

## Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Statistiken Verletzbarkeiten
5. Fachartikel
6. Kreuzworträtsel
7. Literaturverzeichnis
8. Impressum

### 1. Editorial

#### Trügerische Sicherheit?

Die Wassertropfen prasseln gegen die Fensterscheiben unserer Büroräumlichkeiten im Technopark Zürich. Ein guter Tag um zu arbeiten. Die Anzahl der zu erledigenden Pendenzen ist, wie in letzter Zeit immer, im zweistelligen Zahlenbereich. Darunter sind sowohl kundenbezogene Arbeiten wie Offerten, Nachforschungen, Statistiken, Grobkonzepte, Evaluationen, Auditberichte, Hardening Guides etc. als auch Vorbereitungen für die regelmässig durchgeführten IT-Security Diskussionsrunden unter Fachkräften.

Ich bin wiedereinmal früh im Büro. In dieser Zeit sind weder Kunden noch Mitarbeiter zugegen, meine ideale Arbeitszeit...

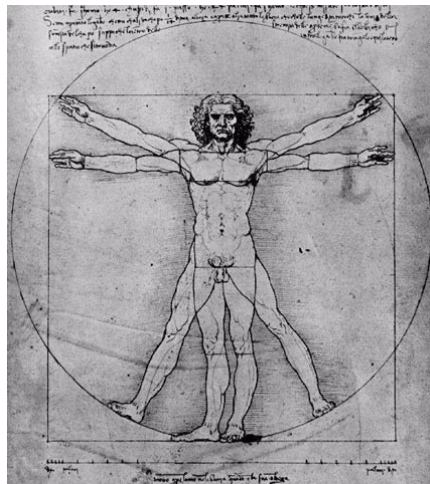
Unverhofft klingelt das Telefon. Um 06:45 Uhr? Das Display zeigt \*XXX\*, eine unterdrückte Telefonnummer. Kann eigentlich nur ein Kunde sein. Entweder falsche Nummer gewählt oder es ist ausserordentlich dringend. Gespannt nehme ich den Telefonhörer in die Hand und melde mich

wie gewohnt: „scip AG Zumstein...“

Am anderen Ende der Leitung meldet sich der Security Officer eines Kunden. – ich erinnere mich, vor zwei Monaten das erste gemeinsame Projekt – Der Security Officer berichtet mir, dass sie soeben Anzeichen eines Incidents bemerkt haben. Gerne würde er uns damit betreuen den Vorfall aufzuklären und zu rekonstruieren, falls wir Ressourcen entbehren können. Die Aufgabe ist sehr zeitkritisch. Nach einer kurzen Konsultation der Abgabetermine der bestehenden Projekte und dem derzeitigen Status dieser, gab ich gerne unsere Zusage.

„Vielen Dank für Ihre Anfrage. Gerne übernehmen wir das Mandat. Erzählen Sie mir die bekannten Informationen...“

Forensik Projekte sind immer sehr interessante Vorhaben. Sisyphus Arbeit welche die gesamte Konzentration fordert. Die Anstrengungen werden dafür mit ausserordentlichen Erfahrungen versüsst. Zum Glück nicht unser erstes Forensik Projekt, wir haben bereits einen Prozess. Das Vorgehen, die durchzuführenen Arbeiten als auch die schlussendlich erwarteten Aussagen und zu übergebenden Informationen sind uns sehr wohl bekannt.



Vier Stunden nach dem Initial-Telefonat sassen wir bereits beim Kunden. Wir liessen uns die Sachlage erörtern und erarbeiteten mit dem Kunden einen Vorgehensplan inklusive Personenliste. Die Grosszahl der bisher durch uns investigierten Incidents haben ihren Startpunkt im internen Netzwerk - so auch dieser.

Der Auftrag wird nicht leicht. Als erstes haben wir einige, für forensische Arbeiten, hinderliche Unschönheiten vernommen (keine konzipierte Loglevelinstellung auf den Systemen, flache Topologie, ein löchriges Rollenkonzept, schwache Authentisierung etc.) desweiteren wird bereits eine Person verdächtigt. Hier ist grosses Fingerspitzengefühl bei den Interviews gefragt. Bei solchen Besprechungen bieten wir immer

einen Mitarbeiter der HR-Abteilung des Kunden mit auf. Wir sind ja auch nur Menschen. Um das Ganze etwas zu verkomplizieren sind die betroffenen Systeme physikalisch in unterschiedlichen DataCenters, die Arbeitsplätze der zu interviewenden Mitarbeiter sind über den Erdball verteilt und diese Personen sprechen die heimische Sprache. Glücklicherweise waren alle der englischen Sprache mächtig.

Ich möchte hier nun nicht näher darauf eingehen, was wir genau umgesetzt haben respektive das Ergebnis des interessanten Projektes erörtern. Dazu reicht weder der Platz noch möchte ich solche Details aus Kundenprojekten, trotz Anonymisierung, hier wiedergeben.

Zusammenfassend kann eine alte Security Weisheit festgehalten werden. Grosse Unternehmungen (egal ob Banken, Industrie, Chemie etc.) sind gezwungen eine immense Information Technologie Infrastruktur zu betreiben. Diese Umgebung wird nicht von Beginn weg für zehntausende von Benutzer oder für TerraBytes von Daten dimensioniert. Die notwendigen Erweiterungen zur Aufrechterhaltung der Verfügbarkeit (z.B. Benutzerverwaltung), die Optimierungen anhand neuer Technologien (z.B. SAP) und die zusätzlichen angebotenen Dienste (z.B. Blackberry) werden teilweise unter Zeitdruck und ohne ausgedehnte Konzeptionsphase in den Betrieb übernommen. Die Information Security ist dabei stets Gesprächsthema und wird als Traktandum aufgelistet. Solange jedoch die eingesetzten Technologien und Produkte IT-Security Grundlagen wie mehrere Administratoren etc. nur teilweise oder garnicht unterstützen oder die verwendeten Applikationen nicht ab der Stange InputValidierung etc. umsetzen sind bereits eine Vielzahl an Schlupflöchern auf technischer Ebene vorhanden. Die Schwere dieser Schwachstellen wird durch den Mangel an internen Ressourcen verschärf. Ganz abgesehen von zielgerichteten Social Engineering Angriffen.

