

## Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Fachartikel
5. Kreuzworträtsel
6. Impressum

### 1. Editorial

#### Sicherheitslücke Mensch?

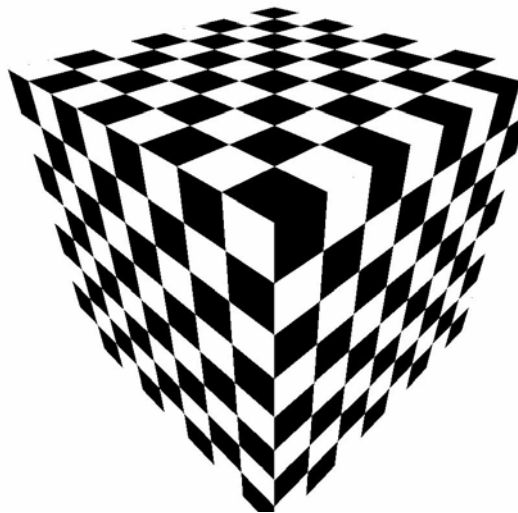
Anfang der 90er Jahre war Kevin Mitnick einer der meistgesuchten Personen der USA. Nach zwei Jahren Fahndungsarbeit wurde er schlussendlich vom FBI verhaftet. Seine Vielzahl seiner Einbrüche in fremde Computersysteme basierten in den meisten Fällen auf sogenannten Social Engineering Attacken.

Bei Social Engineering Angriffen werden zielgerichtet Personen ins Visier genommen. Die Personen werden anhand der zu erreichenden Ziele ausgesucht. Ein Beispiel: Das Ziel ist der physische Zugang in die Büroräumlichkeiten des CEO der Firma. Als erstes wird eruiert, welche Personengruppen Zutritt zum Zielobjekt haben.

Nach erfolgreicher Aufdeckung der Zugangsberechtigten gilt es im nächsten Schritt zu überlegen, welche der potentiellen Möglichkeiten die höchste Erfolgchance zur Erreichung des Zieles bieten. Anhand dieser Einschätzung wird das „Mittel zum Zweck“ gezielt und ungewollt in den Angriff miteingebunden, um das Ziel unentdeckt zu erreichen und wieder zu verlassen.

Die dabei angewandten Methoden können grob in drei Social Engineering Modelle unterteilt werden: Computer Based-, Human Based- und Reverse Social Engineering. Das Computer Based Social Engineering nutzt verschiedene Eintrittsformen technischer Art, bei denen jedoch dem Mitarbeiter die tragende Rolle zukommt. Als Beispiel sei hier Phishing genannt. Das Human Based Social Engineering versucht eher Informationen auf direktem Wege zu erhalten. Als Beispiel nehmen wir hier das vorgetäuschte Lieferantengespräch auf. Bei Reverse Social Engineering agiert der Angreifer als "Retter in der Not". Er verursacht ein Problem und behauptet anschliessend derjenige zu sein, der damit beauftragt wurde, dasselbe zu lösen. Ein Beispiel hierzu ist das melden als Security Engineer, welcher aufgrund von registrierten Attacken im internen Netzwerk schnell die Passwörter ändern muss.

Computer Based Attacken gehören eigentlich zum Standard und wir führen solche bereits seit Gründung der scip AG bei vielen Penetration Test Aufträgen durch. Seien dies nun Inside/Out Attacken, Browserangriffe mit eigenen Exploits oder Phishing-Variationen. Die Erfolgsquote solcher Vorgehen ist für den Kunden jeweils erschreckend hoch.



Seit einigen Monaten registrieren wir zudem eine Zunahme - drei der letzten zehn Projekte - an dedizierten Human Based Social Engineering Aufträgen. Dabei müssen Aufgaben wie die Manipulation des Firmenliftes, das Einschleichen in Büroräumlichkeiten oder die Platzierung und Wiedermitnahme von Keyloggern durchgeführt werden. Es scheint so, als ob das oft angewandte Zitat „Die Kette ist nur so stark wie Ihr schwächstes Glied“ nun auch in der Praxis auf den Menschen appliziert wird.

In den meisten dieser Aufträge geht es darum

der Geschäftsleitung die Verletzbarkeit auf der menschlichen Ebene aufzuzeigen. Das Ziel eines unserer Kunden ist die Erreichung höchster Sensibilisierung auf der obersten Management Ebene durch handfeste Resultate und damit verbunden das Budget zur Durchführung von gezielten Security Awareness Schulungen.

Die Ergebnisse von Social Engineering Aufträgen sind in den meisten Fällen von allen Beteiligten klar nachvollziehbar. Der Verwaltungsrat Präsident versteht die Explosivität und die möglichen Auswirkungen des physischen Zugriffes unbefugter Personen in das Arbeitszimmer des Chief Executive Officers - Wir haben nun mal kein papierloses Büro. Trotz positiver Eigenschaften von Social Engineering Aufträgen muss aufgepasst werden, dass nicht eine weitere Blase à la Intrusion Detection oder PKIs ausgelöst wird. Es ist wohl jedem klar, dass ein Laptop entwendet werden kann, das gilt es nicht zu demonstrieren. Vielmehr geht es darum das Schadenspotential einer Entwendung auf ein Minimum zu reduzieren. Security ist ein Prozess. Die Personen sind auch nur ein Puzzelteil innerhalb eines komplexen und sich ständig weiterentwickelnden Gebildes Namens Information Security. Denn darum geht es: Der Schutz des höchsten Gutes, der Information.

