

## Contents

1. Editorial
2. Neuerungen der scip AG
3. Neue Sicherheitslücken
4. Hintergrundbericht
5. Software-Tipps
6. Buchtipps
7. Kreuzworträtsel
8. Impressum

### 1. Editorial

#### Unüberschaubare Komplexität

Freitagabend, es ist 16:30 Uhr und Sie bereiten sich darauf vor nach Hause zu gehen. Die Kaffeetasse ist abgewaschen, das Mittags-Sandwich wurde zu ende verspeist und die dringenden Arbeiten konnten erledigt werden. Die Termine und Arbeiten der anstehenden Woche sind fixiert und definiert. Voller Genugtuung denken Sie über die durchlebte Woche nach: „So darf es immer sein.“

Dring, Dring, Dring...

Ihr brandneues Büro IP-Telefon meldet sich mit einem unüberhörbaren Klingeln. Das Display zeigt den Namen und die Büronummer des Ressortleiters an. „Hmm, wird noch gearbeitet?“ Pflichtbewusst nehmen Sie den Hörer ab: „Ja, ja, verstehe, sehe gleich nach und melde mich dann bei Dir.“ Sie legen den Hörer in die Gabel zurück. Stille.

Der „Big-Boss“, derzeit in New York, wurde aus



der bestehenden Kommunikation geworfen und kann sich nicht mehr einloggen. Einmal mehr.

Wer weiss, vielleicht hat ja nur der Perimeter Firewall Cluster wieder mal eines seiner Probleme; oder ist es der Strong-Authentication Server welcher mit Zeitproblemen kämpft; ist es möglicherweise ein Routingeintrag eines Layer 3 Switches welcher nach dem erfolgreichen Test nicht gespeichert wurde, vielleicht ist es ja auch der Licensingserver der streikt oder hat sich der Benutzer mehrmals falsch angemeldet und ist nun gesperrt; möglicherweise hat auch der Provider ein Problem; oder hat das Netzwirkabel des „Big-Boss“ einen Wackelkontakt, oder, oder, oder...

Keine Hektik, nimm doch mal die Dokumentation der angesprochenen Umgebung zur Hand. In die Kommunikation sind ja 10 Systeme involviert... Okay. Kreise das Problem ein. Beginn mit der untersten Schicht und arbeite Dich hoch...

Nach einem ersten Augenschein und der ersten Rückfrage ist der Problembereich geschrumpft. Der anzusprechende Host ist eruiert und dadurch lassen sich die angrenzenden und benötigten Systeme definieren. Einige Zeit später kann der „Big-Boss“ wieder arbeiten und Sie können in das Wochenende.

Wie vorgeschrieben füllen Sie den internen Fehlerfragebogen aus. Der exakte Grund respektive das dedizierte System anzugeben ist leider nicht möglich. Mehrere Umstände haben sich kumuliert und schlussendlich dazu geführt. Diese Fehler konnten wiederum nur einfließen, da Ihre derzeitige Umgebung eine enorme Komplexität erreicht hat, so dass Fehlkonfigurationen fast nicht mehr zu verhindern sind. Um

das Ziel A zu erreichen wurden Systeme eingesetzt, welche das Ziel A zwar erfüllen, zudem aber auch die Ziele F und G. Um diese Ziele F und G zu erreichen ist aber bei anderen

Firmen auch eine zusätzliche Person engagiert...

So oder so ähnlich ist es Ihnen bestimmt auch schon ergangen. Sei es als Bezüger einer Dienstleistung, welche nicht verfügbar war, oder als Anbieter, der die Systeme am laufen halten muss. Die unüberschaubare Komplexität kommt nicht anhand der Anzahl von Systemen zustande. Der Begriff „komplex“ ansich wird in der Umgangssprache normalerweise verwendet, um eine Person oder einen Gegenstand zu beschreiben, der aus vielen miteinander interagierenden Komponenten besteht und dessen Verhalten und/oder Struktur einfach nur schwer zu verstehen ist. Eine unüberschaubare Komplexität ergibt sich jedoch meistens aus einer ungenügenden Konzeption, einer fehlenden technischen Gewaltentrennung der Systemanforderungen (nach OSI-Modell), unvollständig durchgeführten Betriebsaufwand-Näherungsberechnungen, den gewachsenen Umgebungen und den produktabhängigen Integrationspartnern.

