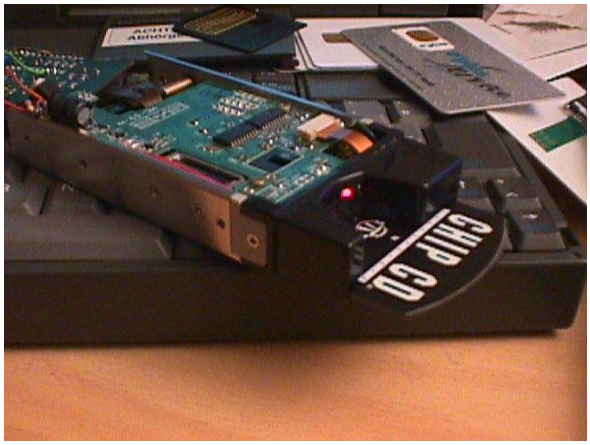

Abbildung 1: Ein Chipkartenterminal liest ein auf eine CD-ROM gestanzten Chip aus.

Ich war schon immer von Computern begeistert. In früher Kindheit, als ich noch keinen eigenen Computer besass, habe ich Basic-Programme auf meiner alten Schreibmaschine vorbereitet, um sie später auf dem 486er meines Vaters abtippen zu können. Neben Computerspielen und kleineren Simulationen (z.B. ein textbasiertes SimCity) hat mich stets die künstliche Intelligenz und das Entwickeln von Computerviren interessiert. Wie ist es nur möglich eine Anwendung zu schreiben, die sich selber reproduziert, sich selber verändert und im Hintergrund Arbeiten erledigt?

„Wie ist es nur möglich, dass sich eine Anwendung im Hintergrund selber reproduziert?“

Mit dem Eintritt ins Internet eröffnete sich eine komplett neue bzw. erweiterte Welt für mich. Webseiten und Publikationen zu Computerviren gab es im Web wie Sand am Meer. Was ich früher in Büchereien nachschlagen musste, wurde mir multimedial ins Arbeitszimmer gebracht. Innert weniger Tage habe ich wohl jede Zeile zum Thema gelesen, die bis dato im Internet publiziert wurde. Beim Besuchen dieser "Hacker-Seiten" kam ich ebenfalls ein erstes Mal mit anderen Themengebieten der Computersicherheit in Berührung. Die Angriffsmöglichkeiten von TCP/IP oder die Sicherheit von Chipkarten waren die Dinge, die mich sofort in ihren Bann zogen. Der Gedanke, das letzte Bit eines Computers verstanden zu haben und mit ihm schier unmögliche Zaubertricks vollbringen zu können, hat mich mehr dennje begeistert.

Wie ich nunmal bin, habe ich nach dem Lesen entsprechender Fachartikel sofort daran gemacht, das neu erworbene Wissen auszuprobieren. Durch den Nachbau eines simplen Chipkarten-Terminals konnte ich mich so hautnah mit den physikalischen und logischen Gegebenheiten der kleinen Plastikkarten beschäftigen. Da ich der Meinung bin, dass "Forschungsarbeit" stets zum Allgemeinwohl dokumentiert werden sollte, habe ich schon sehr früh eine eigene Webseite zum Thema Chipkarten-Sicherheit umgesetzt. Das Projekt mit dem damaligen Namen phreak.chip.ms (eingestellter Fork des Projekts unter http://members.fortunecity.de/alene3390366/) war quasi der Vorläufer von computec.ch, denn vom Prinzip her sollte ebenfalls ein Archiv mit Publikationen aus dem Genre zusammengetragen und zum freien Download angeboten werden.

Die Webseite war klein und dennoch fein genug, um zu Beginn Tag für Tag ein paar Duzent Besucher anzulocken. In dieser vergangenen Zeit war das Internet noch eher ein kleines Dorf, in dem sich jeder kannte. Obschon ich damals nur einen Bruchteil der heutigen Besucherzahlen von computec.ch verbuchen konnte, erhielt ich ein Mehr an Zuschriften von interessierten Lesern. Immerwieder gab es Leute, die mir ihre Erfahrungen mitteilten, über Chipkarten und die Welt philosophieren wollten. Das Schreiben von Emails wurde so schnell zu einem ausfüllenden Hobby, in dem ich mich zu Hause fühlte.