Schlussendlich gilt es folgendes nie zu vergessen: Das Ziel von wirklich böartigen Social Engineering Angriffen ist die Platzierung einer langfristigen Quelle. Es geht in den meisten Fällen nicht darum einmalig Daten zu erlangen. Es geht vielmehr darum, sich einen Zugang zu den Daten des Zielobjektes zu sichern. Aus diesem Grund sind es in den wenigsten Fällen Angriffe sondern vielmehr Social Engineering Prozesse mit mittel- und langfristiger Ausrichtung. Information Security hat bereits in der Personalabteilung zu beginnen, dies mit dem Ziel die Mitarbeiter in den Security Prozess zu integrieren.

Simon Zumstein <sizu-at-scip.ch>  
Geschäftsleiter  
Zürich, 14. Juli 2005

## 2. scip AG Informationen

### 2.1 Neue Rubrik

Der scip monthly Security Summary ist innerhalb der scip AG ein oft und regelmässig besprochenes Thema. Wir diskutieren über redaktionelle Beiträge, interessante News und mögliche Erweiterungen als auch Optimierungen. Im Verlauf eines solchen Meetings kam, wie des öfteren, eine auf den ersten Blick unpassende Idee auf. Auf den zweiten und dritten Gedanken mussten wir alle zugeben, dass das Themengebiet doch in den scip monthly Security Summary (smSS) passen würde.

Also dachten wir: „Mal eine etwas andere Rubrikidee! Fragen wir doch direkt unsere Leser ob das Interesse vorhanden ist und ob uns jemand einen Tipp abgeben kann.“



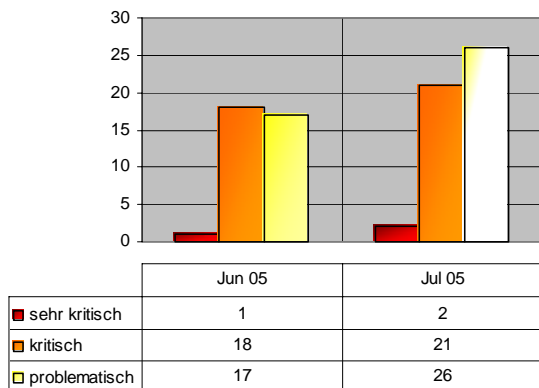
Auf den Punkt gebracht. Gerne würden wir ab einer der kommenden smSS Ausgaben eine neue Rubrik aufnehmen. Ihr Titel: „**IT Hideouts Lokationen**“. In diesem Abschnitt sollen Orte, Bars, Strandabschnitte, Berghütten, Seen etc. aufgenommen werden, in oder um welche man optimal ausschalten und relaxen kann.

Falls Sie als Leser einen Vorschlag haben und diesen gerne publiziert sehen würden, so melden Sie sich bitte bei Simon Zumstein unter der Telefonnummer +41 44 445 18 18 oder per Mail an <mailto:sizu@scip.ch>. Wir freuen uns schon jetzt auf Ihre Erfahrungen. 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 Microsoft Windows XP bis SP2 Kernel unbekannte Denial of Service
- 3.2 Cisco Security Agent bis 4.5.1.616 korruptes IP-Paket Denial of Service
- 3.3 Clearswift MIMESweeper for Web bis 5.1 XML-Verkapselung ActiveX-Code umgehen
- 3.4 Oracle verschiedene Produkte 47 verschiedene Sicherheitslücken
- 3.5 Mozilla Firefox bis 1.0.5 externe Applikationen Webseite öffnen Cross Site Scripting
- 3.6 MIT Kerberos V5 bis 1.4.1 Key Distribution Center korrupte Anfrage Pufferüberlauf
- 3.7 Microsoft Word 2000 bis 2002 Schriftarten Parsing Pufferüberlauf
- 3.8 Microsoft Windows bis XP und Server 2003 Color Management Pufferüberlauf
- 3.9 Adobe Acrobat Reader bis 7.0 UnixAppOpenFilePerform() /Filespec Pufferüberlauf
- 3.10 OpenLDAP bis 2.2.26 Passwort-Wechsel Server-Weiterleitung TLS fehlende Verschlüsselung
- 3.11 Microsoft Internet Explorer 5 und 6 COM Object javaprxy.dll instantiation heap corruption
- 3.12 RealNetworks RealPlayer verschiedene

#### Schwachstellen

### 3.1 Microsoft Windows XP bis SP2 Kernel unbekannte Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 14.07.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1621>

Microsoft Windows XP stellt eine Weiterentwicklung des professionellen Windows 2000 dar. Badpack3t entdeckte eine nicht näher beschriebene Denial of Service-Schwachstelle im Kernel von Microsoft Windows XP; selbst mit installiertem Service Pack 2. Microsoft hat gemeldet, dass sie an einem Patch arbeiten. Als Workaround wird empfohlen, eingehenden Netzwerkverkehr zu den entsprechenden Systemen mittels Firewalling zu limitieren.