Simon Zumstein <sizu-at-scip.ch>  
Geschäftsleiter  
Zürich, 18. Juli 2005

## 2. scip AG Informationen

### 2.1.1 Aufruf IT-Hideouts Lokationen



Wir bedanken uns für die interessanten Zuschriften bezüglich IT-Hideouts Lokationen. Gerne werden wir diese in den kommenden Ausgaben

des scip monthly Security Summary integrieren.

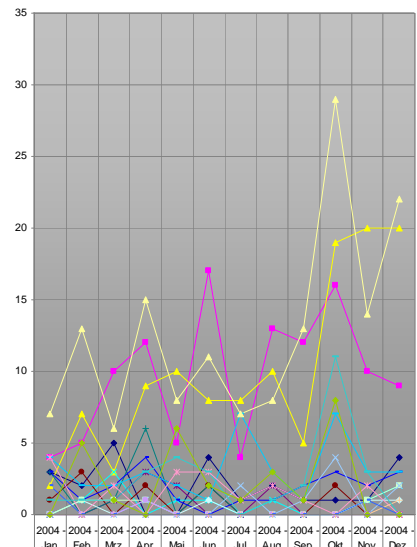
Natürlich freuen wir uns auf künftige über Vorschläge. Falls Sie einen Vorschlag haben und diesen gerne publiziert sehen würden, so melden Sie sich bitte bei Simon Zumstein unter der Telefonnummer +41 44 445 1818 oder per Mail an <mailto:sizu@scip.ch>. Wir freuen uns schon jetzt auf Ihre Erfahrungen.

### 2.1.2 Statistiken Verletzbarkeiten

Ab dieser Ausgabe des scip monthly Security Summary haben wir die neue Rubrik Statistiken Verletzbarkeiten integriert.



Die Statistiken basieren auf unserer deutschsprachigen Verletzbarkeitsdatenbank <http://www.scip.ch/cgi-bin/smss/showadvf.pl>. In dieser CVE [scip AG, 2003a] akkreditierten [scip AG, 2003b] Datenbank tragen wir seit 2003 aktuelle Schwachstellen ein.



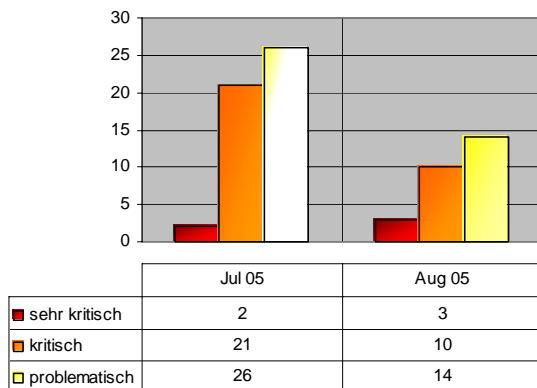
	2004 - Jan	2004 - Feb	2004 - Mrz	2004 - Apr	2004 - Mai	2004 - Jun	2004 - Jul	2004 - Aug	2004 - Sep	2004 - Okt	2004 - Nov	2004 - Dez
Cross Site Scripting (XSS)	3	2	5	0	0	4	1	2	1	1	1	4
Denial of Service (DoS)	4	5	10	12	5	17	4	13	12	16	10	9
Designfehler	2	7	3	9	10	8	8	10	5	19	20	20
Directory Traversal	0	1	3	0	1	1	0	1	0	0	1	2
Eingabeungültigkeit	0	0	1	3	2	0	0	2	0	0	0	0
Fehlende Authentifizierung	1	3	0	2	0	2	0	0	0	0	2	0
Fehlende Verschlüsselung	3	0	1	6	0	2	0	0	0	0	0	0
Fehlerhafte Leserechte	3	1	2	4	1	0	1	1	2	3	2	3
Fehlerhafte Schreibrechte	4	2	2	3	2	1	7	3	1	7	3	3
Format String	0	1	0	0	0	1	0	0	0	0	1	1
Konfigurationsfehler	0	1	1	1	0	0	0	0	0	0	1	2
Pufferüberlauf	7	13	6	15	8	11	7	8	13	29	14	22
Race-Condition	0	0	0	1	0	0	2	0	1	4	0	2
Schwache Authentifizierung	4	0	2	0	3	3	1	2	1	0	2	0
Schwache Verschlüsselung	0	0	0	1	0	0	0	0	0	0	0	0
SQL-Injection	0	0	0	0	0	0	0	0	0	0	0	1
SymLink-Schwachstelle	2	0	0	0	0	0	0	0	0	0	0	1
Umgehungs-Angriff	1	1	1	3	4	3	0	1	2	11	3	0
Unbekannt	0	5	1	0	6	2	1	3	1	8	0	0

Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen. Zögern Sie nicht uns zu kontaktieren.

### 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 Veritas Backup Exec bis 8.6 für Windows erweiterte Leserechte
- 3.2 Novell eDirectory bis 8.7.3 IR4 für Windows iMonitor Pufferüberlauf
- 3.3 Microsoft Internet Explorer bis 6.0 ActiveX COM-Objekte Pufferüberlauf
- 3.4 Microsoft Internet Explorer bis 6.0 JPEG-Bilder Pufferüberlauf
- 3.5 Microsoft Windows 2000 bis Server 2003 Print Spooler Dienst Pufferüberlauf
- 3.6 Microsoft Windows 2000, XP und Server 2003 Kerberos PKINIT-Transaktionen Pufferüberlauf
- 3.7 Microsoft Windows 2000 bis Server 2003 Plug-and-Play Service Pufferüberlauf
- 3.8 Sun Solaris 7 bis 10 printd erweiterte Schreibrechte
- 3.9 CA BrightStor ARCserve Backup Agenten bis 11.1 lange Anfrage Port tcp/6070 Pufferüberlauf
- 3.10 MySQL Eventum bis 1.6.0 verschiedene Klassen SQL-Injection
- 3.11 Novell eDirectory 8.x Novell Modular Authentication Service bis 2.3.8 fehlerhafte Authentisierung
- 3.12 Cisco IOS 12.x logisches Interface korruptes IPv6-Paket Denial of Service
- 3.13 IBM Lotus Domino 5.0 bis 6.5 Public