Die Komplexität selbst ist nicht zu umgehen und ist auch nicht zu bekämpfen. Es gilt vielmehr, die spezialisierten Systeme für die ihnen angedachten Arbeiten einzusetzen. Somit ist es auch möglich zu diesen definierten Tätigkeiten Prozesse einzuführen, welche von den zuständigen Person nachvollzogen und durchgeführt werden können. Als zusätzlichen und nach meiner Auffassung immensen Gewinn kann die Eintrittswahrscheinlichkeit von sicherheitskritischen Fehlkonfigurationen und als temporär angedachten „es muss heute noch laufen“-Regeln erheblich reduziert werden.

Simon Zumstein <sizu@scip.ch>  
Geschäftsleiter  
Zürich, 10. Dezember 2003

## 2. Neuerungen der scip AG

### 2.1 RSS-Feed der Verletzbarkeitsdatenbank

Die sehr erfolgreiche und beliebte deutschsprachige Verletzbarkeitsdatenbank (bislang verweisen über 320 Websites auf die scip AG Datenbank) kann nun auch über einen RSS-Feed eingebunden werden. Somit steht es Ihnen frei über welches Medium Sie sich auf dem laufenden halten wollen. Der Pfad des RSS-Feed lautet <http://www.scip.ch/alertRSS.xml>.

Einen, nach unserer Meinung, ausgezeichneten RSS-Aggregator finden Sie unter

<http://www.activerefresh.com/abilon.php>. Für Anwender des Mozilla Firebird Browser empfehlen wir die „RSS-ReaderPanel“ Extension.

### 2.2 Kunden Online-Cockpit

Vier Wochen Testbetrieb bei zwei Kunden (vielen Dank für die Unterstützung) und das scip AG Online-Cockpit ist freigeschaltet. Somit ist es nun allen unseren Kunden möglich den Status, die Pendenzen usw. ihrer laufenden als auch der bereits beendeten Projekte, jederzeit, einzusehen.



Bei Interesse an einem Testaccount, Fragen zur Security Implementation oder zum Datenschutz, rufen Sie uns direkt an +41 1 4451818 oder senden Sie uns eine E-Mail, mit ihren Koordinaten, an die Adresse [info@scip.ch](mailto:info@scip.ch). Nach Absprache erhalten Sie die Zugangstools für ihren Testaccount.

### 2.3 Workshops

Januar 2004	
08.01.2004	Log-Management [LMVE]
13.01.2004	Attacks [ATVE]
15.01.2004	Viren [VIFT]
26.01.2004	Log-Management [LMFT]

Das scip AG Workshop-Portfolio finden Sie auf der Firmenwebseite <http://www.scip.ch>.

### 3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.

Die Dienstleistungspakete [\)scip\( pallas](#) liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.

#### Contents:

3.1 Microsoft Internet Explorer mhtml: Sicherheitszone umgehen

3.1 Microsoft Internet Explorer mhtml: Sicherheitszone umgehen

Einstufung: **sehr kritisch**

Remote: Ja

Datum: 25.11.2003

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=411>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. In den Versionen 5.01, 5.5 und 6.0 des Microsoft Internet Explorer kann das Umleitungs-Feature von mhtml-URLs dazu missbraucht werden, um die Sicherheitszonen zu umgehen. Dadurch könnte sich ein Angreifer erweiterte Rechte für das Ausführen seiner Skripte erschleichen. Entsprechend wäre das Ausnutzen einer anderen Sicherheitslücke und dadurch das Ausführen beliebigen Programmcodes auf dem Zielsystem möglich. Voraussetzung für den Angriff ist, dass in der Zone Arbeitsplatz Scriptcode ausgeführt werden darf. Ein funktionierender proof-of-concept Exploit wurde zusammen mit dem Advisory veröffentlicht. Als Workaround wird empfohlen Active Scripting nur für vertrauenswürdige Webseiten zuzulassen. Es ist damit zu rechnen, dass Microsoft das Problem mit einem Patch in den kommenden Tagen oder Wochen beheben wird.