#### Expertenmeinung:

Wahrhaftig ist dies eine sehr ernst zu nehmende Sicherheitslücke. Werden Details zu dieser Attacke bekannt, ist es nur eine Frage der Zeit, bis entsprechende Angriffs-Tools und Exploits erhältlich sein werden. Dies heisst jedoch nicht, dass man das Einspielen der entsprechenden Bugfixes nach Erscheinen dieser aufschieben sollte.

### 3.2 Cisco Security Agent bis 4.5.1.616 korruptes IP-Paket Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 13.07.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1620>

Die ursprünglich von der amerikanischen Firma Okena entwickelte Software StormWatch ist eine echte Intrusion Prevention-Lösung. Durch Systemcall-Interception werden unerlaubte Kernel-Zugriffe abgefangen und unterbunden, so dass schwerwiegende Programmierfehler wie Pufferüberlauf-Schwachstellen nicht durch Angreifer ausgenutzt werden können [[http://www.computec.ch/dokumente/intrusion\\_prevention/](http://www.computec.ch/dokumente/intrusion_prevention/)]. Vor einiger Zeit wurde diese Technik durch den Branchenriesen Cisco aufgekauft und neu unter dem Namen Cisco Security Agent (CSA) vertrieben. Wie nun im Cisco Dokument 65545 bekannt wurde, existiert eine nicht näher beschriebene Schwachstelle im Cisco Security Agent bis 4.5.1.616 beim Umgang mit korrupten

IP-Paketen. Es sind keine Details oder Exploits zum Problem bekannt. Der Fehler wurde durch eine neue Software-Version bzw. einen Hotfix behoben.

**Expertenmeinung:**

Okena StormWatch bzw. Cisco Security Agent ist im Verbund mit einer Antiviren-, Firewalling- und Intrusion Detection-Lösung am stärksten. Die einzelnen Elemente können in einem Gesamtkonzept die Schwächen der anderen ausbessern und so für ein Maximum an möglicher Sicherheit in einer Umgebung sorgen. Ironisch ist in diesem Fall, dass eben einer dieser Sicherheitslösungen einen Fehler aufweist - und dies nicht zum ersten Mal -, der die gesamte Sicherheit der Umgebung kompromittieren kann.

### 3.3 Clearswift MIMESweeper for Web bis 5.1 XML-Verkapselung ActiveX-Code umgehen

Einstufung: **kritisch**

Remote: Ja

Datum: 13.07.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1619>

MIMESweeper der Firma Clearswift ist eine populäre kommerzielle Lösung für das Absichern spezifischer Dienste. Vor allem im SMTP-, aber auch im Web-Bereich werden diese Proxy-Produkte eingesetzt. Wie der Hersteller meldete, existiert eine Evasion-Schwachstelle in Clearswift MIMESweeper for Web bis 5.1. So werden ActiveX-Elemente in XML-Verkapselten HTML-Dateien nicht richtig erkannt. Zusammen mit dem Advisory wurde ein entsprechender Patch herausgegeben.

**Expertenmeinung:**

Es ist schon ein bisschen peinlich, dass Clearswift MIMESweeper for Web gegen solcherlei Verkapselungs-Angriffe verwundbar ist. Da diese Schwachstelle relativ einfach ausgenutzt werden kann, ist es umso wichtiger, schnellstmöglich Massnahmen einzuleiten.

### 3.4 Oracle verschiedene Produkte 47 verschiedene Sicherheitslücken

Einstufung: **sehr kritisch**

Remote: Teilweise

Datum: 13.07.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1618>

Oracle ist eine vor allem im professionellen Umfeld gern eingesetzte Datenbank-Lösung.

Oracle gab im Rahmen seines vierteljährlichen Critical Patch Update ein Advisory heraus, das sich 47 verschiedenen - teilweise kritischen - Sicherheitslücken annimmt. Das PDF-Dokument weist in einer Matrix die Schwachstellen aus, zeigt mitunter auch ihre Auswirkungen und Voraussetzung auf. Es ist jedoch nicht ersichtlich, welcher Kategorie (z.B. Pufferüberlauf oder Format String) die jeweiligen Fehler zugeordnet werden müssen. Technische Details oder Exploits zur Schwachstelle sind bisher nicht bekannt, könnten jedoch in den kommenden Tagen auf den einschlägigen Sicherheitsmailinglisten und -Webseiten folgen. Oracle hat entsprechend Patches für die betroffenen Produkte bereitgestellt.