Address Book Passwort erweiterte Leserechte

- 3.14 Microsoft Windows 98 bis XP USB-Treiber Pufferüberlauf
- 3.15 Apache bis 2.0.55 mod\_ssl off-by-one Designfehler
- 3.16 SAP R/3 bis 6.40 Patch 11 Internet Graphics Server Directory Traversal

#### 3.1 Veritas Backup Exec bis 8.6 für Windows erweiterte Leserechte

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 12.08.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1699>

Veritas stellt neben dem Cluster Server für die Lastverteilung bzw. Leistungskombinierung ebenfalls eine Backup-Lösung zur Verfügung. Der Hersteller meldet einen nicht näher beschriebenen Fehler von Veritas Backup Exec bis 8.6 für Windows. Ein Angreifer könne durch einen Logikfehler über das Internet beliebige Dateien vom Betriebssystem beziehen. Dazu ist eine Verbindung auf den Service-Port tcp/10000 erforderlich. Es wurde gemeldet, dass bereits ein Exploit für dieses Problem besteht. Der Hersteller hat noch keinen Patch herausgegeben, empfiehlt jedoch das Limitieren der Zugriffe auf diesen Port mittels Firewalling.

#### Expertenmeinung:

Dieses Problem ist ziemlich schwerwiegend, denn die Schwachstelle ist sehr einfach und über das Netzwerk/Internet auszunutzen (Exploits sind verfügbar). Aus diesem Grund sollte man umgehend die Firewall-Einstellungen anpassen und den entsprechende Patch eingespielen.

#### 3.2 Novell eDirectory bis 8.7.3 IR4 für Windows iMonitor Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 12.08.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1697>

Novell eDirectory ist eine bekannte kommerzielle Lösung für Identity Management in grossen Umgebungen. Peter Winter-Smith entdeckte eine Pufferüberlauf-Schwachstelle in der Komponente iMonitor. Ein Angreifer kann in den Versionen bis 8.7.3 IR4 für Windows beliebigen Programmcode ausführen lassen. Es sind keine Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler wurde durch Novell mit einem Patch adressiert.

**Expertenmeinung:**

Da nahezu keine Details zur Schwachstelle bekannt sind, ist die Einschätzung sehr schwierig und zum jetzigen Zeitpunkt nicht möglich. Sollten Ihre Systeme verwundbar sein, sollen Sie schnellstmöglich auf eine aktuelle Software-Version updaten.

### 3.3 Microsoft Internet Explorer bis 6.0 ActiveX COM-Objekte Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 09.08.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1695>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Der Hersteller gibt in seinem Microsoft Security Bulletin MS05-038 (KB896727) gleich drei kritische Schwachstellen in ihrem beliebten Browser bekannt. Eine davon ist in einem Pufferüberlauf bei der Interpretation von COM-Objekten bei ActiveX gegeben. Ein Angreifer kann so eine Denial of Service-Attacke umsetzen oder beliebigen Programmcode ausführen lassen. Ein Exploit ist publiziert. Microsoft hat zu den jüngsten Problemen einen kumulativen Patch herausgegeben, bei dessen Installation unter Umständen Probleme auftreten können (siehe <http://support.microsoft.com/kb/896727>).

**Expertenmeinung:**

Und schon wieder eine ernstzunehmende Schwachstelle in unserem Lieblings-Browser. Machte man früher Witze über Sendmail, weil praktisch jede Woche eine neue Sicherheitslücke bekannt wurde, mausert sich der Internet Explorer langsam zum "buggiest program on planet earth". Wer sich nicht vom König unter den Browsern - der halt doch durch Kompatibilität und Features brilliert - trennen kann, muss damit leben, dass er alle paar Wochen neue Patches installieren muss. Mit dem Auto-Update von Windows 2000 und XP ist das jedoch auch nicht mehr wirklich ein Problem

### 3.4 Microsoft Internet Explorer bis 6.0 JPEG-Bilder Pufferüberlauf

Einstufung: **sehr kritisch**  
Remote: Ja  
Datum: 09.08.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1693>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Der Hersteller gibt in seinem Microsoft Security Bulletin MS05-038 (KB896727) gleich drei kritische Schwachstellen in ihrem beliebten Browser bekannt. Eine davon ist in einem Pufferüberlauf bei der Darstellung von JPEG-Bildern gegeben. Ein Angreifer kann so eine Denial of Service-Attacke umsetzen oder beliebigen Programmcode ausführen lassen. Ein Exploit kursiert im Netz. Microsoft hat zu den jüngsten Problemen einen kumulativen Patch herausgegeben, bei dessen Installation unter Umständen Probleme auftreten können (siehe <http://support.microsoft.com/kb/896727>).

**Expertenmeinung:**

Eine wahrhaftig kritische Schwachstelle, da der Pufferüberlauf nahezu jedes moderne Windows-System betrifft. Die Interpretation von JPEG-Bildern ist üblich, mitunter auch über HTML im Mail-Verkehr. Spammer und Wurm-Entwickler werden wohl in den kommenden Tagen entsprechende Exploits entwickelt haben, um die Schwachstelle für ihre Zwecke auszunutzen zu können - Gleiches Szenario war schon im letzten September (scipID 833) gegeben. Grossflächige Kompromittierungen von Systemen wird die Folge sein. Gegenmassnahmen sind unverzüglich umzusetzen, um verheerende Ausmasse an Schäden wie im Falle des Blaster-Wurms zu verhindern.

### 3.5 Microsoft Windows 2000 bis Server 2003 Print Spooler Dienst Pufferüberlauf

Einstufung: **sehr kritisch**  
Remote: Ja  
Datum: 09.08.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1692>

Microsoft Windows NT 4.0 ist das professionelle Pendant zu Microsoft Windows 9x, das jedoch mittlerweile vielerorts durch den Nachfolger Microsoft Windows 2000 abgelöst wurde. Microsoft Windows XP mit dem Server 2003 wiederum stellt die Weiterentwicklung und eine indirekte Zusammenführung mit der 98er-Reihe dessen dar. Wie der Hersteller in seinem Microsoft Security Bulletin MS05-043 (KB896423) bekannt gibt, existiert eine Pufferüberlauf-Schwachstelle im Print Spooler Dienst (spoolsv.exe). Ein Angreifer, der sich auf diesen verbinden kann, kann so beliebigen Programmcode ausführen oder eine Denial of Service umsetzen lassen. Ein Exploit zur

Schwachstelle ist bereits im Umlauf. Microsoft hat Patches für die betroffenen Windows-Versionen herausgegeben.

