

## Contents

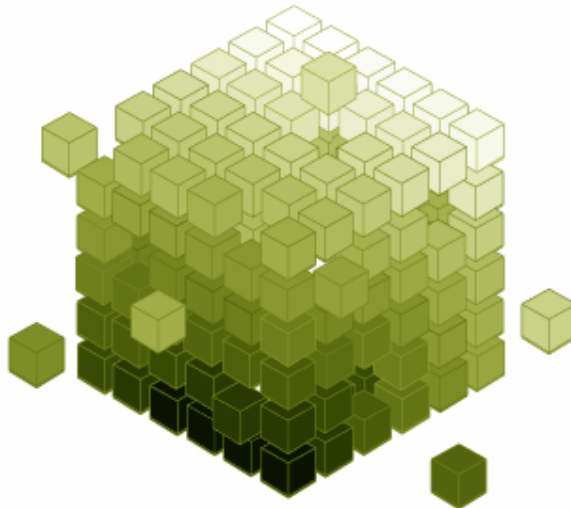
1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Interview
5. Kreuzworträtsel
6. Literaturverzeichnis
7. Impressum

### 1. Editorial

#### Ist Science-Fiction wegweisend?

Der Faszination Science-Fiction können sich die wenigsten entziehen [scip 2003]. Nebst den aufregenden und sonderbaren ausserirdischen Lebensformen ziehen einen vor allem die im Einsatz stehenden technischen Geräte und Gimmicks in ihren Bann.

Die Faszination an diesen Gegenständen beruht vermutlich auf zwei Grundlagen. Deren jetzige Unerklärbarkeit und dem für uns greifbaren und dadurch effektiven Nutzen. Denken wir nur an die Sprachimplantate durch welche wir eine uns fremde Sprache beherrschen ohne diese zuvor mühsam gelernt zu haben. Geschweige denn die Replikatoren, welche uns aus irgendwelchen Molekülen eine feinschmeckende Portion Kartoffelstock mit Sauce, feingedünsteten Karotten und ein schmackhaftes Stück Hackbraten auf den Teller zaubern.



Viele der in Science-Fiction [Wikipedia] Büchern vorhandenen Armaturen werden wohl nie das Antlitz unserer Welt erklimmen. Andere sind bereits in leicht verändert Form auf der Erde angekommen und weitere sind in Arbeit. Selbst „erfundene“ Bezeichnungen werden offiziell in den Sprachduden übernommen: „*bea|men* [':] <engl.> (bis zur Unsichtbarkeit auflösen und an einem anderen Ort wieder Gestalt annehmen lassen [in Science-Fiction-Filmen]); *gebeamt*“.

Die Grenzen zwischen Science-Fiction, Realität, Utopie und Fantasie können nicht klar gezeichnet werden und ändern sich mit jedem Pulsschlag.

Diese Erkenntnis bestimmt auch den Bereich der IT-Security. Vor Jahren wäre ein firmeninterner Rollout mit zertifikatsbasierten Chipkarten, zur Anmeldung an der Firmenworkstation, noch als Utopie verschrien worden (ausgenommen in der PKI-Boom-Seifenblasen-Zeit). Heute steht ein solches Projekt kurz vor seinem Abschluss. Was vor ein paar Jahren noch als Fiktion abgetan wurde sehen wir heute im Einsatz. Wenn ich mir vor Augen führe, wie einige Rechenzentren der Grossfirmen, vor physikalischem Zugriff abgesichert sind und welche technischen Mechanismen dabei Einhalt fanden, so leben einige Personen von uns schon heute in der Zukunft.

Doch in unserer realen Welt sind technische Komponenten nur ein Zahnrad einer gesamtheitlichen Security Lösung. Organisatorische Definitionen unterstützen und bestimmen die technische Umsetzung und sind dadurch ebenbürtig oder gar einflussreicher.

Im Themenkreis der Security sind seit den Terroranschlägen in den USA, vom 11. September 2001, vor allem die gesetzlichen Grundlagen regem Wechsel unterlegen. In diesem Zusammenhang sowie mit der

Globalisierung der Unternehmen, verwischen die klar gezeichneten und in der Schule gepaukten Ländergrenzen zusehens. Ein Gesetzesentwurf der Vereinigten Staaten kann, in der heutigen Zeit, direkte Auswirkungen auf die IT-Umgebung von schweizerischen Firmen haben. Inwiefern solche Vorgaben mit unseren eigenen Datenschutzgesetzen zu vereinbaren sind muss bei jedem Fall dediziert begutachtet und abgeklärt werden.

Die Gesetzes-Spirale hat erst begonnen sich zu drehen. Ich gehe davon aus, dass der IT-Security grössere Änderungen bevorstehen. Diese werden durch den „Motor“ Norm/Gesetze vorantgetrieben.

Resumierend aufgenommen denke ich, dass einige der in Science-Fiction Büchern aufgenommen technischen Komponenten unser Leben verändern werden. Um ein zigfaches bedeutender sind jedoch die kommenden gesellschaftlichen und politischen Entwicklungen der uns bekannten Welt und die vermag keiner vorherzusehen!

Simon Zumstein <sizu@scip.ch>  
Geschäftsleiter  
Zürich, 18. Juni 2004

## 2. scip AG Informationen

### 2.1 Firmenprofil

Sind Sie über die erfolgreich durchgeführten Projekte der scip AG im Bild? Ist Ihnen bekannt nach welchen Leitmotiven die scip AG die ihr anvertrauten Arbeiten ausführt? Wissen Sie was die scip AG für Dienstleistungen anbietet oder wer bei der scip AG arbeitet und welchen Wissensschatz er sein eigen nennen kann?

Antworten auf Ihre Fragen finden Sie im neu publizierten scip AG Firmenprofil. Sie finden dieses über den folgenden Link:  
[http://www.scip.ch/firma/scipAG\\_CompanyProfile\\_de.pdf](http://www.scip.ch/firma/scipAG_CompanyProfile_de.pdf)

Wir beraten Sie gerne. Nutzen Sie unsere Dienstleistungen!

