

Contents

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

1. Editorial

Information Security - Ein Schritt zur Seite

Ein weiteres Jahr ist an uns vorbeigezogen und die neue Zeitperiode hat eben erst begonnen. 2005 war ein sehr erlebnisreiches Jahr. Viele interessante Projekte wurden angerissen und abgeschlossen, etliche gute Gespräche führten zu neuen Erkenntnissen und einige nervenaufreibende Verhandlungen wurden geführt. Das abgelaufene Jahr hatte viel zu bieten und verspricht Aufregendes für das Jahr 2006!

Den Jahreswechsel zum Anlass nehmend, erlaube ich mir eine persönliche und keineswegs abschliessende IT-Security Resümierung des 2005.

Blicke ich zurück so fallen mir insbesondere zwei Themengebiete auf. Als erstes wäre da das Thema IP-Telefonie und VOIP-Sicherheit. Unzählige Male wurden wir als scip AG zu eben diesen Thematiken angefragt. Viele Firmen haben das grundsätzliche Einsparpotential dieser Technologie gesehen. Leider werden grosse Teile dieser Einsparungen, in vielen Fällen,

durch die notwendigen zusätzlichen Investitionen in die Sicherheit zunichte gemacht. Das interne Verkaufsargument Einsparungen ist nicht der ausschlaggebende Grund zur Integration einer VOIP-Anlage. Vielmehr sind dies zukunftssträchtige Gegebenheiten. Voice over IP wird in naher Zukunft die bestehenden Telefonanlagen verdrängen, davon bin ich überzeugt. Derzeit leiden heutige VOIP-Infrastrukturen noch an mir unerklärlichen Kinderkrankheiten. Sowohl aus technischer und konzeptioneller Securitysicht als auch an betrieblichen Unschönheiten. Die notwendigen Anpassungen werden aber in naher Zukunft umgesetzt werden.

Das zweite Themengebiet sind Standards innerhalb der IT-Security. Im Prinzip ein altes Thema aber immer noch ungelöst. Je nach Anforderung des Kunden ist ein anderer bestehender Standard der am ehesten passende. Obwohl die unterschiedlichen Standards im Prinzip dasselbe Ziel verfolgen. Glücklicherweise sind uns die gängigsten Security Standards wie ISO 17799, BSI Grundschutzhandbuch, OSSTM und prozessbezogene Vorgaben wie ITIL, CobIT oder SOX nicht unbekannt und wir können gewisse Nach- und Vorteile einschätzen. Die Sensibilisierung der zuständigen Stellen, dass ein Standard sinnvoll ist, ist auf jeden Fall geglückt. Kein Kunde welcher nicht gewisse Daten nach Standard erhebt, sich in seinen Policies an eine gängige Regel anlehnt oder dies als Ziel definiert. In vielen Fällen haben die regulatorischen Vorgaben diese „Standardisierung“ vorangetrieben [scip 2003].



Standards sind unumgänglich und bieten eine Fülle an positiven Errungenschaften sind aber kein umfassendes Heilmittel. Schlussendlich werden sich die Standards mit dem besten und einflussreichsten Lobbyismus durchsetzen und nicht zwangsläufig die optimalsten.

Zusammenfassend gesehen hat sich die Information Security im 2005 seitwärts bewegt. Es wurden keine wegweisenden neuen Technologien etabliert noch wurden bestehende Grundsätze

ze durch aktuelle Erkenntnisse ausser Kraft gesetzt. Dieser Schluss kann sowohl negativ als auch positiv gewertet werden. Negativ betrachtet ist das Jahr 2005 somit kein Meilenstein der IT-Security Geschichte und schnell abzuhacken. Positiv gesehen ist dieser Schritt zur Seite eine grosse Chance um in den kommenden Jahren eigene Meilensteine zu etablieren. IT-Security ist ein sehr junges Terrain. Wir haben die Möglichkeit diesem Fachgebiet unseren Stempel aufzudrücken!