**Expertenmeinung:**

Am 12.08.2005 wurde ein erster Exploit publiziert. Es gilt diese sehr kritische Sicherheitslücke (sie betrifft alle professionellen Windows-Systeme und ist auch remote ausnutzbar) ernst zu nehmen. Ein solcher Exploit-Angriff wird sich schnellstens grösster Beliebtheit erfreuen und sich gar als Verbreitungsroutine für Computerwürmer und -viren eignen. Umso wichtiger ist es, dass man schnellstmöglich einen Patch installiert, damit das Zeitfenster eines erfolgreichen Angriffs möglichst gering gehalten werden kann.

### 3.6 Microsoft Windows 2000, XP und Server 2003 Kerberos PKINIT-Transaktionen Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 09.08.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1691>

Microsoft Windows XP mit dem Server 2003 stellt die Weiterentwicklung von Windows 2000 und eine indirekte Zusammenführung mit der 98er-Reihe dessen dar. Wie der Hersteller in seinem Microsoft Security Bulletin MS05-042 (KB899587) bekannt gibt, existiert eine Pufferüberlauf-Schwachstelle in Kerberos. Ein Angreifer kann mittels korrupten PKINIT-Transaktionen beliebigen Programmcode ausführen lassen. Technische Details oder ein Exploit zur Schwachstelle sind bisher nicht bekannt. Microsoft hat Patches für die betroffenen Windows-Versionen herausgegeben.

**Expertenmeinung:**

Die Möglichkeit der Denial of Service-Attacke gegen lässt sich nur schwer in einem konstruktiven Kontext nutzen. Entsprechend ist das Interesse an dieser Möglichkeit eher beschränkt. Ein solcher DoS-Angriff wird eher von Skript Kiddies oder verärgerten Mitarbeitern herbeigeführt werden.

### 3.7 Microsoft Windows 2000 bis Server 2003 Plug-and-Play Service Pufferüberlauf

Einstufung: **sehr kritisch**  
Remote: Ja  
Datum: 09.08.2005  
scip DB: <http://www.scip.ch/cgi->

[bin/smss/showadvf.pl?id=1689](http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1689)

Microsoft Windows NT 4.0 ist das professionelle Pendant zu Microsoft Windows 9x, das jedoch mittlerweile vielerorts durch den Nachfolger Microsoft Windows 2000 abgelöst wurde. Microsoft Windows XP mit dem Server 2003 wiederum stellt die Weiterentwicklung und eine indirekte Zusammenführung mit der 98er-Reihe dessen dar. Wie der Hersteller in seinem Microsoft Security Bulletin MS05-039 (KB899588) bekannt gibt, existiert eine Pufferüberlauf-Schwachstelle im Plug and Play Dienst. Ein Angreifer kann so beliebigen Programmcode ausführen lassen. Um den Angriff umzusetzen ist kein Konto erforderlich. Zwei Exploits zur Schwachstelle wurde am Freitag 12.8.2005 publik gemacht. Microsoft hat Patches für die betroffenen Windows-Versionen herausgegeben.

**Expertenmeinung:**

Am 12.08.2005 wurde ein erster Exploit publiziert. Es gilt diese sehr kritische Sicherheitslücke (sie betrifft alle professionellen Windows-Systeme und ist auch remote ausnutzbar) ernst zu nehmen. Ein solcher Exploit-Angriff wird sich schnellstens grösster Beliebtheit erfreuen und sich gar als Verbreitungsroutine für Computerwürmer und -viren eignen. Umso wichtiger ist es, dass man schnellstmöglich einen Patch installiert, damit das Zeitfenster eines erfolgreichen Angriffs möglichst gering gehalten werden kann.

### 3.8 Sun Solaris 7 bis 10 printd erweiterte Schreibrechte

Einstufung: **kritisch**  
Remote: Ja  
Datum: 09.08.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1685>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. H. D. Morre publizierte eine Schwachstelle im Drucker-Daemon printd von Sun Solaris 7 bis 10. Durch einen nicht näher beschriebenen Fehler, kann ein Angreifer beliebige Dateien auf dem System löschen. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Sun hat Patches für die betroffenen Solaris-Versionen herausgegeben.

**Expertenmeinung:**

Die Möglichkeit der Denial of Service-Attacke gegen lässt sich nur schwer in einem konstruktiven Kontext nutzen. Entsprechend ist das Interesse an dieser Möglichkeit eher

beschränkt. Ein solcher DoS-Angriff wird eher von Skript Kiddies oder verärgerten Mitarbeitern herbeigeführt werden.

### 3.9 CA BrightStor ARCserve Backup Agenten bis 11.1 lange Anfrage Port tcp/6070 Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 03.08.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1679>

BrightStor ARCserve ist eine kommerzielle Backup-Lösung in Netzwerken, die von Computer Associates (CA) aufgekauft wurde. Die Agenten binden sich dabei an einen TCP-Port, um die Backup-Funktionalität im Netzwerk zur Verfügung zu stellen. iDEFENSE publizierte ein anonymes Advisory, das auf eine Pufferüberlauf-Schwachstelle in den CA BrightStor ARCserve Backup Agenten bis 11.1 hinweist. Durch eine Anfrage länger als 3'168 Bytes an den Standardport tcp/6070 kann beliebiger Programmcode ausgeführt werden. Der erste Patch zur Beseitigung der Lücke schloss diese nicht vollständig. CA besserte nach und stellt nun einen neuen Patch zur Verfügung.

#### Expertenmeinung:

Diese Sicherheitslücke ist sehr kritisch, wobei man jedoch von Glück sprechen kann, dass das Problem in den meisten Umgebungen aufgrund von Firewalling nur im gleichen Segment ausnutzbar sein wird. Trotzdem sollte man sich schnellstmöglich bemühen, das eigene System entsprechend abzusichern.