### 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 6 %2F Zonenmodell umgehen
- 3.2 Apache bis 1.3.32 mod\_proxy Content-Length Pufferüberlauf
- 3.3 Microsoft ISA Server 2000 Web Proxy Blacklist mit Punkt umgehen
- 3.4 Cisco Catalyst Switches CatOS TCP-Verbindungsaufbau Denial of Service
- 3.5 Squid Web Proxy Cache bis 3.x NTLM Authentication Helper Pufferüberlauf
- 3.6 Microsoft Internet Explorer bis 6 Location URL beliebigen Programmcode ausführen
- 3.7 MIT Kerberos5 krb5\_aname\_to\_localname() Pufferüberlauf
- 3.8 Apache mod\_ssl 2.x ssl\_util\_uuencode\_binary() Pufferüberlauf

#### 3.1 Microsoft Internet Explorer 6 %2F Zonenmodell umgehen

Einstufung: **sehr kritisch**  
 Remote: Ja  
 Datum: 11.06.2004  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=710>

Der Microsoft Internet Explorer ist mit seiner Verbreitung von schätzungsweise 95 % der mitunter populärste Webbrowser der aktuellen Stunde. Seine hohe Verbreitung ist unter anderem darauf zurückzuführen, dass er ein fester Bestandteil moderner Windows-Betriebssysteme ist. bitlance winter hat herausgefunden, dass durch das codierte Slash-Zeichen %2F das Zonenmodell umgangen und Adressbar-Spoofing betrieben werden kann. So wird zum Beispiel über die URL <http://www.scip.ch/%2F%20%20%20.www.computec.ch/> die manipulative Seite [www.computec.ch](http://www.computec.ch) mit den Rechten der vertrauenswürdigen Seite [www.scip.ch](http://www.scip.ch) geladen. Als Lösung wird empfohlen alle Zonen im Internet Explorer auf die Sicherheitsstufe High zu setzen oder sich endlich für einen alternativen Webbrowser zu

entscheiden. Der Artikel "Verrammelt, Internet Explorer sicher konfigurieren" in der aktuellen c't 13/04 erläutert, wie man die Sicherheitszonen des Internet Explorer nutzen kann, um auf unbekanntem Web-Sites potenzielle Sicherheitsrisiken wie ActiveX oder JavaScript zu verbieten. Es ist damit zu rechnen, dass Microsoft dem Problem beim kommenden Patchday Rechnung tragen wird.

#### Expertenmeinung:

Für eine Vielzahl der Angreifer ist diese Schwachstelle interessant. Der Internet Explorer genießt nach wie vor eine sehr hohe Verbreitung und die Schwachstelle öffnet Tor und Angel zu einem System. Von Skript-Kiddies bis hin zu Dialer-Anbieter können alle Schichten ein Interesse an der Sicherheitslücke haben. Umso wichtiger ist es, dass schnellstmöglich Gegenmassnahmen getroffen werden, um die betroffenen Benutzer nicht exponiert zu lassen. Je länger je mehr wird es plausibel, auf den Einsatz des Internet Explorers zu verzichten und sich nach alternativen Webbrowser-Lösungen umzuschauen. Eine im mindesten aus Sicherheitssicht legitime Entscheidung.

#### 3.2 Apache bis 1.3.32 mod\_proxy Content-Length Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 10.06.2004  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=706>

Apache ist ein populärer, freier open-source Webserver, der für viele verschiedene Plattformen erhältlich ist. In der 1er-Familie entdeckte Georgi Guninski eine Pufferüberlauf-Schwachstelle bei der Verarbeitung langer Content-Length-Parameter im HTTP-Header einer Anfrage. Darüber kann das Modul mod\_proxy zum Absturz gebracht und theoretisch auch beliebiger Programmcode ausgeführt werden. Zusammen mit dem Advisory wurde ein in Perl geschriebener proof-of-concept Exploit publiziert. Ebenfalls ist im Advisory ein Fix enthalten, wobei das Problem durch das Apache Team selber in der Version 1.3.32 behoben wurde. Die jeweiligen Linux-Distributoren haben mit einer Aktualisierung ihrer Pakete reagiert. Als Workaround kann empfohlen werden, die HTTP-Anfragen vor der Verarbeitung durch den Apache-Server durch ein restriktives Application Gateway überprüfen zu lassen oder den mod\_proxy direkt zu deaktivieren.

#### Expertenmeinung:

Wie immer bedeutet dies, dass mit einer Vielzahl

neuer Angriffe auf die jungen Schwachstellen zu rechnen ist. Skript-Kiddies werden die Gunst der Stunde nutzen wollen, um ihren Spielereien nachzugehen. Aufgrund der hohen Verbreitung des Apache sind die gefundenen Fehler wahrlich ein gefundenes Fressen. Umso wichtiger ist, es seine Systeme schnellstmöglich zu schützen, was in erster Linie mit dem Einspielen der vorgeschlagenen Patches bzw. den Update auf die aktualisierte Apache Version getan werden sollte. Es ist nur eine Frage der Zeit, bis produktive Exploits die Runde machen werden.

### 3.3 Microsoft ISA Server 2000 Web Proxy Blacklist mit Punkt umgehen

Einstufung: **kritisch**  
Remote: Ja  
Datum: 10.06.2004  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=704>

Der Microsoft Internet Security and Acceleration Server (MS ISA) ist ein Application Gateway für Windows, das verschiedene Proxies zur Verfügung stellt. Microsoft hat im Microsoft Knowledge Base Article 816460, der Versionsinformationen für ISA Server 2000 Service Pack 2 zur Verfügung stellt, bekannt gegeben, dass mehrere Schwachstellen in der Lösung existent sind. Eine davon betrifft den Web Proxy, bei dem die Blacklist von URLs insofern umgangen werden kann, dass am Domain-Name ein zusätzliche Punkt angehängt wird (z.B. [http://www.scip.ch.](http://www.scip.ch)). Zusätzliche technische Informationen zur Schwachstelle oder ein Exploit sind nicht bekannt. Die Schwachstelle wurde mit dem Service Pack 2 behoben.