"Das Gestern ist nur eine Erinnerung, das Morgen ist niemals, was es vorgibt zu sein." - Bob Dylan

Simon Zumstein <sizu-at-scip.ch>
Managing Director
Zürich, 18. Januar 2006

2. scip AG Informationen

2.1 smSS Abonnenten



Ein weiterer Meilenstein ist errungen. Der vorliegende scip monthly Security Summary wird erstmals an mehr als **900** registrierte Abonnenten versandt.

Wir danken allen Leserinnen und Lesern für das Vertrauen und freuen uns darauf Sie auch in Zukunft mit Informationen beliefern zu dürfen.

Natürlich sind wir einem konstruktiv-kritischen Feedback gegenüber nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Wir freuen uns über Ihre Schreiben an smss-feedback@scip.ch.

2.2 scip AG at a glance

Wissen Sie wer die scip AG ist, was für Dienstleistungen sie anbietet oder gar welche Projekte die scip AG erfolgreich durchgeführt hat?



Der „at a glance“ Flyer stellt die Firma scip AG, zusammengefasst auf einer Seite, kurz und verständlich vor. Lassen Sie sich überraschen http://www.scip.ch/scip_at_a_glance.pdf.

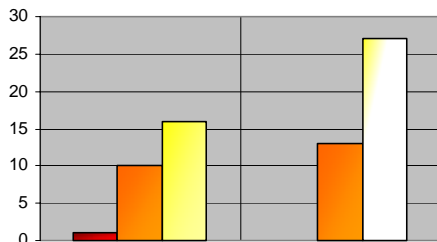
Gerne beantworten wir Ihnen weiterführende Fragen oder stellen uns persönlich und unverbindlich bei Ihnen vor. [Kontaktieren Sie uns](#).

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.



	Dez 05	Jan 06
sehr kritisch	1	0
kritisch	10	13
problematisch	16	27

Contents:

- 3.1 Sun Solaris 8 bis 10 LP Print Service Ipsched erweiterte Rechte
- 3.2 PHP bis 5.1.2 mysqli Fehlermeldung Format String
- 3.3 Cisco Aironet Wireless Access Point ARP-Spoofing Flooding Denial of Service
- 3.4 FreeBSD 6.0 ipfw fragmentierte Pakete Denial of Service
- 3.5 Apple QuickTime bis 7.0.4 korrupte GIF-Bilder Pufferüberlauf
- 3.6 Microsoft Exchange 5, 5.5 und 2000 Email TNEF MIME Attachment Pufferüberlauf
- 3.7 Microsoft Outlook 2000 bis 2003 Email TNEF MIME Attachment Pufferüberlauf
- 3.8 Microsoft Windows 2000, XP und Server 2003 eingebettete Web Fonts Pufferüberlauf
- 3.9 Wine bis 1.12 metafile.c WMF-Bild Denial of Service
- 3.10 IBM Lotus Domino bis 6.5.5 Server korruptes BMP-Bild Denial of Service
- 3.11 RIM BlackBerry Enterprise Server bis 4.0 Server Routing Protocol Denial of Service
- 3.12 RIM BlackBerry Enterprise Server bis 4.0 Attachment Service TIFF-Anhänge Denial of Service
- 3.13 Microsoft Windows korrupte WMF Dateien

ermöglichen Code Execution

- 3.14 VMware verschiedene Produkte NAT korrupte FTP-Anfragen Pufferüberlauf
- 3.15 Symantec verschiedene AntiVirus Produkte korruptes RAR-Archiv entpackten Pufferüberlauf

3.1 Sun Solaris 8 bis 10 LP Print Service Ipsched erweiterte Rechte

Einstufung: **kritisch**

Remote: Teilweise

Datum: 16.01.2006

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1980>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. Der Hersteller weist im Dokument 1-26-102033-1 auf eine Schwachstelle im LP Print Service hin, der zusammen mit Sun Solaris 8, 9 und 10 ausgeliefert wird. Durch einen Fehler in Ipsched kann ein Angreifer erweiterte Rechte erlangen, Dateien lesen und schreiben. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde durch Sun mit dedizierten Patches für die betroffenen Solaris-Versionen adressiert. Als Workaround wird empfohlen, den LP Print Service zu deaktivieren.