#### Expertenmeinung:

Gleich mehrere Sicherheitslücken des Microsoft Internet Explorers hat der zur Zeit arbeitslose Liu Die Yu bekannt gemacht. Die verschiedenen Stellen fassen die Schwachstellen unterschiedlich zusammen. Einzelne Angriffsmöglichkeiten sind nämlich nur Varianten voneinander. Trotzdem ist interessant, wieviele Sicherheitslücken einmal mehr durch das lückenhafte Design des Microsoft Webbrowsers gegeben sind. Der Fortlauf der Zeit zeigt, dass der Internet Explorer in sicherheitskritischen

Umgebungen nichts zu suchen hat. Diese Sicherheitslücke wird vor allem von Webseiten mit dubiosen Inhalten dazu genutzt werden, um Programmcode auf den verwundbaren Systemen auszuführen (z.B. Installation von Dialern oder Hintertüren). Entsprechend wichtig ist es, sofort Gegenmassnahmen einzuleiten.

## 4. Hintergrundbericht

Dieser dreiteilige Hintergrundbericht zum Mythos „Virus“ ist als fundierte Aufarbeitung eines alltäglichen und breitgefächerten IT-Security Themas gedacht.

Im folgenden ersten Teil werden Sie in den Mythos eingeführt und erfahren wie sich die Viren von einem Spiel zu einem veritablen Problem gemausert haben.

In den kommenden zwei Teilen geht der Autor, Marc Ruef, dedizierter auf den Aufbau, die Funktionsweisen, die bestehenden Gefahren und die Einfallsmechanismen ein.

### 4.1 Der Mythos „Virus“

Das Substantiv Virus stammt aus dem Lateinischen und bedeutet ins Deutsche übersetzt „Schleim“ oder „Gift“ (der Plural vom lateinischen „Virus“ lautet „Virii“). Diese Übersetzung trifft die Sache aber nicht ganz. Viren sind submikroskopisch (20 bis 300 nm) kleine Gebilde, die aus einem Stück Erbinformation in Form eines DNA- oder RNA-Moleküls mit einem Proteinmantel und meistens einer Schutzhülle bestehen. Einzelnen betrachtet sind sie unbelebte Kristalle aus organischem Material.

Trifft so ein Kristall auf eine Zelle in einem Organismus, legt er seine Unbelebtheit ab. Er dringt in die Zelle ein und implantiert seine Erbinformation in den Zellkern. Die Zelle interpretiert den neuen genetischen Code und produziert neue Viren anstatt ihrer eigentlichen Aufgabe nachzugehen. Nach kurzer Zeit stirbt die infizierte Zelle, die Zellmembran platzt und die neuen Viren suchen sich zur Verbreitung weitere Zellen.

Es gibt auch Viren, die die Wirtszellen zu ungehemmter Zellteilung anregen. Wird der Stoffwechsel des betroffenen Lebewesens dabei gestört, spricht man von einer Vireninfektion. Die Auswirkungen auf den Organismus können von Unbemerktheit bis zu tödlichen Erkrankungen reichen. Einige bekannte Viruserkrankungen sind Schnupfen, Grippe, Herpes, Tollwut, Pest und AIDS.

Viren sind durch ihre einfache Struktur sehr schwer mit Medikamenten zu behandeln. Der befallene Organismus muss sie durch sein Immunsystem selbst abwehren. Dies kann Tage, Wochen, manchmal sogar Jahre dauern. Jeder

Mensch trägt ständig Viren in sich, die je nach aktuellem Zustand des Immunsystems aktiv werden können.

### Was sind nun Computerviren?

Der Begriff Computervirus oder einfach Virus hat sich in der Umgangssprache für eine ganze Gruppe von Programmen eingebürgert, die vom Fachmann als Malicious Software („böswillige Software“) oder kurz Malware bezeichnet wird. Je nach Funktion wird sie spezifischer als Virus, Wurm, Trojanisches Pferd, logische Bombe oder Hoax bezeichnet.