#### Expertenmeinung:

Diese Schwachstelle wurde unter anderem schon in anderen Proxy-Lösungen, wie zum Beispiel durch Marc Ruef im Finjan SurfinGate, entdeckt. Die Primitivität dieser Schwachstelle sollte eigentlich verhindern, dass eine solche bei der Entwicklung überhaupt übersehen werden kann - Vor allem, wenn der Fehler schon in anderen Produkten besprochen wurde.

### 3.4 Cisco Catalyst Switches CatOS TCP-Verbindungsaufbau Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 09.06.2004  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=699>

Die Firma Cisco hat sich einen Namen mit ihren scip monthly Security Summary  
Marc Ruef & Simon Zumstein  
scip\_mss-19\_06\_2004-1.doc

Netzwerkelementen - Switches und Router - gemacht. Eines dieser Switch-Produkte trägt den Namen Catalyst und ist mit dem hauseigenen Catalyst OS ausgestattet. Wie Cisco in ihrem Advisory bekannt gibt, existiert eine Denial of Service-Schwachstelle während des Verbindungsaufbaus von TCP. Dieser wird dadurch umgesetzt, indem anstatt des obligaten ACK-Bestätigungspakets zur Etablierung der Sitzung ein fehlerhaftes Paket an das Cisco-System geschickt wird. Auf den jeweiligen Elementen sind die Dienste Telnet, SSH und HTTP betroffen. Laut Cisco sind der HTTP- und SSH-Dienst standardmässig unter CatOS deaktiviert. Ob SSH oder HTTP aktiviert sind, können Anwender auf die Schnelle mit einem Telnet-Zugriff auf Port 80 und 22 feststellen. Ein erfolgreicher Angriff führt zu einem Neustart des Geräts. Im Advisory wird eine Patch-Matrix bereitgestellt, die darüber informiert, welches CatOS verwundbar ist und welcher Patch eingespielt werden soll. Eine alternative Lösung ist der Einsatz von ACL auf den Cisco-Geräten oder das Miteinbeziehen dedizierter Firewall-Systeme.

#### Expertenmeinung:

Cisco-Router sind sehr beliebt, weshalb diese Angriffsmöglichkeit mit offenen Armen empfangen wurde. Besonders Skript-Kiddies werden nach Erscheinen eines Exploits wahre Freude daran haben, Teile des Internets abzuschliessen. Diese Schwachstelle kann praktisch als kleiner Bruder der im Juli 2003 publizierten Denial of Service-Schwachstelle in der IPv4-Verarbeitung des IOS [scipID 180; <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=180>] Es gilt unbedingt und unverzüglich entsprechende Gegenmassnahmen einzuleiten und die herausgegebenen Patches einzuspielen.

### 3.5 Squid Web Proxy Cache bis 3.x NTLM Authentication Helper Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 08.06.2004  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=698>

Squid ist ein open-source Projekt, das einen freien und hochskalierbaren Proxy für Unix-Systeme zur Verfügung stellt. Es werden Protokolle wie HTTP und FTP sowie Funktionalitäten wie SSL-Unterstützung, Cache-Hierarchien und Zugriffskontrolllisten bereitgestellt. Im iDEFENSE Security Advisory

06.08.04 wird über eine eingekaufte Schwachstelle berichtet, die den NTLM Authentication Helper von Squid bis 3.x betrifft. `ntlm_check_auth()` in `helpers/ntlm_auth/SMB/libntlmssp.c` weist einen Pufferüberlauf auf, der durch ein zu langes Passwort bei der NTLM-Authentisierung erzwungen werden kann. Darüber wäre das Ausführen beliebigen Programmcodes denkbar. Ein Exploit ist bisher nicht bekannt. Als Workaround wird im Advisory angegeben, den Squid-Proxy ohne NTLM-Support zu re-kompilieren. Das Squid-Team hat jedoch auch einen Patch für die Schwachstelle herausgegeben, der rund einen Tag später auch von den jeweiligen Linux-Distributoren verteilt wurde.

#### Expertenmeinung:

Die Schwachstelle ansich ist nichts besonderes. Interessant hierbei ist, dass es sich um eine eingekaufte Schwachstelle handelt, deren Finder laut iDEFENSE unbekannt bleiben möchte. Die Beweggründe für die Publikation der Schwachstelle können also primär finanzieller Natur sein. Durchaus ist es aber auch möglich, dass jemand die Schwachstelle verkauft hat, der direkt am Squid-Projekt beteiligt war oder ist. Der Ankauf und Verkauf von Informationen zu Schwachstellen wird wohl in Zukunft ein noch grösseres Thema werden.

### 3.6 Microsoft Internet Explorer bis 6 Location URL beliebigen Programmcode ausführen

Einstufung: **sehr kritisch**  
 Remote: Ja  
 Datum: 07.06.2004  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=697>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Wie auf Full-Disclosure seit einiger Zeit heftigst diskutiert wurde, existiert eine Schwachstelle, die es einem Angreifer ermöglicht, beliebigen Programmcode herunterzuladen und auszuführen. Erste Hinweise auf das Problem gab es bereits Mitte Mai auf Bugtraq [<http://www.securityfocus.com/archive/1/363338>]; es wurde also bereits seit etwa einem Monat aktiv ausgenutzt. Eine ausgezeichnete Analyse der Angriffsmöglichkeit wurde unter <http://62.131.86.111/analysis.htm> dokumentiert. Ebenso ist dort ein Link auf einen proof-of-concept Exploit vorhanden. Da der Angriff über ein JavaScript initiiert wird, kann das

Deaktivieren von aktiven Inhalten Abhilfe schaffen. Es ist damit zu rechnen, dass Microsoft spätestens beim nächsten Patch-Day dem Problem Rechnung tragen wird. Der gestrige Patch-Day hat jedoch nur Schwachstellen in Direct Play/DirectX und Crytal Reports adressiert [<http://www.heise.de/newsticker/meldung/48066>].