**Expertenmeinung:**

Wahrhaftig eine Vielzahl an Schwachstellen, die Oracle hier vier Mal im Jahr zusammenträgt. Für Administratoren entsprechender Lösungen ist dies natürlich sodann eine stressige Zeit, in der die jüngsten Patches überprüft und eingespielt werden sollen. Gut und gerne mindestens eine Woche ist man damit beschäftigt, sich auf ein solches Patching - und wir reden hier nur von einem System - vorzubereiten. Überstunden sind deshalb die Regel. Ob dieses Patchday-Prinzip, wie es auch Microsoft seit einigen Monaten umzusetzen pflegt, wirklich so von Vorteil ist, muss nach wie vor bezweifelt werden.

### 3.5 Mozilla Firefox bis 1.0.5 externe Applikationen Webseite öffnen Cross Site Scripting

Einstufung: **kritisch**

Remote: Ja

Datum: 13.07.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1612>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, wobei das aktuelle Ziel der Entwickler ein Marktanteil von 10 % darstellt. Michael Krax entdeckte einen Designfehler in Mozilla Firefox bis 1.0.5. Ruft eine externe Applikation eine Webseite mit javascript-URI im Mozilla Firefox auf, wird für diese die Rechte der zuvor besuchten Webseite übernommen. Ein Angreifer kann diesen Umstand für entsprechende Cross Site Scripting-Zugriffe nutzen. Der Fehler wurde in der Version 1.0.5 behoben.

**Expertenmeinung:**

Schon wieder eine Vielzahl an Sicherheitslücken prasselt auf das Mozilla-Projekt nieder. Keine gute Werbung, in der Tat - Obschon Mozilla immerwieder als Alternative zum beschmutzten Microsoft Internet Explorer empfohlen wird, wird voraussichtlich über längere Zeit auch das Mozilla-Pendant seine weisse Weste nicht sauber halten können. Es scheint, als müsse der sichere Webbrowser erst noch entwickelt werden, denn Mozilla bringt die gleichen (Kinder-)Krankheiten mit, wie auch schon viele vergleichbare Projekte zuvor.

### 3.6 MIT Kerberos V5 bis 1.4.1 Key Distribution Center korrupte Anfrage Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 13.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1600>

Kerberos ist ein etabliertes System zur sicheren Authentisierung von Benutzern und Systemen. Auf praktisch allen wichtigeren Plattformen sind entsprechende Implementierungen gegenwärtig. Im Advisory des MIT wird Daniel Wachdorf als Finder zweier Schwachstellen im Key Distribution Center (KDC) des MIT Kerberos V5 bis 1.4.1 genannt. Zum zweiten kann nämlich mit einem korrupten TCP- oder UDP-Segment eine Pufferüberlauf-Attacke umgesetzt werden. Dadurch lässt sich beliebiger Programmcode ausführen oder das Kerberos-Realm zum Absturz bringen. Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Sun hat diesen Fehler ebenfalls in ihrem Betriebssystem Sun Solaris bestätigt. Das MIT hat einen Patch zu diesem Problem herausgegeben.

#### Expertenmeinung:

Gleich drei kritische Schwachstellen machen dem Kerberos-Projekt das Leben schwer. Da Kerberos oftmals das Rückgrat moderner Netzwerk-Lösungen darstellt und die Verbreitung entsprechend hoch ist, ist das für viele Administratoren - abgesehen von der Vielzahl kritischer Schwachstellen in den Microsoft-Produkten - eine mühsame Aufgabe dieses Monats. Das Einspielen der entsprechenden Patches muss mit Hochdruck geschehen, um allfällige Übergriffe frühzeitig abfangen zu müssen. Der eine oder andere Administrator wird deshalb die eine oder andere Überstunde schieben müssen.

### 3.7 Microsoft Word 2000 bis 2002 Schriftarten Parsing Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 12.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1597>

Microsoft Word ist ein kommerzielles Textverarbeitungsprogramm, das als Teil der Office-Suite ausgeliefert wird. Es wird sowohl im beruflichen als wie auch im privaten Bereich gerne eingesetzt. Im Microsoft Security Bulletin MS05-035 wird eine Pufferüberlauf-Schwachstelle in Microsoft Word 2000 und 2002 gemeldet. Der Fehler besteht im Parsing von Schriftarten, was zum Ausführen bliebigem Programmcodes führen kann. Genaue technische Details und Exploits sind nicht bekannt. Es wird das Einspielen der freigegebenen Patches empfohlen. Alternativ kann das Nutzen einer alternativen Word-Lösung (z.B. WordPad) kurzzeitig Abhilfe schaffen. Es sollten zudem keine Word-Dokumente unbekannter oder zwielichtiger Herkunft geöffnet werden.

#### Expertenmeinung:

Diese Schwachstelle ist vor allem für Viren-Entwicklern interessant. Diese werden voraussichtlich die neue Funktionalität für das Erstellen neuer Schädlinge zu nutzen wissen. Es ist also mit einer erhöhten Anzahl Word-Viren in naher Zukunft zu rechnen.