Viren sind Codefragmente, die sich an andere Daten anhängen und sich bei deren Ausführung oder Verarbeitung vermehren. Die anfälligen Daten können Programme, Bootsektoren oder Dokumente sein. Für sich alleine ist ein Computervirus meist nicht reproduktionsfähig. Die Analogie zu den biologischen Viren liegt auf der Hand. Malware ist natürlich keine Mutation von normaler Software sondern wird gezielt von Spezialisten programmiert. Zum Programmieren eines überlebensfähigen Computervirus oder eines Wurmes gehören sehr hohe Fachkenntnis und Wissen über das zugrundeliegende Betriebssystem. Daher gibt es wohl nur wenige Programmierer, die selbstständig solche Programme entwickeln können – Vor allem in einer Zeit, wo in Hochsprachen programmierten Computerviren mit wenigen Handgriffen umgesetzt werden können. Was häufiger auftritt sind so genannte Mutationen, bei denen ein weniger erfahrener Programmierer eine bestehende Spezies abändert, ihr z.B. eine neue Botschaft oder Aktion mitgibt. Oder das Erstellen mit Viren-Generatoren, die zahlreich auf einschlägigen Internetseiten zu finden sind. Diese Viren gelten jedoch meist als sehr primitiv und werden von Antiviren-Programmen in der Regel auch stets erkannt.

### Die Geschichte der Computerviren

Die Theorie des Computervirus geht bis ins Jahr 1949 zurück, auch wenn damals noch niemand im speziellen an solche Programme dachte: Der ungarische Informatiker John von Neumann (1903-1957) entwickelte die Theorie der sich selbst reproduzierenden Automaten.

Anfang der 70er Jahre erfanden Mitarbeiter der Bell Laboratorien ein Spiel namens "Core Wars" (Krieg der Kerne), dass dem Prinzip eines Virus schon sehr nahe kam. Ziel des Spieles war es, dem Gegner die kostbare Rechnerzeit zu stehlen. "Core Wars" kann man als den ersten Computerwurm der Geschichte Bezeichnen. Er war jedoch zu seiner Verbreitung noch auf die Hilfe des Programmierers angewiesen.

Der Begriff "Computervirus" wurde 1981 von Professor Adleman eingeführt. Er rief diesen Begriff während eines Gesprächs mit dem Doktoranden Fred Cohen ins Leben. Fred Cohen war es dann auch, der zwei Jahre später den ersten funktionsfähigen Virus vorstellte. Er war unter Unix programmiert und nistete sich im Befehl VD ein. Der Virus erbte bei jeder Ausführung die Systemprivilegien des infizierten Programms und konnte so innerhalb kürzester Zeit jedem Benutzer diese Privilegien übertragen.

1984 lieferte Fred Cohen seine Doktorarbeit ab, deren Veröffentlichung lange Zeit umstritten war. Sie enthielt neben dem beschriebenen Virus noch andere experimentelle Viren. Von da an, fand eine rasante Entwicklung statt: Ständig kamen neue Viren in Umlauf. 1985 wurde in den USA ein Virus namens EGABTR über Mailbox verbreitet. Das Programm war als Hilfsmittel zur Verbesserung der damals noch sehr mangelhaften Grafikmöglichkeiten getarnt. Nach dem Start löschte EGABTR alle Dateien auf der Festplatte und gab folgende Meldung aus: "Arf, arf Gotcha!" (Arf, arf hab Dich!)

#### **Die Anfänge der nervenden Computerviren**

Im darauf folgenden Jahr kam dann der erste MS-DOS-Virus in Umlauf. Der Pakistani- oder auch Brain-Virus war von zwei Softwarehändlern in Pakistan entwickelt worden. Da das Kopieren von Software dort nicht strafbar war, verkauften die Händler billige Raubkopien von Originalsoftware, die mit Pakistani-Virus verseucht waren. Die Absicht der Händler war es, ihre Kunden auf diese Weise an ihren eigenen Servicedienst zu binden. Zu diesem Zweck enthielt der Viruscode auch die volle Anschrift der Softwareladens. Überraschend mag es für die beiden mag es dann allerdings gewesen sein, dass sich der Virus sogar bis in die USA verbreitete.

McAfees erster Virens Scanner kannte 1987 bereits 19 Viren, im Jahre 1997 lag die Zahl der erkennbaren Viren bei über 5'000 Stück. Dr. Solomons Anti-Virus war einen Schritt voraus, denn er war in der Lage über 14.000 Viren bzw. ihre Abarten zu erkennen.

Nachdem 1987 der erste Virus für Macintosh-Rechner entdeckt wurde, lieferte Apple seine Rechner gleich mit einem Virensucher aus. Dieses Programm war allerdings lediglich auf die eine Virusfamilie spezialisiert und somit nicht für die Verhütung neuer Viren geeignet.