#### Expertenmeinung:

Für eine Vielzahl der Angreifer ist diese Schwachstelle interessant. Der Internet Explorer genießt nach wie vor eine sehr hohe Verbreitung und die Schwachstelle öffnet Tor und Angel zu einem System. Von Skript-Kiddies bis hin zu Dialer-Anbieter können alle Schichten ein Interesse an der Sicherheitslücke haben [<http://www.heise.de/newsticker/meldung/48128>]. Umso wichtiger ist es, dass schnellstmöglich Gegenmassnahmen getroffen werden, um die betroffenen Benutzer nicht exponiert zu lassen. Interessant ist, dass nun tatsächlich der Worst Case in Bezug auf Microsofts Patch-Day Politik eingetroffen ist: Kurz vor einem Patch-Day wird ein schwerwiegender Fehler publik, der im kommenden Patch-Day nicht mehr behoben werden kann. Die Benutzer und Administratoren sind nun dazu verdammt, mindestens 30 Tage bis zum nächsten Patch-Day zu warten, bis das Problem adressiert wird. Dies bedeutet 30 Tage höchste Verwundbarkeit für die Benutzer des Internet Explorers. Stephen Toulouse, Sicherheitschef bei Microsoft, liess jedoch Tage nach dem Bestätigen der Schwachstelle verlauten, dass man noch vor dem kommenden Patch-Day einen Bugfix herausgeben wolle.

### 3.7 MIT Kerberos5 krb5\_aname\_to\_localname() Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 01.06.2004  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=684>

Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen. Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Wie das MIT meldet, existieren mehrere Pufferüberlauf-Schwachstellen in der Funktion `krb5_aname_to_localname()`. Einem Angreifer ist es darüber möglich, administrative Rechte zu erlangen. Laut des Advisory bedarf es einer "ungewöhnlichen Kombination" an Faktoren, um den Fehler auszunutzen. Default-Installationen sind voraussichtlich nicht betroffen, da das regelbasierte Mapping aktiviert worden sein

müsse. Dadurch sind auch Login-Dienste wie ftp, rsh und rlogin anfällig, sofern sie die Kerberos5-Library mit der fehlerhaften Funktion nutzen. Exploits für die Schwachstelle sind nicht bekannt, technische Details lassen sich aber indirekt aus dem Advisory extrahieren. Das MIT stellt einen Patch zur Verfügung - Alternativ kann die besagte Mapping-Funktion deaktiviert werden.

#### Expertenmeinung:

Die hohe Verbreitung von Kerberos sowie die Möglichkeiten eines Angriffs machen diese Schwachstelle für eine Vielzahl an Angreifern sehr interessant. Jedoch ist das Risiko eingedämmt, da die Sicherheitslücke nur unter gewissen Umständen ausnutzbar ist. Administratoren werden angehalten so schnell wie möglich ihre Systeme zu überprüfen und im Notfall unverzüglich Gegenmassnahmen einzuleiten. Es ist damit zu rechnen, dass in den kommenden Tagen ein Exploit erscheinen wird.

### 3.8 Apache mod\_ssl 2.x ssl\_util\_uencode\_binary() Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 17.05.2004  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=673>

Apache ist ein populärer, freier open-source Webserver, der für viele verschiedene Plattformen erhältlich ist. Durch verschiedene Module kann der Webserver um gewisse Funktionalitäten erweitert werden. Das Modul mod\_ssl ermöglicht das Einbinden von mit SSL geschützten HTTPS-Kommunikationen. Wie Georgi Guninski auf Full-Disclosure berichtet, besteht in diesem Modul ein Pufferüberlauf in der Funktion ssl\_util\_uencode\_binary(). Diese ist für das Verarbeiten von Client-Zertifikaten zuständig. Wird bei einem solchen eine überlange Subject-DN (mehr als 6KB) herangezogen, kann das Modul zum Absturz oder theoretisch gar beliebiger Programmcode über den Heap Overflow ausgeführt werden. Die erfolgreiche Umsetzung dieses Angriffs erfordert jedoch, dass das besagte SSL-Modul sowie die Funktion FakeBasicAuth aktiv ist und das Client-Zertifikat von einer Trusted CA (Certificate Authority) stammt. Es wurde die aktualisierte Version 2.8.18 von mod\_ssl für Apache 1.3.x herausgegeben. Für Apache 2.x steht ein Fix im CVS-Tree zur Verfügung. Die jeweiligen Linux-Distributoren werden voraussichtlich in den kommenden Tagen mit Patches nachziehen. Als Workaround wird empfohlen unerwünschten

SSL-Verkehr mittels Firewalling zu limitieren.

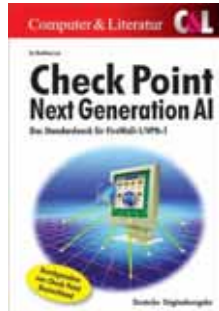
#### Expertenmeinung:

Glücklicherweise müssen verschiedene Voraussetzungen erfüllt sein, damit die Schwachstelle erfolgreich ausgenutzt werden kann. Dies soll jedoch nicht über die potentielle Gefahr der Schwachstelle hinwegtäuschen. Zur Zeit sind noch keine Details zur Schwachstelle oder ein Exploit bekannt. Die hohe Verbreitung von Apache-Lösungen wird jedoch das seinige tun, damit in den kommenden Tagen entsprechende Tools entwickelt und Angriffe umgesetzt werden. Es gilt deshalb so schnell wie möglich Gegenmassnahmen anzustreben.

## 4. Interview

### 4.1 Interview mit Matthias Leu – Autor des Buches „Check Point Next Generation AI – Das Standardwerk für FireWall-1/VPN-1“

scip AG: Hallo Matthias, schön, dass Du Dir die Zeit für dieses Interview nimmst. Ich möchte Dir zur neuen und erweiterten Auflage Deines Buches "Check Point Next Generation AI - Das Standardwerk für FireWall-1/VPN-1" gratulieren. Die Neuauflage ist noch dicker als die Erstausgabe. Wie lange hast Du an dem Buch geschrieben?



Matthias Leu: Erstmal danke für Dein Lob. Ja, das aktuelle Buch ist dicker, wobei einige Teile, die noch mit hineinsollten, dann doch im Internet veröffentlicht wurden. Kein Wunder eigentlich, weil mit NG AI hat sich einiges getan und die Funktionalität stark zugenommen, vor allem gegenüber Version 4.1. Natürlich weiss ich auch, was ich nicht bis in die volle Tiefe behandelt habe. Insofern wollte ich als Untertitel eigentlich den Satz "Eine Einführung". Aber das geht natürlich nicht bei so vielen Seiten...