### 3.8 Microsoft Windows bis XP und Server 2003 Color Management Pufferüberlauf

Einstufung: **sehr kritisch**  
Remote: Ja  
Datum: 12.07.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1596>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Im Microsoft Security Bulletin MS05-036 wird eine schwerwiegende Pufferüberlauf-Schwachstelle in sämtlichen Windows-Versionen gemeldet. Während des Validierens eines ICC-Tags kann beliebiger Programmcode über das Color Management Module ausgeführt werden. Der Angriff lässt sich durch ein korruptes Bild, das beispielsweise Teil einer Webseite oder eines HTML-Emails ist, umsetzen. Genaue technische Details sind öffentlich nicht bekannt.

Microsoft meldet jedoch, dass erfolgreiche Einbrüche schon umgesetzt wurden. Entsprechend wurde schnellstmöglich mit einem Patch für die betroffenen Windows-Versionen reagiert.

**Expertenmeinung:**

Wahrhaftig ist dies eine sehr ernst zu nehmende Sicherheitslücke. Werden Details zu dieser Attacke bekannt, ist es nur eine Frage der Zeit, bis entsprechende Angriffs-Tools und Exploits öffentlich die Runde machen werden. Dies heisst jedoch nicht, dass man das Einspielen der entsprechenden Bugfixes aufschieben sollte. Die von Microsoft zur Verfügung gestellten Patches sollten unverzüglich eingespielt werden, um das Risiko eines erfolgreichen Angriffs zu minimieren.

### 3.9 Adobe Acrobat Reader bis 7.0 UnixAppOpenFilePerform() /Filespec Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 05.07.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1582>

Der Acrobat Reader der Firma Adobe ist eine Software für das Interpretieren, Darstellen und Drucken von PDF-Dokumenten. Besonders in der Geschäftswelt ist dieses Dateiformat sehr gern aufgrund seiner hohen Verbreitung, Kompatibilität und der dargelegten Komprimierung gern genutzt. iDEFENSE meldete einen Pufferüberlauf in der Funktion UnixAppOpenFilePerform() beim Umgang von /Filespec während des Öffnens einer Datei. Das Problem existiert im Adobe Acrobat Reader bis 7.0 auf Linux und Solaris sowie bis 5.0.11 auf IBM AIX und HP-UX. Ein Angreifer kann darüber bliebigem Programmcode auf dem Zielsystem ausführen lassen. Ein Update auf eine nicht verwundbare Acrobat-Version wird deshalb empfohlen.

**Expertenmeinung:**

Dieses Problem könnte durchaus in der Geschäftswelt zu einem Risiko für Linux-Umgebungen werden. Der eine oder andere Angriff könnte durchaus umgesetzt werden, denn der Umgang mit PDF-Dokumenten wird gut und gerne gepflegt. Firewall- und Mail-Systeme filtern nur selten PDF-Dokumente, so dass das Einschleusen von Code in ein internes Netzwerk durchaus eine Möglichkeit darstellt. Gegenmassnahmen, also das Informieren der Mitarbeiter und/oder das Einspielen der aktuellen

Version, sollten also in den kommenden Tagen umgesetzt werden.

### 3.10 OpenLDAP bis 2.2.26 Passwort-Wechsel Server-Weiterleitung TLS fehlende Verschlüsselung

Einstufung: **kritisch**

Remote: Ja

Datum: 04.07.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1580>

LDAP (Lightweight Directory Access Protocol) ist ein Netzwerkprotokoll, das die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes (eine im Netzwerk verteilte hierarchische Datenbank) erlaubt [<http://www.ietf.org/rfc/rfc2251.txt>]. Wie gemeldet wurde, existiert ein schwerwiegender Designfehler in OpenLDAP bis 2.2.26 und pam\_ldap bis 1.76. Wird ein Passwort-Wechsel initiiert und der Slave-Server leitet den Benutzer zum Master-Server weiter, wird keine TLS-Verschlüsselung genutzt. Sensitive Daten werden sodann im Klartext über das Netzwerk übertragen. Ein Angreifer kann diese dann mit einem Sniffer (z.B. Dsniff) mitlesen. Genaue technische Details zur Schwachstelle sind nicht bekannt. Die betroffenen Projekte haben aktualisierte Versionen ihrer betroffenen Lösungen herausgegeben.

**Expertenmeinung:**

Man kommt fast nicht umher, den betroffenen Projekten nach solchen Patzern Inkompetenz vorzuwerfen. Eine ausgiebige Testreihe der herauszugebenden Patches scheint erforderlich, denn so hätten frühzeitig entsprechende Komplikationen entdeckt und gehandelt werden können.