Hacker-Vereinigungen

Selbstverständlich vergass ich beim Betreuen der Webseite und dem Schreiben von Emails nicht, ebenfalls das Internet nach neuen und interessanten Artikeln zu durchforsten. Damals spriessten Hacker-Seiten wie Pilze aus dem Boden. Keine Woche verging, ohne dass irgendeine neue Gruppierung gegründet wurde. Viele von diesen überlebten jedoch kein Jahr oder die mangelnde Qualität ihrer Publikationen machte ein Besuch nicht wirklich lohnenswert. Eine bestimmte Projekt-Gruppe war jedoch für Kontuinität und Qualität bekannt: Auf kryptocrew.de wurde ein umfassendes Archiv geschaffen, das eine Vielzahl an Artikeln aus den verschiedensten Themenbereichen der Computersicherheit zusammenfasste. Unzählige Stunden habe ich mit dem Verschlingen der dort abgedruckten Artikel verbracht - Selbst das Blinzeln mit meinen Augen habe ich als unnötige Verschwendung meiner Zeit betrachtet, so gebannt war ich durch die umfassende Darlegungen der Funktionsweise von polymorphen Dateiviren und erweiterten Blueboxing-Angriffen (dies ist eine klassische Disziplin des Phone Hackings).

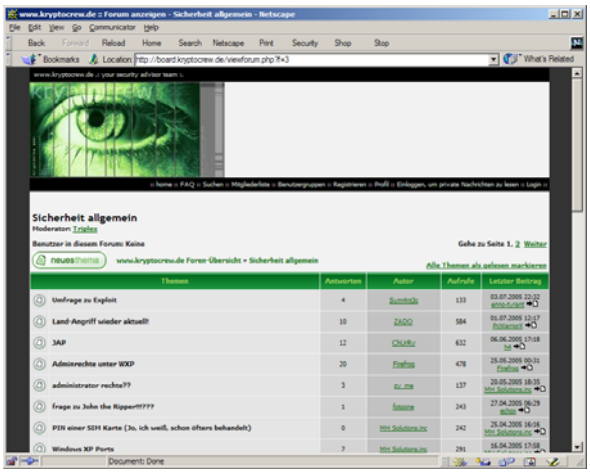

Abbildung 2: KryptoCrew.de galt jahrelang als die Anlaufstelle für Neulinge auf dem Gebiet der Computersicherheit.

Durch Neugierde getrieben wollte ich die neuen Dinge stets selber sehen. Nach dem Lesen einer Vielzahl an Publikationen zum Thema Firewalling habe ich bei meinem damaligen Lehr-Betrieb (ein internes Reisebüro der ABB) eine Möglichkeit gefunden, wie ich mit meinem Arbeitsplatzrechner das Internet nutzen konnte (ein falsch konfigurierter FTP-Proxy konnte mittels IP-Spoofing zur Weiterleitung überredet werden). Und dies, obschon unsere Abteilung, geschweige denn die Lehrlings-Rechner, überhaupt freigeschaltet waren. Nun konnte ich also auch während meinen Arbeitspausen die interessanten RFCs lesen oder in meinen Lieblingsforen vorbeischauen.