1987 verbreitete sich auch der erste Wurm in einem IBM-System. Ein deutscher Student lies

auf allen Rechnern eines IBM-Netzwerks einen Weihnachtsbaum auf dem Bildschirm erscheinen. Der Weihnachtsbaum verschwand nur, wenn der Benutzer CHRISTMAS eintippte. Im Hintergrund durchsuchte das Programm die Mailliste des Benutzers und schickte sich selbst an alle eingegebenen Adressen. Auf diese Weise konnte sich der IBM-Wurm explosionsartig vermehren.

Ein weiterer berühmter Fall war der Lehigh-Virus. Er verlängerte die COMMAND.COM um 555 Bytes und überschrieb dabei den Stack am Ende einer Datei. Der Virus überprüfte dann bei jedem Lesen einer Diskette, ob die Datei COMMAND.COM bereits infiziert ist oder nicht. Nach jeder vierten Infektion wurde ein Teil der gelesenen Diskette überschrieben. Entdeckt wurde der Virus, nachdem mehrere hundert Studenten der Lehigh-Universität in den USA ihre Systemdisketten zurückgaben, da sie nicht mehr bootfähig waren.

Einer der ersten Viren, die eine gewisse Berühmtheit erlangten, war der PLO- oder Jerusalem-Virus, bekannter unter dem Namen Freitag-der-13.-Virus. Er hat zwei Auswirkungen: An jedem 13. eines Monats der auf einen Freitag fällt, löscht er alle COM- und EXE-Dateien. An allen anderen Tagen, verringert der Virus nach 30 Minuten die Rechnergeschwindigkeit.

#### **Der Virus wird langsam zum Problem**

1989 kam eine Version vom McAfees Virens Scanner auf den Markt, die bereits 44 Viren erkannte. IBM hatte ebenfalls ein Virensuchprogramm entwickelt. Es kannte jedoch erst 28 Viren.

In diesem Jahr tauchte in Australien und Neuseeland der Marihuana-Virus auf. Er infizierte die Bootsektoren von 5,25-Zoll-Disketten mit 360 KB Kapazität. Bei jedem achten Programmaufruf wird auf dem Bildschirm ein Text ausgegeben, der dazu auffordert, Marihuana zu legalisieren. Durch den Internet-Wurm wurden innerhalb weniger Stunden tausend Rechner infiziert - An das amerikanische Internet-Netz sind unter anderem auch die Weltraumbehörde, NASA und das amerikanische Verteidigungsministerium (Pentagon) angeschlossen.

Ebenfalls 1989 wurde ein gravierender Fall der Verbreitung eines Virus über ein Trojanisches Pferd bekannt: Die in Panama registrierte Firma PC Cyborg Corporation verschickte an Fachkräfte und Teilnehmer einer internationalen AIDS-Konferenz Disketten mit angeblich wichtigem Informationsmaterial. Es sollte sich um eine Art Datenbank handeln, die zuerst mit dem

Befehl INSTALL auf die Festplatte installiert werden musste. Im beiliegenden Lizenzvertrag wies der Hersteller darauf hin, das bei längerer Nutzung eine Gebühr von 378 US-Dollar zu zahlen sei. Andernfalls würden wichtige Daten verschlüsselt werden. Bei der Installation benannte das Programm die AUTOEXEC.BAT in AUTO.BAT um und setzte das eigentliche Trojanische Pferd in den Computer. Dieses enthält einen Zähler der bei dem neunzigsten Neustart des Rechners den Inhalt der Festplatte verschlüsselt. Einer der Firmeninhaber wurde kurz darauf in Großbritannien verurteilt und anschliessend in eine geschlossene Psychiatrische Anstalt eingewiesen.

Nicht verwechseln darf man das Trojanische Pferd mit dem AIDS-Virus, der aus dem gleichen Jahr stammt. Der AIDS-Virus überschreibt den Anfang von Dateien und gibt auf dem Bildschirm die Meldung aus, "Your Computer now has AIDS" (Ihr Computer hat nun AIDS) Nach dieser Meldung bricht das System ab, und der Rechner muss neu gestartet werden. Gegen diesen Virus hilf nur das Löschen der Infizierten Datei.