### 3.11 Microsoft Internet Explorer 5 und 6 COM Object javaprxy.dll instantiation heap corruption

Einstufung: **sehr kritisch**

Remote: Ja

Datum: 30.06.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1578>

Der Microsoft Internet Explorer (MS IEX) ist fester Bestandteil moderner Windows-Betriebssysteme und damit der weitverbreiteste Webbrowser. Wiederum wurde eine Schwachstelle bestätigt. Die am 17.06.2005 an Microsoft gemeldete Schwachstelle wurde vorerst nicht bestätigt. Erst am 30.06.2005

erstellte Microsoft ein Advisory und bestätigt damit die Existenz des Bugs. Wie die Firma SEC Consult meldet, kann das Laden von HTML Dokumenten mit bestimmten eingebundenen CLSIDs (ClassIdentifier) [Link 1] in einer null-pointer exception resultieren oder eine memory corruption die Folge sein. Dadurch kann es theoretisch möglich sein, beliebigen Code im Kontext des Browsers auf dem betroffenen System auszuführen. Ein proof of concept des Denial of Service (DOS) Angriffes steht bereits zur Verfügung. Die Ausnutzung der Schwachstelle beruht auf der Tatsache, dass der Internet Explorer die Ausführung von nicht ActiveX Kontrollen (Zb COM Objekte) via den <object> Tag zulässt. Vorerst empfiehlt der Hersteller die Einstellungen der Intranet Security Zone auf "high" zu justieren. Betroffen sind sowohl Internet Explorer 5 und 6. Microsoft hat am 12. Juli 2005 nun den ersehnten Patch veröffentlicht

#### Expertenmeinung:

Ein weiterer sehr unschöner Bug wovon der Internet Explorer betroffen ist. Auch hier gilt es wiederum sicherzustellen, dass in Outlook keine HTML-Mails angezeigt werden können inkl. Preview. Denn egal ob Sie einen alternativen Browser als Standard Browser eingestellt haben, Outlook verwendet den IEX zur Darstellung von HTML-Inhalt. Es trifft sich gut, dass ich erst letztes mit Leuten von Microsoft gesprochen habe. Die haben mir mitgeteilt, dass Microsoft darüber nachdenkt, den IEX 7 lediglich mit Gast-Rechten laufen zu lassen. Eine löbliche Idee von Seiten Sicherheit. Mal schauen ob es die Benutzer zu schätzen wissen. Ein erster Exploit wurde veröffentlicht. Es ist nur eine Frage der Zeit bis weitere und gefährlichere "in the wild" auftauchen.

### 3.12 RealNetworks RealPlayer verschiedene Schwachstellen

Einstufung: **kritisch**  
Remote: Ja  
Datum: 24.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1576>

Der Real Player der Firma Real Networks kann für das Abspielen der hauseigenen Real-Formate (RealAudio und RealVideo) genutzt werden. Die Software ist als Freeware-Version für Windows, UNIX und Macintosh verfügbar. Wie der Hersteller meldet, existieren verschiedenste Schwachstellen in den RealPlayer und RealOne Player Software. Durch das Ausnutzen dieser Bugs können externe Angreifer lokale Dateien überschreiben oder gar

das gesamte System kompromittieren. Die Schwachstelle zum Überschreiben lokaler Dateien resp. dem Ausführen eines ActiveX kann über ein speziell aufbereitetes MP3 umgesetzt werden, ist jedoch nicht näher beschrieben. Schwerwiegender ist die Schwachstelle innerhalb des RealText Streams, namentlich in der Funktion "CRealTextFileFormat::ReadDone()". Bei der Ausnutzung dieses Bugs innerhalb des RealMedia files wird ein heap-based Pufferüberlauf erzwungen. Dadurch sieht sich der Angreifer in der Lage beliebigen Code auf dem System umzusetzen. In die gleiche Kerbe und mit den selben Auswirkungen schlägt die Schwachstelle in den AVI Dateien zu. Dank korruptierten AVI Dateien wird ein heap-based Pufferüberlauf erzwungen und dem Angreifer steht es frei Code auf dem angegriffenen System auszuführen. Die letzte rapportierte Schwachstelle kann via einer malicious Webseite ein lokales HTML file erstellen welches eine RM Datei ausführt welche wiederum auf das File HTML verweist. Alle Schwachstellen benötigen eine Interaktion des Benutzers. Entweder muss eine präpariertes MP3, RealMedia oder AVI Datei geöffnet werden oder aber eine entsprechende Webseite aufgerufen werden, welches automatisch die Dateien öffnet. Betroffen sind RealPlayer 8, 10, 10.5 und Enterprise, RealOne Player v1 und v2. Sowohl auf den Windows Betriebssystemen als auch auf Linux und Mac. Ausgenommen sind die Handheld Devices. Eine Auflistung der betroffenen Softwares finden Sie unter Link 2.

#### Expertenmeinung:

Einmal mehr zeigt auch diese Verwundbarkeit, dass harmlose Client-Applikationen für schwerwiegende Attacken missbraucht werden können. Das Einspielen der Patches ist entsprechend empfohlen.