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 - vor allem exponierte Hosts und Multiuser-Umgebungen -, sollen Sie schnellstmöglich auf eine aktuelle Software-Version updaten.

3.2 PHP bis 5.1.2 mysqli Fehlermeldung Format String

Einstufung: **kritisch**

Remote: Ja

Datum: 13.01.2006

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1978>

PHP ist ein frei verfügbares open-source Skripting-Paket, das für sämtliche populären Betriebssysteme zur Verfügung steht. Es findet vorwiegend im Web-Einsatz seine Verwendung. Mit der jüngsten Version wurden drei bekannte Schwachstellen geschlossen. Eine besteht als Format String im Umgang mit Fehlermeldungen bei der Erweiterung mysqli. Ein Angreifer kann, sofern verschiedene Gegebenheiten zusammenspielen, erweiterte Rechte erlangen. Genaue technische Details oder ein Exploit sind

nicht bekannt. Der Fehler wurde in der Version 5.1.2 behoben.

Expertenmeinung:

Eine der wenigen Format String Attacks dieses Jahres. Trotzdem zeigt sie sehr imposant, wie wirkungsvoll diese Angriffsart sein kann. Hier ist es jedoch ein riesen Glück, dass verschiedene Gegebenheiten erforderlich sind, damit die Schwachstelle wirklich existent ist und ausgenutzt werden kann.

3.3 Cisco Aironet Wireless Access Point ARP-Spoofing Flooding Denial of Service

Einstufung: **kritisch**
 Remote: Teilweise
 Datum: 13.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1976>

Die Cisco Aironet Serie stellt einen hochwertigen Access Point (Abk. AP) für Wireless LANs zur Verfügung. Die Administration dieses Netzwerkelements erfolgt wahlweise über eine Web-Schnittstelle, deren Kommunikation via HTTP (Hypertext Transfer Protocol) gewährleistet wird. Wie Cisco im SA-20060112 vermerkt, sind die jeweiligen Serien gegen eine Denial of Service-Attacke verwundbar. Durch das Flooden der Admin-Schnittstelle mit gefälschten ARP-Paketen kann die ARP-Tabelle gefüllt und damit der Betrieb verhindert werden. Es wurden Patches für die jeweiligen Produkte herausgegeben.

Expertenmeinung:

ARP-Flooding ist eine klassische und sehr einfach umzusetzende Angriffsform, die nur auf lokale Netze begrenzt ist. Betroffene Systeme sollten die Gegenmassnahmen schnellstmöglich umsetzen, um Reibereien zu verhindern.

3.4 FreeBSD 6.0 ipfw fragmentierte Pakete Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 11.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1970>

Die BSD-Betriebssysteme basieren auf Unix. Es gibt verschiedene Arten und Abkömmlinge, die sich jedoch in ihren Grundzügen stark gleichen. Wie das Entwickler-Team gemeldet hat, existiert eine Denial of Service-Schwachstelle im Firewall-Modul ipfw. Durch fragmentierte Zugriffe lässt sich das System zum Absturz bringen.

Erforderlich dabei ist, dass die Pakete auf eine der gegebenen reset, reject oder react Regeln angewendet werden. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Fehler wurde mit einem simplen Patch adressiert.

Expertenmeinung:

Eine denkbar ungünstige Schwachstelle für ein Firewall-Produkt. Man kann von Glück sprechen, dass hier lediglich eine spezifische Version von FreeBSD anfällig ist. Trotzdem ist dies ein wirklich unschöner Fleck auf der ansonsten doch so schön weissen Weste des alternativen Betriebssystem.