„Durch Neugierde getrieben wollte ich neue Dinge stets selber sehen...“

Die KryptoCrew war eine kleine Gruppe, bestehend aus etwa 5 Leuten, die zusammen die Webseite administrierten, Publikationen verfassten und Software entwickelten. Da ich den freien Dienst der Truppe sehr gut zu schätzen wusste, schrieb ich - einfach mal aus Spass - ein Email an den Seitenadministrator. In meinen Zeilen brachte ich meine Hochachtung vor ihrer Arbeit zum Ausdruck, verwies kurz auf mein eigenes Webseiten-Projekt und offerierte eher nebenbei eine Zusammenarbeit. Das Antwortschreiben, zwar relativ knapp aber dennoch ausserordentlich freundlich, kam für mich unerwartet. Ich dachte mir, dass ein solch grosses und etabliertes Projekt wohl kaum die Zeit finden wird, um auf meine unwichtigen Anfragen einzugehen. Man hat sich für das Lob bedankt und im Abschluss des Emails wurde darauf verwiesen, dass meine Webseite und Artikel durchaus Begriffe seien und ich mich doch mal über das offizielle Antrags-Formular um eine Mitgliedschaft bewerben solle.
Darum liess ich mich natürlich nicht zwei Mal bitten. In knappen Worten habe ich einen computer-bezogenen Lebenslauf zusammengestellt, kurz meine Möglichkeiten und Absichten geschildert. Rund eine Woche später erhielt ich dann tatsächlich die Zugangsdaten zum Mitgliederbereich und dem Webserver. Aus einem anonymen Projekt hat sich so für mich schnell eine Gruppe von Gleichgesinnten entwickelt, die Spass am Wissen haben wollten. Also genau nach meinem Geschmack!

Der Mensch rückte sodann eigentlich immer mehr in den Mittelpunkt. Es war irgendwann viel

interessanter mit Leuten über Gott und die Welt zu philosophieren, weder nur immer irgendwelche C-Quelltexte auseinanderzunehmen. Ein Camping-Ausflug oder das alljährliche Treffen am Chaos Communication Congress in Berlin wurde schon fast zur gern umgesetzten Pflicht. Dass man an derlei Events noch viele weitere interessante Leute kennenlernen würde, war ein scheinbar ungeschriebenes Gesetz. Diese Treffen waren immer sehr chaotisch und dennoch familiär. Da diskutierte eine Gruppe die Neuerungen im jüngsten Linux-Kernel, zwei unterhielten sich über die Angriffsmöglichkeiten von stationären Satelliten und einige machten die ersten Gehversuche im Schlossöffnen (engl. lockpicking). Halt wie eine Party, nur mit Leuten, die etwas merkwürdige intellektuelle Neigungen mit sich brachten.

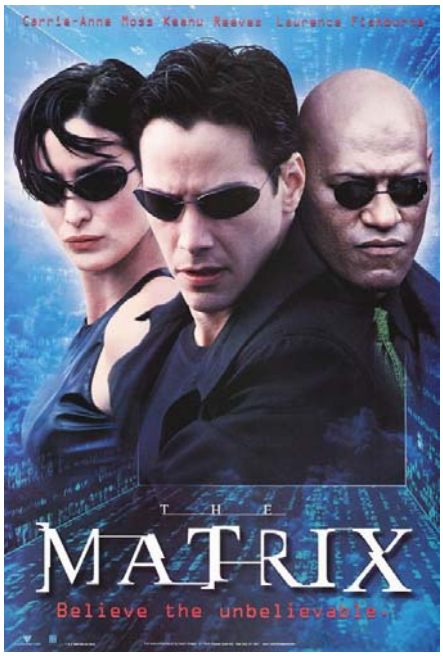

Abbildung 3: Der Film "The Matrix" (1999) veränderte plötzlich die Akzeptanz der Hacking-Kultur in der Gesellschaft

Ich verlagerte meine Hauptinteressen auf das Schreiben von Artikeln zum Thema Computersicherheit. Zu dieser Zeit begann ich auch mit dem ersten Manuskript für ein Buch; manchmal habe ich in meiner Lehrzeit gar heimlich während des Schulunterrichts daran gearbeitet. Teile dieser Arbeiten flossen tatsächlich ein halbes Jahrzehnt in das im Data Becker-Verlag erschienene Buch "Hacking Intern" mit ein. Für mein erstes Anstellungsgespräch als IT Security Specialist brauchte ich keine Zeugnisse oder Zertifikate vorzuweisen - Meine Publikationen machten das ihrige.

Computerbenutzer, die sich an das Thema Sicherheit heranwagen wollten, beschäftigten sich als erstes mit zwei Themen: Computerviren und Desktop Firewalls. Letztere erfuhren einen wahren Hype, denn wer etwas auf sich hielt, der erweiterte sein System um diese Firewalling-Funktionalität. Unendliche Diskussionen, welches Produkt nun das höchste Mass an Sicherheit lieferte und ob diese durch eine solche Lösung überhaupt gewährleistet werden kann, waren an der Tagesordnung. Firewalling war nicht mehr nur ein Thema für Administratoren grosser Netzwerke – Firewalls waren nun ein Zubehör für jedermann.