## 4. Fachartikel

### 4.1 1997 bis 2007 - Die Entwicklung der (deutschsprachigen) Hacker-Szene, Teil 1

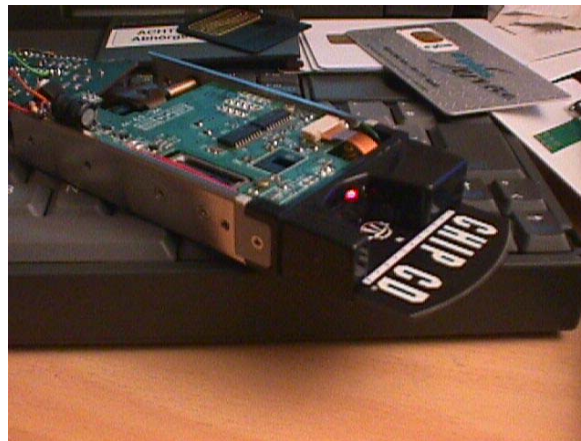
Marc Ruef, scip AG, maru-at-scip.ch

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

Ich war schon immer von Computern begeistert. In früher Kindheit, als ich noch keinen eigenen Computer besass, habe ich Basic-Programme auf meiner alten Schreibmaschine vorbereitet, um sie später auf dem 486er meines Vaters abtippen zu können. Neben Computerspielen und kleineren Simulationen (z.B. ein textbasiertes SimCity) hat mich stets die künstliche Intelligenz und das Entwickeln von Computerviren interessiert.

Wie ist es nur möglich eine Anwendung zu schreiben, die sich selber reproduziert, sich selber verändert und im Hintergrund Arbeiten erledigt?

Mit dem Eintritt ins Internet eröffnete sich eine komplett neue bzw. erweiterte Welt für mich. Webseiten und Publikationen zu Computerviren gab es im Web wie Sand am Meer. Was ich früher in Büchereien nachschlagen musste, wurde mir multimedial ins Arbeitszimmer gebracht. Innert weniger Tage habe ich wohl jede Zeile zum Thema gelesen, die bis dato im Internet publiziert wurde. Beim Besuchen dieser "Hacker-Seiten" kam ich ebenfalls ein erstes Mal



mit anderen Themengebieten der Computersicherheit in Berührung. Die Angriffsmöglichkeiten von TCP/IP oder die Sicherheit von Chipkarten waren die Dinge, die mich sofort in ihren Bann zogen. Der Gedanke, das letzte Bit eines Computers verstanden zu haben und mit ihm schier unmögliche Zauberticks vollbringen zu können, hat mich mehr dennje begeistert.

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

Die Webseite war klein und dennoch fein genug, um zu Beginn Tag für Tag ein paar Duzent Besucher anzulocken. In dieser vergangenen Zeit war das Internet noch eher ein kleines Dorf, in dem sich jeder kannte. Obschon ich damals nur einen

Bruchteil der heutigen Besucherzahlen von computec.ch verbuchen konnte, erhielt ich ein Mehr an Zuschriften von interessierten Lesern. Immerwieder gab es Leute, die mir ihre Erfahrungen mitteilten, über Chipkarten und die Welt philosophieren wollten. Das Schreiben von Emails wurde so schnell zu einem ausfüllenden Hobby, in dem ich mich zu Hause fühlte.

### Hacker-Vereinigungen

Selbstverständlich vergass ich beim Betreuen der Webseite und dem Schreiben von Emails nicht, ebenfalls das Internet nach neuen und interessanten Artikeln zu durchforsten. Damals spriessten Hacker-Seiten wie Pilze aus dem

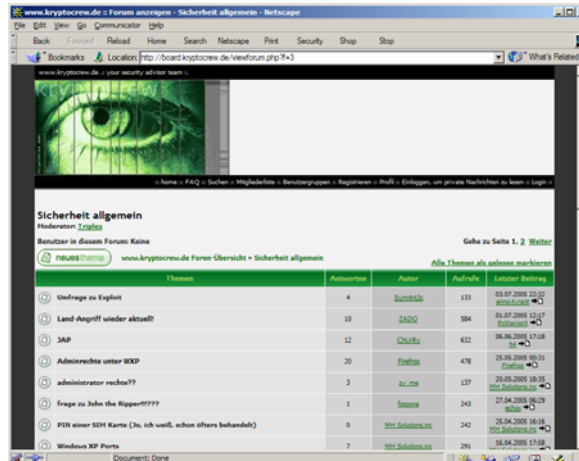
Boden. Keine Woche verging, ohne dass irgendeine neue Gruppierung gegründet wurde. Viele von diesen überlebten jedoch kein Jahr oder die mangelnde Qualität ihrer Publikationen machte ein Besuch nicht wirklich lohnenswert. Eine bestimmte Projekt-Gruppe war jedoch für Kontinuität und Qualität bekannt:

Auf [kryptocrew.de](http://kryptocrew.de) wurde ein umfassendes Archiv geschaffen, das eine Vielzahl an Artikeln aus den verschiedensten Themenbereichen der Computersicherheit zusammenfasste. Unzählige Stunden habe ich mit dem Verschlingen der dort abgedruckten Artikel verbracht - Selbst das Blinzeln mit meinen Augen habe ich als unnötige Verschwendung meiner Zeit betrachtet, so gebannt war ich durch die umfassende Darlegungen der Funktionsweise von polymorphen Dateiviren und erweiterten Blueboxing-Angriffen (dies ist eine klassische Disziplin des Phone Hackings).