## 5. Software-Tipps

### 5.1 PasswordSafe

<http://www.schneier.com/passsafe.html>

Hersteller: Counterpane  
Thema: Kryptographie  
Kategorie: Utility, Security  
Plattform: Microsoft Windows  
Lizenztyp: Freeware

Funktionalität	Sehr gut
Technik	Sehr gut
Ergonomie	Gut
Gesamtbewertung	Sehr gut

Sind Sie eine der glücklichen Personen welche sich seine Passwörter merken kann? Privat und Geschäftlich? Ändern Sie diese auch regelmässig? Zum Beispiel für Ihren Webmail Account oder ist es seit 4 Jahren unverändert? Sind Sie der Betreuer einer VPN-Umgebung in welcher pre-shared Keys zum Einsatz kommen?



Wir alle benötigen eine Unzahl von Passwörtern oder ID's. Sei dies nun für den Firmenlogin, die Website, das private Mail oder die pre-shared Keys der VPN-Umgebung.

Ein nicht ganz neues aber stets sehr nützliches Tool ist PasswordSafe von Counterpane <http://sourceforge.net/projects/passwordsafe/>. Dank dieser Freeware Software können Sie Ihre persönlichen oder auch geschäftlichen Passwörter verwalten. Es steht Ihnen frei mehrere Datenbanken zu eröffnen. Somit kann der Zugang zu Daten dediziert erlaubt werden. Eine für die PSK's eine für die Root-Logins der Webserver usw. Zudem ist es nicht notwendig die Software zu installieren.

Ein einfaches aber sehr hilfreiches Tool welches ich schon seit geraumer Zeit verwende.

Falls Sie detaillierte Informationen zur Software

und dessen Programmierung suchen so wagen sie einen Blick in dieses Dokument [http://passwordsafe.sourceforge.net/passwordsafe\\_software\\_patterns.pdf](http://passwordsafe.sourceforge.net/passwordsafe_software_patterns.pdf).

## 6. Buchtipps

### 6.1 Das Hannibal-Syndrom – Phänomen Serienmord

Autor: Stephan Harbort  
Verlag: Militzke  
Datum: März 2001  
ISBN: 386189209X  
Thema: Kriminalität, Serienmord, Profiling  
Kategorie: Sachbuch  
Sprache: Deutsch



Lesefluss	Sehr gut
Handlungsstrang	Sehr gut
Bezug zur IT-Security	Indirekt
Gesamtbewertung	Gut

Im Moment scheint es in der Fernsehlandschaft mehr denn je Mode zu sein, über Verbrechen aufzuklären und diese in wissenschaftlicher Weise vorzutragen. Sendungen wie „Anwälte der Toten“ oder „Autopsie – Mysteriöse Todesfälle“ zeigen auf, dass die Kriminologie nicht nur aus Polizisten besteht, die einem Verbrecher nachjagen, um ihn dingfest zu machen. Oft steckt bei der Ermittlung in einem Verbrechen ein ganzer Apparat dahinter, der das Aufspüren und Überführen des Verdächtigen erst ermöglicht.

#### Vom Profil zum Täter

Stephan Harbort erläutert in seinem Buch anhand von begangenen Taten sehr eindrucksvoll, wie Serienmorde entstehen und wie die Polizei bei Ermittlungen in solchen Fällen vorgeht.

Eine wichtige Aufgabe wird sodann den Profiliern zuteil, die durch psychologische und soziologische Analysen ein Täterprofil erstellen sollen. Anhand dem kann der Kreis der verdächtigen Personen eingeschränkt werden. Es wird aber auch ein „berechnen“ des Täters möglich: Wann, wo und in welcher Form wird er wahrscheinlich wieder zuschlagen? Können diese Fragen frühzeitig beantwortet und kann dadurch rechtzeitig gehandelt werden, lassen sich weitere Morde verhindern und der Täter überführen.

#### Der Bezug zur IT-Sicherheit

Die Kontroversen um das Thema des Schutzes

von Daten und Systemen hat sich in einer ersten Phase auf das kompetente Protokollieren und Eindämmen des Datenverkehrs durch sogenannte Firewalls konzentriert. Erst in einem weiteren Schritt wurde das bis dato noch junge Konzept der elektronischen Einbruchserkennung aufgegriffen und salonfähig gemacht. Intrusion Detection-Systeme halten Ausschau nach Anomalien im Netzwerk oder auf einzelnen Systemen, melden etwaige Abweichungen der Richtlinien und lassen gar in Extremsituationen automatisiert Gegenaktionen in die Wege leiten.