Erste Schritte in der Professionalität

Neben kryptocrew.de habe ich natürlich meine private Webseite weitergeführt, unter anderem auf die offizielle Domain computec.ch gewechselt. Die KryptoCrew-Truppe, vorwiegend bestehend aus Deutschen und einigen wenigen Schweizern, war um keinen Spass verlegen - Durch Zusammenarbeit und den Austausch von Informationen konnten regelrechte Kunststücke erbracht werden, die einem ein bisschen aus dem grauen Alltag von Schule und Studium reissen vermochte. Hatte jemand eine tolle Idee, wurde sie diskutiert. Verworfen wurde nur, was wirklich unsinnig erschien. Eine Vielzahl der Projekte entpuppten sich aber als wahre Abenteuer. So wurde zum Beispiel „per Zufall“ eine unzureichend geschützte Datenbank des U.S. Amerikanischen Militärs entdeckt. Die schwache Authentisierung ermöglichte das Einsehen sämtlicher persönlicher Daten aller Mitglieder der Streitkräfte. Der Puls schnellte unweigerlich in die Höhe, als sich unser Bildschirm mit den Anschriften und Telefonnummern hochrangiger Militärs füllte.

„Ich verlagerte meine Hauptinteressen auf das Schreiben von Artikeln zum Thema Sicherheit.“

Spätestens als der Kultfilm "The Matrix" (http://www.imdb.com/title/tt0133093/) im Jahr 1999 ins Kino kam, war der bis dato grösste "Hacker-Boom" zu verzeichnen. Kein Chat-Raum war mehr vorhanden, in dem nicht mindestens ein Halbstarker "Neo", das Pseudonym der Hauptfigur des Films, als seinen Benutzernamen wählte. Meine Webseite und das KryptoCrew-Projekt konnten sich zwischenzeitlich über Jahre als gute deutschsprachige Quellen des Genres etablieren. Und es gab Tage, an denen wurde ich regelrecht mit Emails überschwemmt. In Höchstzeiten erreichten mich rund 40 Schreiben, in denen ich zu einem Thema befragt oder um etwas gebeten wurde (Mit welchem Algorithmus

soll ich meine Festplatten verschlüsseln? Wo finde ich leere Chipkarten? Um was für einen Virus handelt es sich hier?). Eine aufregende und zugleich stressige Zeit, in der das Knüpfen von soliden Kontakten gerade wegen dieser grossen Quantität und der fehlenden Übersichtlichkeit nicht einfacher war.

Der Trend der Hacker-Gruppen setzte sich entsprechend fort, obschon ein merklicher Anstieg der Qualität der Projekte - vor allem die der "alten Hasen" - zu verzeichnen war. Durch Kooperationen, Affiliationen und Allianzen konnten starke Bande geknüpft werden und der Informationsaustausch funktionierte deshalb immer effizienter. Das Ziel war für uns stets das Weitergeben von Wissen. Wer nur nur nach einem Angriffstool für das Attackieren eines bestimmten Betriebssystems fragte, wurde höflichst mit dem Verweis auf ein Buch wie „The Design and Implementation of the 4.4BSD Operating System“ (http://www.amazon.de/exec/obidos/ASIN/0201549794/) abgespiesen.

Es wurden immer professionellere und umfassendere Scanning- und Angriffs-Tools entwickelt, mit denen sich nun teilweise sehr effizient Schwachstellen in Systemen entdecken liessen. Die Handhabung dieser Utilities war nicht immer einfach und so blieb das Nutzen derer doch vorerst einem elitär anmutenden Kreis vorbehalten. Es zählte nun nicht mehr nur die ausgefallene Idee, sondern auch die Umsetzung wollte effektiv gestaltet werden.