Das Buch habe ich neben der Arbeit geschrieben. Das musste so sein, weil ich in den letzten Jahren eine Firma aufgebaut habe. Und so wurden es dann ungefähr anderthalb Jahre "nebenbei" am Schreibtisch.

#### Wie bist Du auf die Idee gekommen, ein Buch über CheckPoint Firewalls zu schreiben?

Ungefähr Weihnachten 1999 hatte ich das erste Buch über diese Firewall in der Hand. Natürlich auf englisch. Und von Kunden hatte ich immer wieder die Frage, ob es hierzu nicht auch Literatur auf Deutsch gibt. Nein, die gab es damals noch nicht. Also meinte ich, dass ich hierzu ein Buch schreiben könnte, wobei es nicht nur einfach eine Bedienungsanleitung sein sollte, sondern viele Tipps und Tricks aus der Praxis gibt. Und die wollte ich reinbringen, zumal ich seit Version 1.02 mit der Check Point FireWall-1 intensiv arbeite.

#### Handelte es sich dabei um eine Auftragsarbeit, die Dir durch den Vertrag zugeteilt wurde, oder hast Du die Mühe aus

scip monthly Security Summary  
Marc Ruef & Simon Zumstein  
scip\_mss-19\_06\_2004-1.doc

#### freien Stücken auf Dich genommen und erst danach potentielle Verläge angeschrieben?

Zum Computer- & Literaturverlag hatte ich schon Kontakte, weil hier im Februar 1997 mein erstes Buch erschienen ist. Anfang 2000, nachdem ich ein Konzept gemacht hatte, habe ich beim Verlag angefragt. Schliesslich kam die Zusage, und auch das Eingeständnis, dass ich mich nicht auf einen festen Abgabetermin festlegen möchte oder kann. Auch das erste Buch über die Check Point FireWall-1 habe ich in meiner Freizeit geschrieben, und nach ungefähr zwei Jahren war es dann im Handel. Dem Verlag bin ich vor allem auch für seine Geduld mit mir sehr dankbar.

#### Die erste Auflage des Buches ist Ende 2001 erschienen. Die zweite ist Ende 2003 auf den Markt gekommen. Dies ist keine schlechte Leistung für ein technisches Buch in dieser Preisklasse. Ist schon eine neue Auflage geplant?

Seit Ende 1999 bzw. Anfang 2000 war ich in der Freizeit eigentlich (fast) immer am Schreibtisch - und bin mit meiner Traumfrau verheiratet. Nein, eine neue Version habe ich noch nicht angefangen. Vier Sommer habe ich mehr oder weniger am Schreibtisch verbracht, da brauche ich auch mal eine Pause. Und Check Point ist so nett, dass sich seit Erscheinen des aktuellen Buchs nicht soo viel getan hat. Wenn eine vollständig neue Version herauskommen würde, käme ich ins Überlegen, im Herbst wieder anzufangen...

#### Gab es beim Ausarbeiten des Buchs eine Zusammenarbeit mit CheckPoint? Falls ja, wie sah eine solche aus? Haben sie Dir vorgeschrieben, über was Du wie zu schreiben hattest? Sahen sie Dich als eher Verbündeten oder unliebsamen "Schnüffler"?

Also hier muss ich Check Point Deutschland erstmal herzlich für die Zusammenarbeit danken. Nein, sie haben mir nicht vorgeschrieben, was ich schreiben soll oder darf und ich bin auch dort nicht angestellt. Es hat sehr viel gebracht, hier Ansprechpartner zu haben, um Fragen zu stellen und mir das eine oder andere nochmal genau erklären zu lassen. Kritische Stellen wurden nicht "zensiert", sondern eher ausdiskutiert. Es war also kein "Meinungsaustausch", nach dem ich dann mit einer anderen Meinung wieder heimkam.

Als ich mit dem ersten Buch über die Check

Point anfang, meinte ich genug zu wissen, um es zu schreiben. Aber, wenn man dann richtig "abgetaucht" ist und die Testumgebung "glüht", kommen nach und nach immer mehr Fragen - und da hat der direkte Kontakt zu Check Point wirklich viel gebracht. Und, ich konnte dann auch sicher sein, dass später keine grundsätzlich falschen Dinge zu lesen sind.

**Es gibt mittlerweile eine ganze Reihe von Büchern zu den Themen Computersicherheit und Firewalling. Hast Du Kontakt mit Autoren vergleichbarer Werke (z.B. Firewall-Systeme von Dr. Norbert Pohlmann) und wie siehst Du den Vergleich Deines Buches mit anderen?**

Ja, die Anzahl der Bücher über Sicherheit, Firewalls und verwandte Themen wird immer mehr. Natürlich kenne ich auch andere Autoren. Der Vergleich eines eigenen Buches mit anderen ist nicht ganz leicht. Trotzdem versuche ich es mal. Allgemeine Bücher über Netzwerksicherheit und anderen Gebieten geben oft einen guten Überblick zum Thema, ohne zu tief in Details zu gehen. Das ist für Leute, die neu in das Gebiet kommen, genau richtig. Dann gibt es noch wirkliche Spezialbücher wie z.B. die "Kurzanleitung" zu Sendmail. Die sind dann so speziell, dass sie dem Experten eigentlich in allen Fragen weiterhelfen, der normale Leser ohne Vorwissen aber nach den ersten Seiten fast nichts mehr versteht.

Mit meinem Buch habe ich versucht, die Bedienung der Check Point FireWall-1 zu erklären. Dabei war und ist mir sehr wichtig, dass die Administratoren "wissen, was sie tun". Daher die ersten vier Kapitel mit den Grundlagen. Die braucht ein erfahrener Administrator nicht, klar. Aber ohne diese Kapitel bestünde die Gefahr, dass der unerfahrene Leser zwar lernt, wo er bei dieser Firewall klicken muss - und dann nicht weiss, was überhaupt eine IP-Adresse ist. Das Buch sehe ich als Mittelding zwischen einem Nachschlagewerk und einem Buch, mit dem sich die Bedienung erlernen lässt. Auch wenn es über 1'000 Seiten hat, wurden einige Dinge nur gestreift und nicht ausführlich behandelt. Der Grund hierfür ist einerseits der Platz, andererseits gibt es einige Konfigurationen, die nur sehr selten eingesetzt werden. Trotzdem glaube ich, die wichtigsten Punkte angesprochen zu haben.