### 3.10 MySQL Eventum bis 1.6.0 verschiedene Klassen SQL-Injection

Einstufung: **kritisch**  
Remote: Ja  
Datum: 01.08.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1676>

SQL ist eine Datenbank. MySQL ist eine SQL-Datenbank für viele verschiedene Betriebssysteme, die der open-source Lizenz unterliegt. Sie hat aufgrund ihrer Geschwindigkeit und Zuverlässigkeit ein sehr hohes Mass an Popularität erreicht. In MySQL Eventum bis 1.6.0 wurden einige Schwachstellen gefunden. Das MySQL-Team publizierte unter anderem eine nicht näher beschriebene SQL-Injection Schwachstelle verschiedener Klassen. Es sind

keine technischen Details oder ein Exploit bekannt. Der Fehler wurde in der jüngsten Version 1.6.0 von MySQL Eventum behoben.

#### Expertenmeinung:

Wahrhaftig, so scheint SQL Injection zur Zeit in Mode zu sein. Durch diese Schwachstelle lassen sich viele aktuelle Web-Anwendungen überlisten, Daten auslesen oder schreiben. Da bei diesem hier beschriebenen Problem bald ein proof-of-concept Exploit folgen könnte, ist damit zu rechnen, dass in den kommenden Wochen eine Vielzahl von Skript-Kiddies die neue Schwachstelle ausprobieren wollen. Entsprechend ist es wichtig, dass der Patch schnell installiert wird.

### 3.11 Novell eDirectory 8.x Novell Modular Authentication Service bis 2.3.8 fehlerhafte Authentisierung

Einstufung: **kritisch**  
Remote: Ja  
Datum: 28.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1672>

Novell eDirectory ist eine bekannte kommerzielle Lösung für Identity Management in grossen Umgebungen. Eine klassische Funktion stellt dabei der Novell Modular Authentication Service (NMAS) zur Verfügung: Durch das Beantworten einer geheimen Frage kann ein Benutzer sein Passwort - falls es vergessen oder verloren wurde - zurücksetzen. Novell gab nun eine aktualisierte Version eben dieser Komponente heraus, das ein Angreifer in den Versionen bis 2.3.8 das Passwort ohne das Beantworten der "Secret Question" zurücksetzen konnte.

#### Expertenmeinung:

Diese Designschwäche wäre sehr einfach zu vermeiden gewesen, wenn spätestens während der Entwicklungs- und Test-Phase eine ausgiebige Überprüfung der Passwort-Funktionalität durchgeführt worden wäre. Leider muss man hier Schlampigkeit der Entwickler nachsagen. Eine solche ist grundsätzlich unakzeptabel, denn dadurch könnte ein beachtlicher wirtschaftlicher oder persönlicher Schaden entstehen. Da das Problem nun bekannt ist, sollte man seine Rechnerkonfiguration überprüfen und gegebenenfalls anpassen, um nicht erwünschte Zugriffe zu verhindern.

### 3.12 Cisco IOS 12.x logisches Interface korruptes IPv6-Paket Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 29.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1670>

Die Firma Cisco hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Internet Operating System (IOS) wird die Firmware von Cisco-Routern genannt. Wie der Hersteller in seinem Dokument 65783 meldet, existiert eine nicht näher beschriebene Denial of Service-Schwachstelle in IOS 12.x. Erhält ein logisches Interface ein korruptes IPv6-Paket, kann das System zum Absturz gebracht werden. Ein Exploit ist bisher nicht bekannt. Cisco hat wie immer Patches für die betroffenen IOS-Versionen bereitgestellt.

#### 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. Es gilt unbedingt und unverzüglich entsprechende Gegenmassnahmen einzuleiten und die herausgegebenen IOS-Updates einzuspielen.

### 3.13 IBM Lotus Domino 5.0 bis 6.5 Public Address Book Passwort erweiterte Leserechte

Einstufung: **kritisch**  
Remote: Ja  
Datum: 28.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1661>

Lotus Notes ist ein System für das Management und die Verarbeitung auch wenig strukturierter Informationen in elektronischer Form für einen heterogenen Anwenderkreis. Dabei ist diese Definition eng an den Begriff "Groupware" geknüpft, Lotus Notes galt (und gilt noch) lange Zeit als die Standard-Groupware-Plattform. Leandro Meiners entdeckte einen schwerwiegenden Designfehler in IBM Lotus Domino 5.0 bis 6.5. Das Public Address Book stellt ein öffentliches Adressbuch für die Nutzen des gleichen Domino-Systems dar. In einem solchen Eintrag wird in einem Hidden-Feld des HTML-Quelltexts das Passwort des angezeigten Benutzers geführt. Mit der Durchsicht des

Quellcodes kann ein Angreifer also ohne weiteres in den Besitz sensibler Benutzerinformationen kommen. IBM wurde über das Problem informiert, empfiehlt jedoch lediglich das Deaktivieren der entsprechenden Herausgabe.

#### Expertenmeinung:

Absolut peinlich, was sich IBM hier geleistet hat. Eine derartige Schwachstelle lädt Angreifer regelrecht ein, mit den einfach zu erhaltenden Benutzerinformationen Schabernack zu treiben. Dass es sich bei diesem Fehler lediglich um Nachlässigkeit eines Entwicklers handelt, wage ich ernsthaft zu bezweifeln.

### 3.14 Microsoft Windows 98 bis XP USB-Treiber Pufferüberlauf

Einstufung: **kritisch**  
Remote: Indirekt  
Datum: 22.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1653>

Microsoft Windows 98 ist die Weiterentwicklung von Microsoft Windows 95, ein kommerzielles Betriebssystem, das von der amerikanischen Firma Microsoft entwickelt und vertrieben wird. Microsoft Windows NT 4.0 ist das professionelle Pendant, das jedoch mittlerweile vielerorts durch den Nachfolger Microsoft Windows 2000 abgelöst wurde. Microsoft Windows XP wiederum stellt die Weiterentwicklung und eine indirekte Zusammenführung mit der 98er-Reihe dessen dar. SPI Dynamics entdeckte einen schwerwiegenden Pufferüberlauf im Umgang mit einigen USB-Geräten. Ein Angreifer mit physikalischem Zugriff zu einem betroffenen Windows-System kann dieses so innert Sekunden kompromittieren. Es sind keine Details oder ein Exploit zur Schwachstelle bekannt. Als Workaround wird empfohlen, die USB-Ports zu deaktivieren und nur vertrauenswürdigen Personen physikalischen Zugriff zu Systemen zu gewähren.