Firewalling war das erste wirtschaftlich (und technisch) ausgeschlachtete Gebiet der Computersicherheit. Die Erfolge der New Economy Zeit verlangten nach Mehr. Es bot sich entsprechend an einen Schritt weiter zu gehen und mit Intrusion Detection-Systemen (Abk. IDS) Angriffe frühzeitig erkennen zu können. In der Branche hiess es plötzlich, dass Firewalling nur ein kleiner Teil einer umfassenden Sicherheitslösung sei und wer etwas auf sich halte, der müsse zwingend IDS einsetzen. Der eine oder andere Kunde hat sich dazu – oftmals wirklich sehr gute Lösungen - überreden lassen. Übersehen wurde aber einmal mehr, dass bei derlei Lösungsansätzen das frühzeitige Umsetzen eines soliden Konzepts – wie auch schon beim Firewalling - unabdingbar ist. Eine weitere Schwierigkeit in der elektronischen Einbruchserkennung ist in der stetigen und kompetenten Betreuung einer IDS-Lösung gegeben. Ein solches System war nicht in der Lage autonom und selbstständig zu arbeiten. Fortwährend hätte ein Administrator die Protokolle auswerten und Anpassungen am Regelwerk vornehmen können. Ein Full Time Job, der in den wenigsten Unternehmungen, die sich ein Intrusion Detection-System haben integrieren lassen, gebilligt wurde.

„Firewalling war das erste wirtschaftlich und technisch umfassend ausgeschlachtete Gebiet der IT-Sicherheit.“

Mittlerweile waren langsam alle Mitglieder der KryptoCrew mit der Entscheidung ihrer beruflichen Entwicklung konfrontiert. Eine Vielzahl entschied sich für das Studium in einem naturwissenschaftlichen Bereich, wobei natürlich der Gang Richtung Informatik oder Mathematik offensichtlich schien. Andere wollten direkt in die Wirtschaft, liessen sich irgendwo als Administrator oder Security Consultant anstellen. Unter der Hand wurden einige Auftragsarbeiten, vorwiegend Security Audits, durchgeführt. Viele Firmen meldeten sich bei uns, weil sie die Sicherheit ihrer Systeme überprüft haben wollten und das umfassende Angebot unserer Webseiten eine gute Referenz darstellten. Dies ehrte natürlich, gleichzeitig war es die Möglichkeit, durch unser erworbenes Wissen ein bisschen Geld machen zu können. Eine Guppe von Freaks, die ihre Wochenenden vor den Bildschirmen verbracht hatten, wurden nun plötzlich von namhaften Firmen engagiert - Die intellektuelle Anarchie, die ansonsten nur im Internet umgesetzt werden konnte, wurde nun plötzlich Realität und zu unserem Vorteil.

Man wird langsam Erwachsen

Aus derlei Spass-Arbeiten wurde dann dennoch ernst. Dies bedeutet, dass wir es irgendwann auch leid waren, uns unter der Hand verkaufen zu müssen. "Hobby-Arbeiten" dieser Art wurden aus Mangel an Zeit und Interesse ausgeschlagen. Viele von uns arbeiteten nämlich schon vollberuflich im Metier und Nebenberuflich auch noch vor dem Rechner zu sitzen, das wird selbst dem härtesten Freak irgendwann zu viel. Es gibt schliesslich auch noch andere Dinge, weder Modems und Computer.

Dieser Umstand führt ebenso eine gewisse

Lustlosigkeit im Betreuen der Inhalte der Webseite herbei. Wer des Abends von der Arbeit als Administrator oder Webmaster nach Hause kam, der wollte nicht noch bis spät in die Nacht irgendwelchen HTML-Code pflegen oder Textdokumente kategorisieren. Es kam wie es kommen musste und die Ära kryptocrew.de ging langsam zu Ende. Die zu dieser Zeit geknüpften Freundschaften halten aber grösstenteils bis heute an. Obschon, ich gebe es gerne zu, man nicht mehr nur über Computer und Telefone redet. Einige sind mittlerweile verheiratet, andere haben Kinder. Es soll aber dennoch immer noch solche geben, die mal den einen oder anderen Hack anstreben...