**Du bist nun auch schon einige Jahre im IT-Business tätig. Mir gegenüber hast Du einmal erwähnt, dass Du die CheckPoint-Lösung seit den ersten Versionen kennst. Was hast Du für ein Gefühl, wie haben sich die CheckPoint-Firewalls entwickelt, welche Marktposition**

**hat das Produkt und in welche Richtung wird es weiterhin gehen?**

Der letzte Teil ist eher schwierig zu beantworten, ehrlich. Wer hätte bei Version 3.0 gedacht, wie NG AI R55 aussieht? Die ersten Versionen waren richtig gut und einfach zu bedienen, auch ohne Lesen des Handbuchs. Neben der eingesetzten Technologie war, glaube ich, dies ein Grund, warum sich diese Firewall so weit durchgesetzt hat.

Jetzt habe ich hier keine genauen Zahlen, aber diese Firewall ist schon sehr weit verbreitet und kommt bei sehr vielen Unternehmen unterschiedlichster Grösse zum Einsatz. Da zeigt sich die Flexibilität und Skalierbarkeit dieser Firewall. Inzwischen ist die Bedienung nicht mehr so ganz einfach, wobei hier der Grund nicht das GUI, sondern die inzwischen erreichte Komplexität ist. Genau die aber möchte der Markt scheinbar, insofern ist dies nicht als Nachteil zu sehen. War bei den ersten Versionen noch eine Bedienung ohne Blick ins Manual möglich, sollte der Administrator von heute doch einen Kurs drüber besuchen. Danach ist vielen auch das heutige GUI mit all seinen Optionen übersichtlich.

Wo es hinget, weiss ich nicht genau. Ich schätze aber, dass es weiter zum wirklich zentralen Sicherheitsmanagement gehen wird. Das hat Check Point bereits lange, aber vielleicht kommen früher oder später noch weitere Funktionen dazu. Die zentrale Verwaltung hat den Vorteil, dass ein Administrator nur mit einem GUI arbeitet und daher die Gefahr, dass etwas vergessen wird, niedriger ist. Insgesamt wird dadurch die Sicherheit also erhöht.

**Woran sollte Deiner Meinung CheckPoint am ehesten an ihrer Firewall feilen? In welchem Bereich ist das Produkt am schwächsten?**

Wenn die Frage vor zwei Jahren gekommen wäre, fiel die Antwort leicht. Check Point hat Next Generation neu herausgebracht und da war doch die eine oder andere "Kinderkrankheit" dabei. Seit "Next Generation with Application Intelligence" sind diese grösstenteils behoben - und auch die Geschwindigkeit zur Einführung neuer Features hält sich momentan in Grenzen. Jetzt scheint Check Point eher an der Qualität zu feilen, und das macht sich inzwischen bemerkbar.

Direkte Schwächen sehe ich im Moment nicht. Kaum eine andere Firewall ist so flexibel und individuell zu konfigurieren (und lizenzieren). Von den kleinen bis zu den grössten Unternehmen

kann diese Firewall eingesetzt werden, bei gleichem, zentralen Management. Gut, wenn ich etwas "finden" muss - bei den Zertifikaten, wie sie bei der Verschlüsselung eingesetzt werden, könnte noch was verbessert werden. Manchmal ist's hier ein wenig eigen.

Einige bemängeln bei Check Point, dass sie eine "unsichere Firewall" ist, weil Hotfixes herausgegeben werden, die kritische Probleme beheben. Aufgrund der Komplexität heutiger Firewalls kann es aber passieren, dass unter gewissen Bedingungen auch sicherheitsrelevante Fehler erkannt werden. Hier ist Check Point aber meist schnell mit der Veröffentlichung von Verbesserungen. Diese Vorgehensweise finde ich besser als die Behauptung, dass eine Firewall von Haus aus sicher ist und immer sicher sein wird.

### **Und was würdest Du bei der Entwicklung einer Firewall grundsätzlich anders machen?**

Den Preis? (*grinst*) Im Ernst, diese Firewall ist meines Erachtens sehr gut, flexibel, bedienbar, ausbaubar... Insofern würde ich nichts Grundsätzliches anders machen. Andererseits sollten, das habe ich mal vor vielen Jahren gelernt, Sicherheitsprodukte möglichst einfach sein. Das ist die FireWall-1 nun wirklich nicht, eher megakomplex. Aber das sind wohl die Anforderungen des Marktes, und der bestimmt letztendlich, welche Features eine Firewall bieten soll oder muss.

### **Was macht für Dich ein gutes Firewall-Produkt aus?**

Eine gute Firewall zeichnet sich meines Erachtens dadurch aus, dass sie so flexibel ist, dass sie den Anforderungen des Unternehmers wirklich entspricht, ohne wenn und aber. Dass eine Firewall wirklich die notwendige Sicherheit bietet, setze ich einfach mal voraus. Neben der Flexibilität finde ich die Funktionalität wichtig. Wenn die Firewall als zentrales Gateway für die Sicherheit eingesetzt wird, sollte sie Sachen wie VPN und Authentisierung können. Viele Unternehmen wünschen ausserdem die Möglichkeit zum Accounting, Bandbreitenmanagement oder auch die Option, die Firewall von speziellen Anbietern managen zu lassen.

Die Sicherheit hatte ich schon angesprochen. Für mich gehört zwingend dazu, dass die Firewalls auch in einer komplexeren Umgebung noch zu managen sind und vor allem der Administrator die Übersicht behält. Oft ist dies

das A und O für die Sicherheit. Check Point ist hier eine Art Vorreiter gewesen und hat das Management von Haus aus zentral. Wenn ich das mit anderen Anbietern vergleiche... Anders gesagt: Nicht bei allen Anbietern von Firewalls ist ein zentrales und übersichtliches Management vorhanden.