3.5 Apple QuickTime bis 7.0.4 korrupte GIF-Bilder Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 11.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1968>

Der Quicktime Player der Firma Apple wird seit vielen Jahren für die Wiedergabe von Multimedia-Dateien (z.B. mov) verwendet. Diese Software ist als Shareware-Version für verschiedene Betriebssysteme verfügbar. Wie Apple im Advisory APPLE-SA-2006-01-10 schreibt, ist der QuickTime Player bis 7.0.4 gegen eine Reihe von Sicherheitsschwachstellen verwundbar. Eine davon schlägt sich in einem Pufferüberlauf bei der Interpretation korrupter GIF-Bilder nieder. Ein Angreifer kann so beliebigen Programmcode ausführen lassen. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Fehler wurde in der jüngsten QuickTime-Version behoben.

Expertenmeinung:

Diese Schwachstelle ist einmal mehr interessant und zeigt deutlich, dass auch normale Client-Software für indirekte Angriffe genutzt werden kann. Umso erschreckender ist, dass dieser Pufferüberlauf sofort nach dem Einlesen einer korrupten Datei herbeigeführt werden kann. In sicherheitsrelevanten Umgebungen sollte man so oder so auf unnötige Software verzichten. Ist der Quicktime-Player trotzdem benötigt, gilt es auf die neueste Version zu aktualisieren.

3.6 Microsoft Exchange 5, 5.5 und 2000 Email TNEF MIME Attachment Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja

Datum: 10.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1964>

Microsoft Exchange ist ein von vielen Unternehmen gern eingesetzter Mailserver für Windows-Umgebungen. Wie Microsoft in MS06-003 (KB902412) beschreibt, existiert eine schwerwiegende Schwachstelle im Umgang mit TNEF MIME Attachments (Transport Neutral Encapsulation Format). Ein Angreifer kann den gegebenen Pufferüberlauf ausnutzen, um beliebigen Programmcode ausführen zu lassen und damit erweiterte Rechte zu erlangen. Dazu reicht die Interpretation eines entsprechend präparierten Emails. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat das Problem mit einem Patch innerhalb des zyklischen Patch-Days behoben.

Expertenmeinung:

Dieses Problem ist ziemlich schwerwiegend, denn die Schwachstelle ist potentiell einfach und über das Netzwerk/Internet auszunutzen und verspricht die volle Übernahme der Benutzerrechte. Aus diesem Grund sollte man umgehend den entsprechenden Patch einspielen.

3.7 Microsoft Outlook 2000 bis 2003 Email TNEF MIME Attachment Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 10.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1963>

Microsoft Outlook ist ein sehr beliebter Mail-Client (SMTP, POP3 und IMAP4) für die Windows-Reihe. Wie Microsoft in MS06-003 (KB902412) beschreibt, existiert eine schwerwiegende Schwachstelle im Umgang mit TNEF MIME Attachments (Transport Neutral Encapsulation Format). Ein Angreifer kann den gegebenen Pufferüberlauf ausnutzen, um beliebigen Programmcode ausführen zu lassen und damit erweiterte Rechte zu erlangen. Dazu reicht die Interpretation eines entsprechend präparierten Emails. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat das Problem mit einem Patch innerhalb des zyklischen Patch-Days behoben.

Expertenmeinung:

Dieses Problem ist ziemlich schwerwiegend,

denn die Schwachstelle ist potentiell einfach und über das Netzwerk/Internet auszunutzen und verspricht die volle Übernahme der Benutzerrechte. Aus diesem Grund sollte man umgehend den entsprechenden Patch einspielen.