Genauso wie wir erwachsen wurden, wurde die IT-Security Branche ansich erwachsen. Zum einen ist das Bewusstsein für die sichere Umsetzung von Software und Implementierungen bei den Entwicklern und Administratoren enorm gestiegen. Zum anderen hat der Kapitalismus in seiner reinsten Form Einzug ins Gebiet gehalten. Sicherheit ist ein Geschäft und als solches wird es auch behandelt.

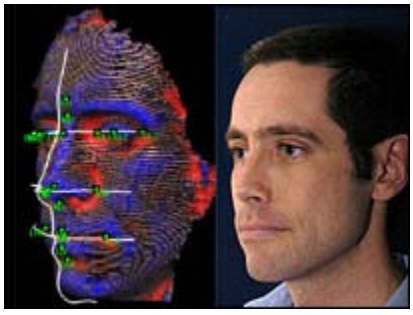

Abbildung 4: Biometrische Authentisierungs-Systeme sollen klassische Methoden mit Benutzername und Passwort in absehbarer Zukunft ablösen.

Wo Geld fliesst, sind in einem Rechtsstaat Anwälte nicht weit und so drohen viele Firmen heute lieber zuerst mit einer einstweiligen Verfügung, weder sich technisch mit einem Problem in ihren Produkten auseinanderzusetzen. Beispiele von Antiviren-Herstellern, die den Finder von Schwachstellen in ihrem Produkt vor Gericht gezerrt haben, liest man alle paar Monate auf den einschlägigen News-Seiten. Früher war man stolz darauf, wenn man eine neue Sicherheitslücke gefunden hat. Heute fragt man sich als erstes, welche rechtlichen Konsequenzen eine solche Suche mit sich ziehen könnte. Ein wunderschönes Genre, das ursprünglich durch kindliche Neugierde vorangetrieben wurde, hat seine Unschuld endgültig verloren und wurde dadurch aus dem Paradies vertrieben.

Die Angst vor dem Neuen wird aber längerfristig keine Vorteile bringen. Schwachstellen müssen nach wie vor so früh wie möglich gefunden werden, um ebenso rasch Gegenmassnahmen umsetzen zu können; bevor die Fehler durch bösartige Indivduen für ihre Zwecke ausgenutzt werden. Vor allem bei Systemen, von denen eine Vielzahl an Leuten abhängig ist, ist eine solche Vorgehensweise wünschenswert. Durch das Verschrecken dieser Suchenden wird die Qualität der Produkte leiden. In einem ersten Augenblick können Hersteller so ihre Weste weiss halten - Bis zu jenem Augenblick, wenn ein wütendes Kind es wirklich wagt, Pandoras Box zu öffnen. Dann verlieren unweigerlich alle Beteiligten!

Die Zukunft bringt aber nicht nur Schlechtes

Die Entwicklungen im Bereich der Computersicherheit gingen in einer Zeit, die als New Economy in die Geschichte eingehen wird, rasant voran. Eine Vielzahl an kreativen Ideen und innovativen Umsetzungen ist mit dem Boom des Internets einhergegangen. Eine wichtige Entwicklung dabei war das Etablieren einer gewissen Professionalität im Sicherheits-Bereich. Sicherheit ist nicht mehr nur ein Geschäft von einigen Freaks, die mit Neugierde und Elan nach neuen Möglichkeiten suchen. Durch ein kalkuliertes Geschäft und die messbar höheren Anforderungen ist Sicherheit immer mehr im Begriff eine Art Wissenschaft zu werden. Umfassende Risikoanalysen, durchdachte Konzepte, intensive Spezialschulungen - All das wäre vor 10 Jahren noch Fiktion gewesen. Heutzutage sieht sich aber jeder Programmierer früher oder später mit den Tücken von "bösartigen Anwendern", die eine Schwachstelle zu ihrem Vorteil ausnutzen wollen, konfrontiert. Und die meisten Internet-Benutzer wissen, was ein Computervirus ist und wo sie eine freie Personal Firewall herunterladen können.

„Die Verbesserung des allgemeinen Verständnisses für Sicherheit wird sich in Zukunft weiterziehen.“

Diese Verbesserung des Verständnisses für Sicherheit wird sich auch in Zukunft weiterziehen. Die Steigerung ist zwar nicht mehr so überproportional wie vor wenigen Jahren. Doch mit einer beharrlichen Konstanz werden Entwickler, Administratoren und Anwender ihr Verständnis für die alltäglichen Gefahren einer technokratischen Gesellschaft festigen und verbessern können.