### **Die Meinungen zu Personal Firewalls (PF) sind gespalten. Auf der einen Seite sind Leute, die derlei Lösungen als grösstes Übel des Internetzeitalters sehen, da sie falsche Sicherheit versprechen. Andere wiederum halten die zusätzlichen Schutzmassnahmen für hilfreich und in der heutigen Zeit unabdingbar. Wie stehst Du Produkten wie ZoneAlarm oder BlackICE PC Protection gegenüber?**

Personal Firewalls verteufle ich nicht, wenn der Benutzer mit ihnen richtig umgeht. Sicherlich hat der Benutzer nur eine (gefährliche) Scheinsicherheit, wenn er vor zwei Jahren mal eine Personal Firewall mit den Default-Einstellungen installiert und sich nie wieder drum gekümmert hat. Aber ich kenne auch Benutzer, die ihre Personal Firewall sorgfältig konfiguriert haben und immer auf dem aktuellen Stand der Technik halten. Dann ist so eine Software wirklich gut für den Benutzer, der sich mit seiner ISDN- oder DSL-Anbindung nicht hinter der Firewall seiner Firma verstecken kann. Eigentlich sollten alle Benutzer eine aktuelle Personal Firewall in Kombination mit einem guten Virenschutz einsetzen. Es ist doch zum Teil erschreckend, wie leicht Recher in den Einwahlbereichen der Provider angreifbar sind.

### **Intrusion Prevention-Systeme (IPS) sind immer mehr im Kommen. Durch das grundlegende Einschränken der Möglichkeiten eines Systems sollen klassische Angriffsformen (z.B. Pufferüberlauf-Schwachstellen) verhindert werden. Denkst Du, dass diese Technik heutige Firewalls überflüssig machen und die IT-Security revolutionieren werden?**

IPS sehe ich als eine Weiterentwicklung von Intrusion Detection Systemen, die ja eigentlich eine reine Alarmanlage sind. Und dann kommt die Frage an den Administrator eines IDS, was passiert, wenn nachts um drei ein Alarm kommt. Mit Hilfe von IPS lassen sich einige Angriffsformen erkennen und verhindern. Vor allem im internen Netzwerk können solche IPS die Sicherheit erhöhen, indem sie z.B. Angriffe von Würmern erkennen und die befallenen Systeme ggf. gleich isolieren. Allerdings glaube

ich nicht, dass IPS Firewalls ersetzen werden. Eine Firewall sehe ich als Pfortner, der gewisse (harmlose) Pakete durchlässt und andere eben nicht. Das IPS entdeckt Unregelmäßigkeiten und verhindert diese. Zwar geht die Entwicklung bei Firewalls zum Teil dahin, dass auch ein Angriff wie z.B. ein potenzieller Pufferüberlauf erkannt und automatisch gesperrt wird. Aber ich glaube, es wird (noch) keine gravierenden Änderungen in der IT-Security geben, vielmehr ein sinnvolles, sich gegenseitig ergänzendes Miteinander von Firewalls und IPS.

**Die letzten Monaten hatte Dein Unternehmen AeraSec mit Advisories zum Thema Denial of Service gegen diverse Antiviren-Lösungen für Aufsehen gesorgt. Längerfristiger Gewinner der Publikation sind die Kunden, die mit einer Verbesserung ihrer Produkte rechnen können. Welche Informations-Politik scheint für Dich im Bereich der Computersicherheit angemessen? Müssen die Leute schnellstmöglich informiert werden oder kann Sicherheit nur durch Geheimhaltung "gefährlicher Informationen" erfolgreich umgesetzt werden?**

Vorweg möchte ich erst einmal feststellen, dass es weder eine fehlerfreie Software gibt, noch die ab und zu zitierte Sicherheit von 100 %. Die Hersteller von Software wissen auch, dass in den von ihnen vertriebenen Produkten Fehler sein können, die sie noch nicht entdeckt haben. Bei sicherheitskritischen Lücken sollte auf jeden Fall zuerst der Hersteller davon erfahren, damit er eine Chance hat, den Fehler möglichst zügig zu verbessern. Wenn er es allerdings nicht nötig hat, auf einen kritischen Fehler zu reagieren, dann sollte auch ohne die Veröffentlichung eines Patches auf den entsprechenden Seiten und Listen im Internet auf den Fehler hingewiesen werden - möglichst auch mit der Anleitung zu einem Workaround, der die Konsequenzen des Fehlers möglichst verhindert.

Meine Erfahrung ist, dass sich die meisten Hersteller bei der Meldung eines Fehlers sehr kooperativ verhalten und auch relativ schnell einen Patch herausgeben. Insofern wäre es fast unfair, erst einen Exploit zu veröffentlichen und dann den Hersteller darauf hinzuweisen.

**Und wie stehst Du dem Patchday-Prinzip von Microsoft gegenüber?**

Diese Sache sehe ich eher zweispältig. Hotfixes sollten einerseits möglichst zügig erscheinen, damit die Lücken geschlossen werden können. Andererseits waren gewissenhafte

Administratoren von Microsoft Windows bisher wirklich nicht zu beneiden. Sie sind ja mit dem Test und der Installation von Hotfixes ja bald nicht mehr nachgekommen. Insofern ist das Patchday-Prinzip gut für die Administratoren - aber nicht unbedingt gut für die Sicherheit der Systeme selbst. Und einige Lücken werden schon vor der Veröffentlichung des Patches im Internet diskutiert. Das kann zur Folge haben, dass gewisse Insider möglicherweise die Server schädigen können, ohne dass der Administrator eine Idee hat, dass sein Server unsicher sein könnte. Also, das Ganze sehe ich wirklich mit einem lachenden und einem weinenden Auge.