3.8 Microsoft Windows 2000, XP und Server 2003 eingebettete Web Fonts Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 10.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1962>

Microsoft Windows 2000 ist ein professionelles Betriebssystem, das jedoch nach und nach durch den Nachfolger Microsoft Windows XP bzw. Server 2003 abgelöst wird. eEye Digital Security hat einen Fehler herausgefunden, der Microsoft in ihrem Advisory MS06-002 (KB908519) adressiert. Durch eine korrupte eingebettete Web Font kann ein Pufferüberlauf erzwungen und dadurch beliebiger Programmcode ausgeführt werden. Betroffen sind Windows 2000, XP und Server 2003. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Hersteller hat einen Patch für die betroffenen Windows-Versionen herausgegeben.

Expertenmeinung:

Für eEye Digital Security ist es eigentlich untypisch, dass gar keine technischen Informationen zu einer Schwachstelle bereitgestellt werden. Es ist abzusehen, dass dieser Ansatz gewählt wurde, weil die Wirkung eines Exploits verheerend für die Windows-Welt gewesen wäre. Ein Horror-Szenario, wie es W32.Blaster.Worm geschaffen hat, wäre die mögliche Folge gewesen. Dies steigert natürlich das Interesse der Angreifer, die voraussichtlich in den kommenden Wochen mit Details oder gar einem handlichen Exploit aufwarten werden. Das Umsetzen von Gegenmassnahmen darf deshalb keinen Tag länger hinausgezögert werden.

3.9 Wine bis 1.12 metafile.c WMF-Bild Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 08.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1958>

Wine ist der populärste freie Windows-Emulator für Linux, von dem es mittlerweile auch einen

kommerziellen Ableger namens CrossOver gibt. Eine bislang unbekannte Schwachstelle in der Windows Graphics Rendering Engine wurde ursprünglich in Windows gefunden. Durch das Ausnutzen dieser Verwundbarkeit könnte ein externer Angreifer in der Lage sein willkürlich Code auf dem infizierten Rechner auszuführen. Dies mit den Rechten des Benutzers. Bekannt ist, dass sich die Schwachstelle einen Fehler in der Abhandlung korrupter Windows Metafile Dateien (.wmf) zu Nutze macht. Bislang hat der Hersteller noch keinen Patch zur Verfügung gestellt. Ein Exploit ist im Umlauf (in the wild) und über einschlägige Kanäle beziehbar. Die Interpretation von WMF/EMF-Dateien ist üblich, mitunter auch über HTML im Mail-Verkehr. Benutzer des Internet Explorer können bereits durch die Ansicht einer präparierten Datei in Mitleidenschaft gezogen werden. Das bedeutet eine Infizierung kann automatisiert umgesetzt werden. Benutzer alternativer Browser können durch das explizite Öffnen der Datei infiziert werden. Denselben Fehler, wie er in Windows anzutreffen war, wurde auch bei Wine übernommen. Dort wurde das Problem im CVS mit der Version 1.12 behoben.

Expertenmeinung:

Wiedereinmal eine schwerwiegende Lücke in hauseigener Software, hiess es. Erst diesen November wurde eine sehr kritische Pufferüberlauf Schwachstelle bei der Interpretierung von WMF Dateien rapportiert und per Patch behoben. Wiedereinmal sind Benutzer von HTML-Mails gefährdet. Dass es nun auch einen Emulator trifft, mutet da schon fast irgendwie komisch an.

3.10 IBM Lotus Domino bis 6.5.5 Server korruptes BMP-Bild Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 06.01.2006
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1956>

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. Wie IBM bekanntgab, existieren eine Reihe von Fehlern in den vergangenen Software-Versionen. Einer davon ist als Denial of Service auf den Server gegeben, wenn diese ein korruptes BMP-

Bild verarbeiten müssen. Weitere Details oder gar ein Exploit sind nicht bekannt. Der Fehler wurde in der Version 6.5.5 von IBM Lotus Domino behoben.