#### Expertenmeinung:

Schwachstellen physikalischer Natur, die man als Sicherheitslücken klassifizieren könnte, sind relativ selten. Die Gefahr bei Pufferüberlauf ist aber durchaus gegeben. Vor allem öffentlich (z.B. Internet-Cafés) oder von einer Gruppe Menschen zugängliche Systeme (z.B. Büro) könnten so mittelfristig ohne direkten Systemzugriff kompromittiert werden. Am besten ist deshalb ein BIOS-Passwort gesetzt und USB-Ports deaktiviert, so dass nicht ohne weiteres Angriffe durchgeführt werden können.

### 3.15 Apache bis 2.0.55 mod\_ssl off-by-one Designfehler

Einstufung: **kritisch**  
Remote: Ja  
Datum: 26.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1652>

Apache ist ein populärer, freier open-source Webserver, der für viele verschiedene Plattformen erhältlich ist. Watchfiren entdeckte einen Designfehler in mod\_ssl bei Apache bis 2.0.55. Es sind keine genauen Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler wurde in der jüngsten Apache-Version behoben.

#### Expertenmeinung:

Ende Juli wurden gleich zwei kritische Sicherheitslücken im Apache Webserver entdeckt. 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 Update auf die aktualisierte Apache Version getan werden sollte.

### 3.16 SAP R/3 bis 6.40 Patch 11 Internet Graphics Server Directory Traversal

Einstufung: **kritisch**  
Remote: Ja  
Datum: 25.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1647>

SAP wurde 1972 von fünf ehemaligen Mitarbeitern der IBM gegründet. Mit NetWeaver soll der zunehmenden Komplexität der SAP-Produkte Rechnung getragen werden. Gegenwärtig bietet die SAP mit dem Produkt SAP NetWeaver, eine Plattform an, mit deren Hilfe unterschiedliche Business-Anwendungen integriert werden können. Wo es vor einigen Jahren nur eine quasi monolithische ERP-Software mit unterschiedlichen Modulen gegeben hat (SAP R/3), gibt es heute eine breite Palette an unterschiedlichen Produkten. Die SAP R/3-Software ist in der SAP eigenen Programmiersprache ABAP programmiert. [[http://de.wikipedia.org/wiki/SAP\\_AG](http://de.wikipedia.org/wiki/SAP_AG)] Martin O'Neal entdeckte ein Directory Traversal-Schwachstelle im SAP R/3 bis 6.40 Patch 11 Internet Graphics Server. Durch das

Heranziehen klassischer Kombinationen ../ können erweiterte Leserechte auf dem System erlangt werden. Es sind keine detaillierten technischen Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler wurde durch die SAP AG mit einem Patch behoben.

#### Expertenmeinung:

Martin O'Neal informierte frühzeitig die SAP AG, um die Handhabung der Schwachstelle zu koordinieren. Die Zusammenarbeit gestaltete sich aber schwierig, denn der Hersteller schlug eine solche gänzlich aus. So wurde behauptet, dass das Problem schon länger bekannt sei. Auf die Frage hin, ob O'Neal Einsicht in die bisher gesammelten Informationen haben könnte, wurde er mit dem Verweis abgespiesen, dass diese Daten lediglich SAP-Kunden zugänglich seien. SAP AG täte gut daran, in solchen Fällen besser zu kooperieren, denn Ignoranz hat schon so manchen Black Hat zu einem Rundumschlag verleitet.

#### 4. Statistiken Verletzbarkeiten

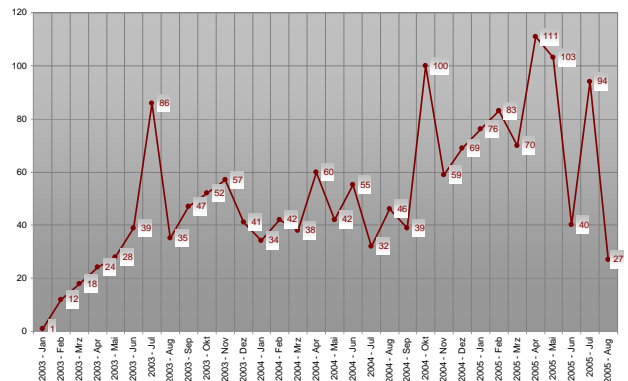
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

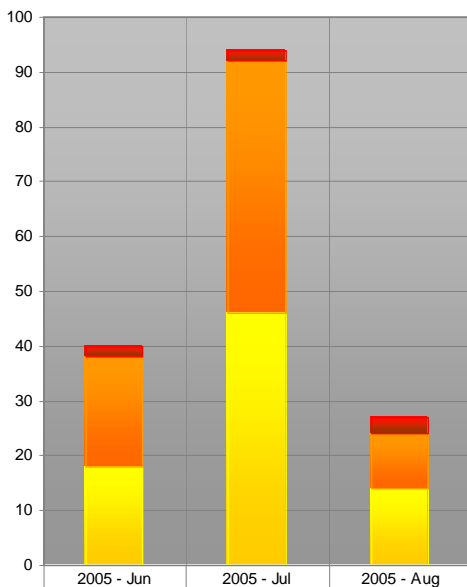
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

Registrierte Schwachstellen by scip AG



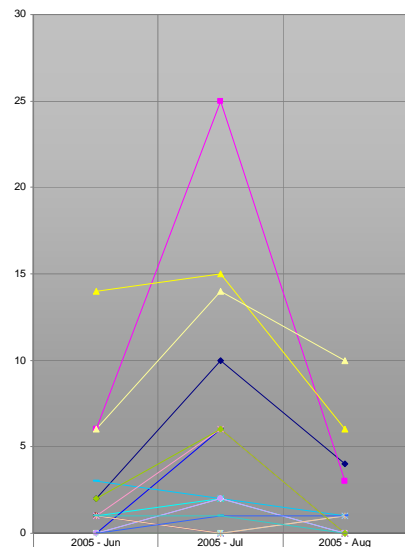
Verlauf der Anzahl Schwachstellen pro Monat