Man kann also sagen, dass sich die Sicherheit auf dem Computersektor in rasendem Tempo weiterentwickelt; und doch ist ein wichtiger Aspekt teilweise vergessen oder ignoriert worden: Auch in der Technik spielt die menschliche Psyche und die damit unweigerlich verbundenen sozialen Aspekte eine gewichtige Rolle, denn bis ins jüngste Jahrtausend wird die Entwicklung, Realisierung, Betreuung von technischen Geräten durch den Menschen begleitet. So ist es nicht verwunderlich, dass sich Angreifer psychologischen Tricks bedienen um ihre Opfer besser verstehen zu können. Wieso sollte also nicht auch das potentielle Opfer einen Angreifer analysieren und manipulieren können, wie es die Kriminalpolizei schon seit Jahren durch das "Täterprofiling" erfolgreich praktiziert?

Genau hier helfen Bücher wie dieses, die einem das Denken und Vorgehen eines Profilers vortragen, weiter. Nicht wenige Methodiken können übernommen und auf das Gebiet der Computersicherheit angewendet werden.

### Fazit

Die von Harbort zusammengetragenen Fallstudien würde ich gerne als Standardwerk im nicht-wissenschaftlichen Sinne für den deutschen Raum bezeichnen. Er schildert sehr detailliert die Geschehnisse und versucht sich sehr tiefgründig, auch auf verschiedenen Ebenen (Psychologie, Soziologie, Ethik, Moral), mit einem enorm vielschichtigen Problem auseinanderzusetzen.

Das einzige, was mich etwas gestört hat ist, dass das Buch eher wie ein Roman aufgebaut ist. Mir fehlen da die jeweiligen Sortierungen nach Kapiteln, zum Beispiel in Form von Tathergang oder Motive. Dies ist wiederum ein Vorteil für all jene, die sich nicht hustenderweise an einem trockenen Werk eines Puristen verschlucken wollen. Trotzdem erdreiste ich mich, nicht die volle Punktzahl zu geben, denn auch die direkten Querverweise auf andere Quellen - im Anhang werden zwar Buchtitel genannt, aber die

Sortierung ist in meinen Augen etwas unglücklich - vermisste ich in einem solchen semi-wissenschaftlichen Werk schmerzlich.

Stephan Harbort hat im September 2002 den zweiten Teil seiner Reihe, das Buch trägt den Titel „Mörderisches Profil – Phänomen Serientäter“ (ISBN 3861892685) herausgegeben.

Weitere Verweise auf Bücher aus dieser Sparte finden sich im World Wide Web unter <http://www.serienkiller.de/shop.html>



## 8. Impressum

Herausgeber:

scip AG

Technoparkstrasse 1

CH-8005 Zürich

T +41 1 445 1818

<mailto:info@scip.ch>

<http://www.scip.ch>

Zuständige Person:

Marc Ruef

Security Consultant

T +41 1 445 1812

<mailto:maru@scip.ch>

PGP:

[http://www.scip.ch/firma/facts/maru\\_scip\\_ch.asc](http://www.scip.ch/firma/facts/maru_scip_ch.asc)

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserung möglich. Senden Sie Ihr Schreiben an [smss-feedback@scip.ch](mailto:smss-feedback@scip.ch). Anfragen bezüglich der Erstellung eines **Erfahrungsaustausch Artikels**, senden Sie bitte an die E-Mail <mailto:sizu@scip.ch>.

Die ausgewiesenen IT-Security Spezialisten der scip AG verfügen, in diesem sehr komplexen sowie breitgefächerten Spezialgebiet, über jahrelang erarbeitetes und angewandtes Wissen. Wir sind der **effiziente** und **persönliche** Partner im Sektor: IT-Sicherheit. Bei Fragen, Schulungen, Assessments und Projekten im Bezug zur IT-Security finden Sie eine kompetente Anlaufstelle in uns.

### Nutzen Sie unsere Dienstleistungen!

Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online unter <http://www.scip.ch/publikationen/smss/>.

Der Bezug des scip monthly Security Summary ist **kostenlos**. Sie können sich mit einer Email an die Adresse [smss-subscribe@scip.ch](mailto:smss-subscribe@scip.ch) eintragen. Um sich auszutragen, senden Sie Ihr Email an die Adresse [smss-unsubscribe@scip.ch](mailto:smss-unsubscribe@scip.ch)