Expertenmeinung:

Werden in einem neuem Software-Release so viele Schwachstellen behoben, wie in dem jüngsten von Lotus, lohnt sich ein Upgrade allemal. Auf einen Schlag können so eine Vielzahl an Sicherheitslücken gestopft und das System wieder auf den neuesten Stand gebracht werden. Das Interesse der Angreifer ist ebenfalls als hoch anzusehen, da Lotus Domino eine enorme Verbreitung im professionellen Umfeld genießt und deshalb die Chancen, auf ein verwundbares System zu stossen, relativ hoch sind. Skript-Kiddies werden die Gunst der Stunde nutzen wollen und sich an den verwundbaren Systemen gütlich tun.

3.11 RIM BlackBerry Enterprise Server bis 4.0 Server Routing Protocol Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 30.12.2005
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1939>

BlackBerry ist eine kommerzielle Mobile-Lösung aus dem Hause Research In Motion Limited (RIM). Durch entsprechende BlackBerry-Handhelds kann stets ein Abgleich mit dem Enterprise Server umgesetzt werden, um stets bezüglich Emails und Terminen auf dem neuesten Stand zu sein. AM diesjährigen Congress des Chaos Computer Club (CCC) referierte Phenoelit über die Sicherheit von BlackBerry-Systemen. In ihrem Vortrag mit dem Titel "Blackberry: call to arms, some provided" haben sie einige grundlegende und kritische Schwachstellen des Produkts offengelegt. Eine davon ist eine Denial of Service-Schwachstelle des des Server Routing Protocols (SRP). Durch eine Manipulation über den Port tcp/3101 kann ein den Verbindungsabbruch zum Server und damit eine DoS umgesetzt werden. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Als Workaround wird empfohlen, dass der besagte Port mittels Firewalling geschützt wird.

Expertenmeinung:

Das BlackBerry-System ist auf dem Vormarsch und erste grossflächige Evaluierungen bzw. Integrationen haben begonnen. Schwachstellen wie diese fördern natürlich nicht den Verkauf der

RIM-Lösung. Vor allem ist dies wohl einer der ersten umfassenden Audits des Produkts, bei dem die Resultate ebenfalls der Öffentlichkeit zugänglich gemacht werden. Die Jungs von Phenoelit sind für ihre saubere Arbeit bekannt und dementsprechend war ihr Vortrag einer der Highlights des diesjährigen Congresses.

3.12 RIM BlackBerry Enterprise Server bis 4.0 Attachment Service TIFF-Anhänge Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 30.12.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1938>

BlackBerry ist eine kommerzielle Mobile-Lösung aus dem Hause Research In Motion Limited (RIM). Durch entsprechende BlackBerry-Handhelds kann stets ein Abgleich mit dem Enterprise Server umgesetzt werden, um stets bezüglich Emails und Terminen auf dem neuesten Stand zu sein. AM diesjährigen Congress des Chaos Computer Club (CCC) referierte Phenoelit über die Sicherheit von BlackBerry-Systemen. In ihrem Vortrag mit dem Titel "Blackberry: call to arms, some provided" haben sie einige grundlegende und kritische Schwachstellen des Produkts offengelegt. Eine davon ist eine Denial of Service-Schwachstelle des Attachment Service im Umgang mit korrupten TIFF-Anhängen. Dies verhindert es, dass die Attachments einer Nachricht angesehen werden können. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. RIM empfiehlt, dass der Attachment Service von der Interpretation von TIFF-Bildern ausgeschlossen wird.

Expertenmeinung:

Das BlackBerry-System ist auf dem Vormarsch und erste grossflächige Evaluierungen bzw. Integrationen haben begonnen. Schwachstellen wie diese fördern natürlich nicht den Verkauf der RIM-Lösung. Vor allem ist dies wohl einer der ersten umfassenden Audits des Produkts, bei dem die Resultate ebenfalls der Öffentlichkeit zugänglich gemacht werden. Die Jungs von Phenoelit sind für ihre saubere Arbeit bekannt und dementsprechend war ihr Vortrag einer der Highlights des diesjährigen Congresses.