Auswertungsdatum: 18. Aug 2005



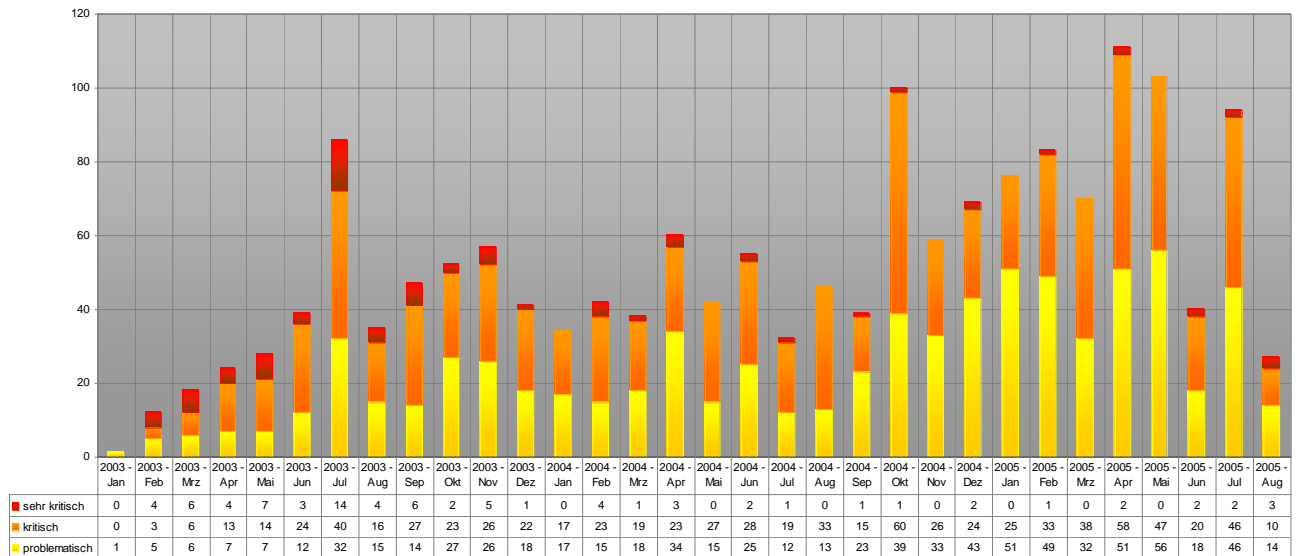
	2005 - Jun	2005 - Jul	2005 - Aug
sehr kritisch	2	2	3
kritisch	20	46	10
problematisch	18	46	14