In zweierlei Hinsicht werden ihnen Hindernisse,

die jedoch durchaus überwindbar sind, in den Weg gestellt. Zum einen führt die wirtschaftliche Entwicklung der Branche dazu, dass sich die Politik einschalten will und muss. Das Politisieren birgt immer die Gefahr einer Verblendung in sich. Wenn denn nun ungeschulte Politiker über biometrische Authentifizierungen, den Sinn von Softwarepatenten oder das Strafmass für Computerdelikte diskutieren, hat dies immer etwas propagierendes ansich. Lobbyismus, eine der wichtigsten Waffen in einem demokratischen System, hat auch hier längst Einzug gehalten, wie man sehr schön an den unendlichen Disputen bezüglich der Patentierbarkeit von computerbasierender Entwicklungen sehen kann. Der Mensch muss also mehr denn je lernen, kritisch mit Informationen und den Medien umzugehen. Ein Medium wie das Fernsehen oder das Internet ist nur für die Übertragung und Aufbereitung von Informationen zuständig. Das Zusammentragen und Auswerten dieser bleibt nach wie vor den Menschen überlassen.

Die andere Gefahr ist die zunehmende Komplexität heutiger Computersysteme. Ein Rechner war vor 20 Jahren ein einfaches Gerät, das mit simplen Kommandos gefüttert werden wollte. Heutzutage gibt es tausend Möglichkeiten, wie ein System programmiert werden kann. Und entsprechend gibt es eine Million Möglichkeiten, wie dies falsch umgesetzt werden kann. Und da wir heute keinen Schritt mehr ohne technische Hilfsmittel machen können, sind wir stets der Gefahr einer solchen Fehlnutzung ausgesetzt. Betrachtet man die Wichtigkeit von Computern in unsererer Gesellschaft, dann wird einem zwangsweise das existierende Risiko dieser Abhängigkeit bewusst.

Fazit

Die IT-Branche hat in den letzten Jahren unheimlich turbulente Zeiten erlebt. Der Boom des Internets und das Zeitalter von New Economy machte Computer endgültig zu einem festen bestandteil der modernen Gesellschaft.

Mit dem Nutzen einer Technologie kommen jedoch auch immer Gefahren im Umgang mit dieser einher. Sicherheitslücken in Software-Lösungen können dazu führen, dass die Sicherheit gesamter Systeme und somit die sich dahinter befindlichen Menschen gefährdet sind.

Die IT-Branche hat die Gefahren erkannt und wollte diese in erster Linie kommerziell ausschlachten. Dass sich Sicherheit aber nur bedingt durch ein Produkt realisieren lässt, ist spätestens bei den Marketing-Hypes zu Themen wie Intrusion Detection-Systeme und PKIs klar geworden.

Das Interesse an den neuen Technologien, kindliche Neugierde und Spieltrieb hat ganze Generationen an Jugendlichen dazu getrieben, sich intensiver und kritisch mit den technischen Gegebenheiten unserer Zeit auseinanderzusetzen. Dabei sind viele wunderschöne Entwicklungen und Erfahrungen gemacht worden, die sowohl die IT-Branche als auch die Nutzer entsprechender Systeme nachhaltig geprägt haben. Der rasante Fortschritt der Technik wird es auch weiterhin wichtig und richtig machen, dass sich interessierte Leute mit dem Thema auseinandersetzen, um dieses immerwährend zu verbessern.

Der Autor

Marc Ruef arbeitet als Security Consultant bei der schweizer Firma scip AG (http://www.scip.ch), welche sich auf Sicherheitsberatungen im Bankenumfeld spezialisiert hat. Er hat eine Vielzahl an Artikeln, Büchern und Übersetzungen im Bereich Computersicherheit publiziert, betreut einige namhafte internationale Projekte auf diesem Gebiet und unterrichtet an diversen Fachhochschulen sowie Universitäten.

Impressum

scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 44 445 1818
mailto:info-at-scip.ch
http://www.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 im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. 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.