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

Die KryptoCrew war eine kleine Gruppe, bestehend aus etwa 5 Leuten, die zusammen die Webseite administrierten, Publikationen verfassten und Software entwickelten. Da ich den freien Dienst der Truppe sehr gut zu schätzen wusste, schrieb ich - einfach mal aus Spass - ein Email an den Seitenadministrator. In meinen Zeilen brachte ich meine Hochachtung vor ihrer Arbeit zum Ausdruck, verwies kurz auf mein eigenes Webseiten-Projekt und offerierte eher nebenbei eine Zusammenarbeit. Das Antwortschreiben, zwar relativ knapp aber dennoch ausserordentlich freundlich, kam für mich unerwartet. Ich dachte mir, dass ein solch grosses und etabliertes Projekt wohl kaum die

Zeit finden wird, um auf meine unwichtigen Anfragen einzugehen. Man hat sich für das Lob bedankt und im Abschluss des Emails wurde darauf verwiesen, dass meine Webseite und Artikel durchaus Begriffe seien und ich mich doch mal über das offizielle Antrags-Formular um eine Mitgliedschaft bewerben solle.



anonymen Projekt hat sich so für mich schnell eine Gruppe von Gleichgesinnten entwickelt, die Spass am Wissen haben wollten. Also genau nach meinem Geschmack!

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

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

brauchte ich keine Zeugnisse oder Zertifikate vorzuweisen - Meine Publikationen machten das ihrige.

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

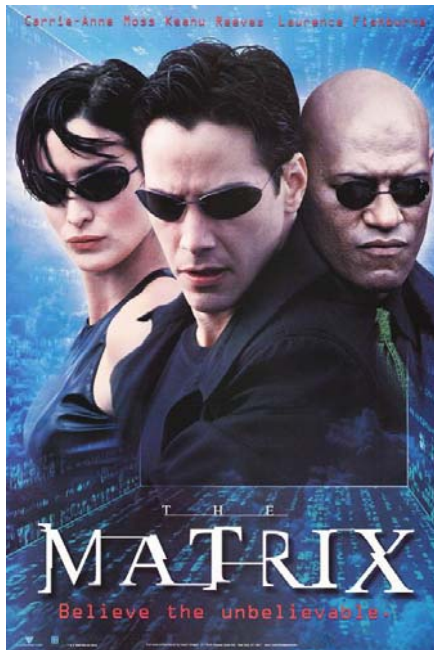
### Erste Schritte in der Professionalität

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

Spätestens als der Kultfilm "The Matrix" (<http://www.imdb.com/title/tt0133093/>) im Jahr 1999 ins Kino kam, war der bis dato grösste "Hacker-Boom" zu verzeichnen. Kein Chat-Raum war mehr vorhanden, in dem nicht mindestens ein Halbstarker "Neo", das Pseudonym der

Hauptfigur des Films, als seinen Benutzernamen wählte. Meine Webseite und das KryptoCrew-Projekt konnten sich zwischenzeitlich über Jahre als gute deutschsprachige Quellen des Genres etablieren. Und es gab Tage, an denen wurde ich regelrecht mit Emails überschwemmt. In Höchstzeiten erreichten mich rund 40 Schreiben, in denen ich zu einem Thema befragt oder um etwas gebeten wurde (Mit welchem Algorithmus soll ich meine Festplatten verschlüsseln? Wo finde ich leere Chipkarten? Um was für einen Virus handelt es sich hier?). Eine aufregende und zugleich stressige Zeit, in der das Knüpfen von soliden Kontakten gerade wegen dieser grossen Quantität und der fehlenden Übersichtlichkeit nicht einfacher war.

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



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

Firewalling war das erste wirtschaftlich (und technisch) ausgeschlachtete Gebiet der Computersicherheit. Die Erfolge der New Economy Zeit verlangten nach Mehr. Es bot sich entsprechend an einen Schritt weiter zu gehen und mit Intrusion Detection-Systemen (Abk. IDS) Angriffe frühzeitig erkennen zu können. In der Branche hiess es plötzlich, dass Firewalling nur ein kleiner Teil einer umfassenden Sicherheitslösung sei und wer etwas auf sich

halte, der müsse zwingend IDS einsetzen. Der eine oder andere Kunde hat sich dazu – oftmals wirklich sehr gute Lösungen - überreden lassen. Übersehen wurde aber einmal mehr, dass bei derlei Lösungsansätzen das frühzeitige Umsetzen eines soliden Konzepts – wie auch schon beim Firewalling - unabdingbar ist. Eine weitere Schwierigkeit in der elektronischen Einbruchserkennung ist in der stetigen und kompetenten Betreuung einer IDS-Lösung gegeben. Ein solches System war nicht in der Lage autonom und selbstständig zu arbeiten. Fortwährend hätte ein Administrator die Protokolle auswerten und Anpassungen am Regelwerk vornehmen können. Ein Full Time Job, der in den wenigsten Unternehmungen, die sich ein Intrusion Detection-System haben integrieren lassen, gebilligt wurde.

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



## 6. 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)

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!](#)