Verlauf der letzten drei Monate Schwachstelle/Schweregrad

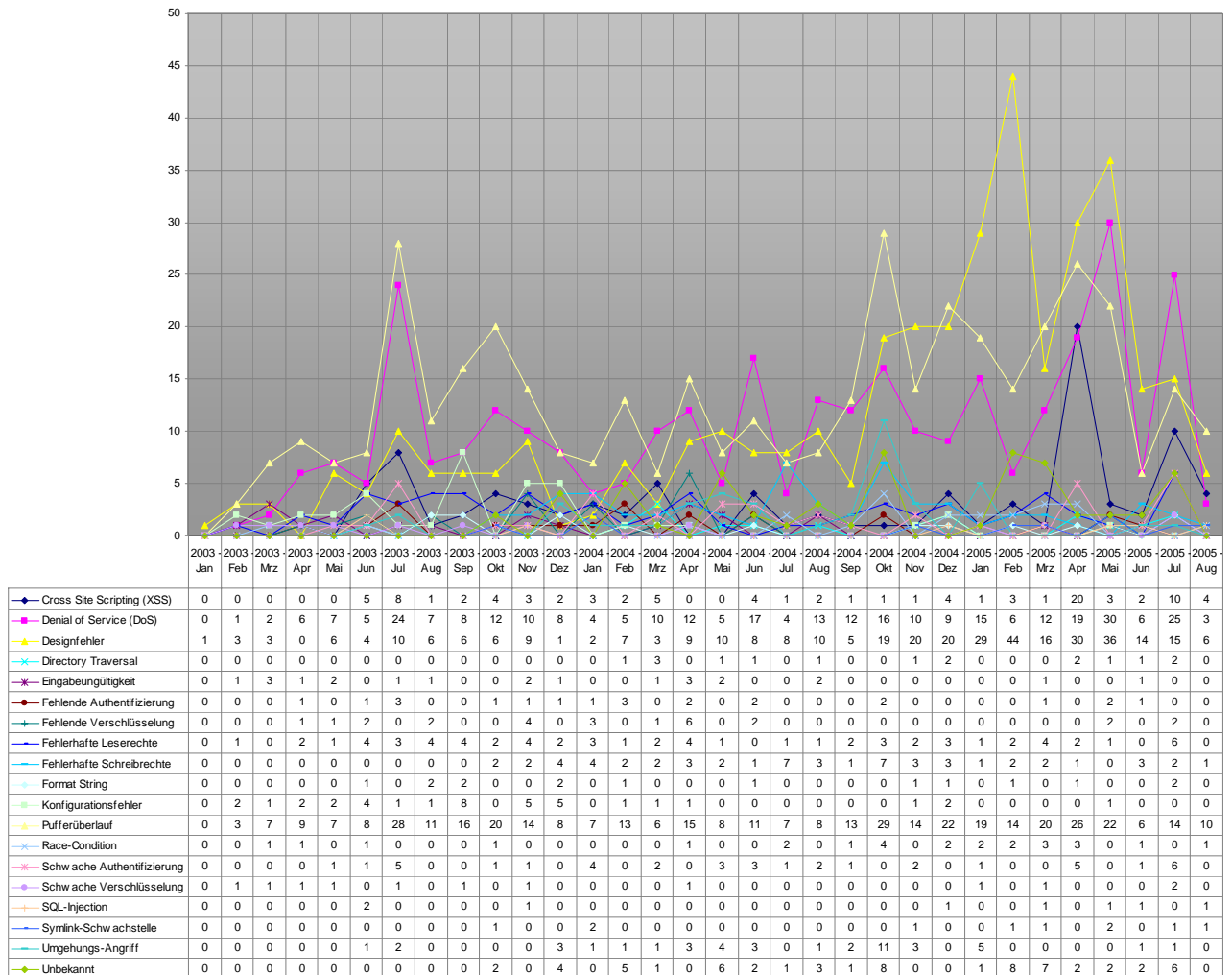


	2005 - Jun	2005 - Jul	2005 - Aug
Cross Site Scripting (XSS)	2	10	4
Denial of Service (DoS)	6	25	3
Designfehler	14	15	6
Directory Traversal	1	2	0
Eingabegültigkeit	1	0	0
Fehlende Authentifizierung	1	0	0
Fehlende Verschlüsselung	0	2	0
Fehlerhafte Leserechte	0	6	0
Fehlerhafte Schreibrechte	3	2	1
Format String	0	2	0
Konfigurationsfehler	0	0	0
Pufferüberlauf	6	14	10
Race-Condition	1	0	1
Schwache Authentifizierung	1	6	0
Schwache Verschlüsselung	0	2	0
SQL-Injection	1	0	1
Symink-Schwachstelle	0	1	1
Umgehungs-Angriff	1	1	0
Unbekannt	2	6	0

Verlauf der letzten drei Monate Schwachstelle/Kategorie



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat



Verlauf der Anzahl Schwachstellen/Kategorie pro Monat

## 5. Fachartikel

### 5.1 1997 bis 2007 - Die Entwicklung der (deutschsprachigen) Hacker-Szene, Teil 2

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

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 der Gang Richtung Informatik oder Mathematik natürlich offensichtlich erschien. Andere wollten direkt in die Wirtschaft, liessen sich irgendwo als Administrator oder Security Consultant anstellen. Unter der Hand wurden einige Auftragsarbeiten, vorwiegend Penetration Tests, 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 haben, wurden nun plötzlich von namhaften Firmen engagiert - Die 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.

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 Individuen 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!

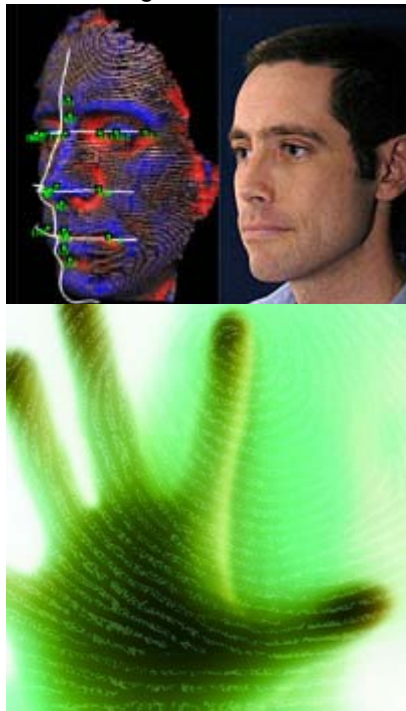
### Die Zukunft bringt aber nicht nur Schlechtes

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 "bösaartigen 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.

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 unserer 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.

## 6. Kreuzworträtsel

Computer Online Adventure	Klassischer Security Scanner		Zeichen-Codierung	Linux ist ...	Back Office			Abk. Emergency Room	Web adresse	Auf Chipkarten genutzte Verschlüsselung
		3	Person welche die IT-Umgebung betreut							Betriebssystem von Cisco
Worum handelt es sich bei RJ-46					1	Deutscher Philosoph und Logiker	Acid Burn im Film "Hackers"			5
Virtual Private Network	Abk. Pro Evolution Soccer		Abk.: Initiale Sequenznummer		Deutsche Hacker-Gruppe					Briefqualität
			Kommandozeilen-Web browser	DOS: Kopiert Dateien	Unix: Löschen einer Datei		DOS: Löscht den Bildschirm			
		DOS: Vergleicht den Inhalt von Dateien	Deutscher Hacker-Club			Chat-System				Unix: Verschieben einer Datei
Top-Level-Domain von Schweden			Windows Version für Desktop		Kommando für ICMP echo request				Würde von Apple Records verklagt	
Klassischer UNIX-Texteditor	Hersteller von Proventia				Nachfolgerin der TCPA			Analog-Digital-Wandler		
2		Unix: Dateiinhalt anzeigen		Abk.: General Public License		Objektorientierte Programmierung	6		Fernsehnorm	
			Hersteller von Solaris		Linux: Anzeige Speicher und Nutzung		DOS: Bearbeitet Dateien mit Texteditor	Abk. Intrusion Prevention System		4
Taste für Sonderfunktionen / Steuerzeichen					Disketten-Controller					
Bedienoberfläche für OS/2	Übertragung multi-medialer Inhalte auf Mobiles				Hauptbausteine sicherer HW der TCPA					
		Künstliche Intelligenz		Javascript						
Bundesamt für Sicherheit in der Informatik			Vorgänger von Windows 2000							

### 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 **15.09.2005**. 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 einen Monat des [Securitytracker](#) Dienstes [pallas](#).

### SECURITYTRACKER



## 7. Literaturverzeichnis

scip AG, 2003a, scip monthly Security Summary,  
Ausgabe März 2003

[http://www.scip.ch/publikationen/smss/scip\\_mss-mar03.pdf](http://www.scip.ch/publikationen/smss/scip_mss-mar03.pdf)

scip AG, 2003b, scip monthly Security Summary,  
Ausgabe März 2003

[http://www.scip.ch/publikationen/smss/scip\\_mss-19\\_08\\_2003-1.pdf](http://www.scip.ch/publikationen/smss/scip_mss-19_08_2003-1.pdf)

## 8. Impressum

Herausgeber:

scip AG

Technoparkstrasse 1

CH-8005 Zürich

T +41 44 445 1818

<mailto:info@scip.ch>

<http://www.scip.ch>

Zuständige Person:

Marc Ruff

Security Consultant

T +41 44 445 1812

<mailto:maru@scip.ch>

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. 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.

### Nutzen Sie unsere Dienstleistungen!

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).

Das **Errata** (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online.

Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)