**Die IT-Branche hat nach dem Boom in den Jahren 2000 und 2001 enorme Einbussen verkraften müssen. Der Markt scheint sich aber langsam wieder zu erholen. Wie hat Dein Unternehmen diese Krise erlebt und welche Prognosen stellst Du für die kommenden Jahre?**

Die Zeiten der Internet-Blase sind zum Glück vorbei. Es war ja nicht wirklich natürlich, dass ein kleines Unternehmen mit einer guten Idee besser bewertet wurde als ein seit Jahrzehnten erfolgreich produzierendes Unternehmen. Die AEARsec wurde Mitte 2000 gegründet. Da könnte man sagen, dass hiermit die Krise begann (*lacht*). Auch heute ist es noch nicht einfach, sich weiter am Markt zu platzieren und neue Projekte zu akquirieren. Die Unternehmen sparen noch immer sehr und es wird wirklich nur das nötigste investiert. So sind die Bereiche Weiterbildung und Einführung neuer Systeme noch immer sehr gebremst. Aber ich bin optimistisch, dass es mit den Jahren wieder besser wird.

Unser Unternehmen hat die Krise so erlebt, dass von Kunden und Interessenten viele Dinge in die Zukunft verlagert wurden. Wir haben bisher die Krise gemeistert, weil wir Qualität liefern und einen hohen Wert auf eine langfristige Kundenbindung legen. Auch ist der Wachstum unseres Unternehmens eher vorsichtig und konservativ.

Die Zukunft sehe ich nicht so, wie die Neunziger Jahre ausgeklungen sind. Vielmehr schätze ich, dass der Markt eher langsam wieder besser wird und die Unternehmen, die die Krise überstehen, langfristig ein gesundes Wachstum zeigen werden. Die Zeiten, in denen man im Alter von 20 seine ersten 10 Millionen verdient hatte, sind vorbei.

**Noch eine in solchen Gesprächen eher untypische Frage: Wenn Du auf eine einsame**

**Insel gehen müsstest, was würdest Du am liebsten mitnehmen oder was würdest Du vermissen?**

Gute Frage, vor allem weil Du nicht eingeschränkt hast, wie viel ich mitnehmen kann und ob auf der Insel eine Satellitenanbindung an das Internet ist (*lacht*).

Mitnehmen würde ich auf jeden Fall meine Frau, und wenn ich ehrlich bin, wären Dinge wie Handy, Internet oder CD-Sammlung gar nicht so notwendig. Insofern kann ich nur verweisen auf Seite 13 im aktuellen Buch (*lacht*).

**Ich möchte mich für diesen unterhaltsamen und interessanten Dialog bedanken und wünsche Dir weiterhin viel Glück.**

**Ich danke Dir auch sehr herzlich für Deine Zeit und wünsche auch Dir alles Gute für die Zukunft!**

## 5. Kreuzworträtsel

|   |                                       |  |  |  |   |  |   |                            |   |                                      |                            |                               |
|---|---------------------------------------|--|--|--|---|--|---|----------------------------|---|--------------------------------------|----------------------------|-------------------------------|
| Mail-Teil welcher Informationen enthält                   |                                       |  | Überfluten eines Dienstes                      |  | DOS: Vergleicht den Inhalt von Dateien    | Emergency-... (scip AG)                                  |   | Back Office                |   | Objekt orientierte Programmierung    | Wonach sucht WLAN reiter   |                               |
| Distributed Denial of Service                             |                                       |  | Linux: Kopiert Dateien                         |  |   | Prozessoren in Apple's                                   |   |                            |   |                                      |                            |                               |
|   |                                       |  |  |  | Soll den Data Encryption Standard ablösen |  |   | HW-Grundlage für Palladium |   |                                      | Künstliche Intelligenz     |                               |
|   |                                       |  |  |  |   | Council of European National Top Level Domain Registries | Top-Level Domain von Schweden                             |                            |   | Virtual Private Network              |                            |                               |
| Entwickler von nmap                                       | Begründer der Relativitätstheorie     |  | Analog-Digital-Wandler                         |  |   |  | ... beginnt (Schach)                                      |                            |   |                                      |                            | scip monthly Security Summary |
| Hersteller von Solaris                                    |                                       |  |  |  |   |  |   | Basic Input Output System  |   |                                      |                            |                               |
|   |                                       |  |  |  | Data Encryption Standard                  | Internet Protocol  | Privat personen TLD                                       |                            |   | Protokoll für Fehler und Information |                            |                               |
| Klassischer UNIX-Texteditor                               | Abk.: Intrusion Detection-System      |  |  |  |   | Speicherresidentes Programm                              |   |                            | Forum of Incident Response and Security Teams |                                      |                            |                               |
|   |                                       |  | Krypto-graphische Weiterentwicklung von Telnet |  |   | Lachend auf dem Boden wälzen                             |   |                            |   |                                      | Hersteller von Real Secure |                               |
| Von IIST vorgeschlagener Standard für Digitale Signaturen |                                       |  |  |  | Protokoll für das Übertragen von Daten    |  | Zeichensatz, der für japanische Tastaturen verwendet wird |                            |   |                                      |                            |                               |
|   |                                       |  |  |  | Was schrieb Robert Tappan Morris          |  |   | Unix: TEXT-Datei anzeigen  | Port scanner                                  |                                      |                            |                               |
| Cross Site Scripting                                      | Verschlüsselungs-Mechanismus für HTTP |  |  |  | Dateisystem von Windows NT und 2000       | Gezielt informiert (scip AG)                             | Aho, Weinberger, Kemighan                                 |                            |   |                                      |                            |                               |
|   |                                       |  | UNIX-Kommando equivalent zu dir unter DOS      |  |   | Gleitkomma-Prozessor                                     |   |                            |   |                                      |                            |                               |
| Javascript  |                                       |  |  |  |   |  | Briefqualität   |                            |   |                                      |                            |                               |

### Wettbewerb

Mailen Sie uns das erarbeitete Schlüsselwort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten. Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.07.2004**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

Gewinnen Sie eins von drei Exemplaren des Security Fachbuches: **Hacking Intern** (ISBN 381582284X)



## 6. Literaturverzeichnis

scip AG, 2003, scip monthly Security Summary, Ausgabe 19. September 2003, Neuromancer-Trilogie, <http://www.scip.ch>

Wikipedia, Begriffserklärung Science-Fiction, <http://de.wikipedia.org/wiki/Science-Fiction>

## 7. 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).

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)