3.13 Microsoft Windows korrupte WMF Dateien ermöglichen Code Execution

Einstufung: **sehr kritisch**

Remote: Ja
 Datum: 28.12.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1934>

Microsoft Windows ist die meistverwendete Betriebssystemreihe auf dem Globus. Eine bislang unbekannte Schwachstelle in der Windows Graphics Rendering Engine wurde gefunden. Betroffen sind die Windows Versionen 98, ME, 2000, XP und 2003. Durch das Ausnutzen dieser Verwundbarkeit könnte ein externer Angreifer in der Lage sein willkürlich Code auf dem infizierten Rechner auszuführen. Dies mit den Rechten des Benutzers. Bekannt ist, dass sich die Schwachstelle einen Fehler in der Abhandlung korrupter Windows Metafile Dateien (.wmf) zu Nutze macht. Bislang hat der Hersteller noch keinen Patch zur Verfügung gestellt. Ein Exploit ist im Umlauf (in the wild) und über einschlägige Kanäle beziehbar. Die Interpretation von WMF/EMF-Dateien ist üblich, mitunter auch über HTML im Mail-Verkehr. Benutzer des Internet Explorer können bereits durch die Ansicht einer präparierten Datei in Mitleidenschaft gezogen werden. Das bedeutet eine Infizierung kann automatisiert umgesetzt werden. Benutzer alternativer Browser können durch das explizite Öffnen der Datei infiziert werden.

Expertenmeinung:

Wiedereinmal eine schwerwiegende Lücke in hauseigener Software. Erst diesen November wurde eine sehr kritische Pufferüberlauf Schwachstelle bei der Interpretierung von WMF Dateien rapportiert und per Patch behoben. Wiedereinmal sind Benutzer von HTML-Mails und der Maillösung von Microsoft Exchange/Outlook besonders gefährdet. Ein präpariertes Mail genügt zur Ausführung des Schadcodes. Da nützt auch nichts, wenn der Standardbrowser z.B. Mozilla ist. Outlook interpretiert HTML Dateien mit den hauseigenen IEX Routinen. Gleiches gilt für Groupware welche ebenfalls auf die von Microsoft zur Verfügung gestellte .dll zugreifen (z.B. Notes). Ein gefundenes Fressen für explizite Angriffe und leider auch für ScriptKiddies. Vorallem in der Jahresendzeit (Abschlussbuchungen, Abschlüsse etc.) sind Systemänderungen kaum durchführbar, respektive die Implementierung spezifischer strengerer Regeln auf Sicherheitssystemen. Wer möchte schon an der Behinderung der Abschlussbuchungen schuld sein? In der Windowswelt ist leider nicht alles transparent.

3.14 Vmware verschiedene Produkte

NAT korrupte FTP-Anfragen Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 21.12.2005
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1933>

Vmware ist eine kommerzielle Lösung, mit deren Hilfe auf einem System virtuelle Systeme betrieben werden können. Es existiert ein schwerwiegender Fehler in der NAT-Verarbeitung der Lösung (vsnat.exe bei Windows und vnet-natd bei Linux). Durch ein korruptes Kommando über einen FTP-Datenkanal kann ein Pufferüberlauf umgesetzt und mit diesem beliebiger Programmcode innerhalb des Muttersystems ausgeführt werden. Das grundlegende Vorgehen wurde diskutiert. Ein umfassender Exploit ist jedoch noch nicht bekannt. Vmware empfiehlt das deaktivieren des NAT-Modus oder das Einspielen der neuesten Vmware-Versionen.

Expertenmeinung:

Diese Schwachstelle ist höchst interessant, erlaubt sie einem Angreifer nämlich das Ausbrechen aus dem virtuellen System. Besonders in Umgebungen, in denen komplexe virtuelle Dienste angeboten werden, kann dies nützlich sein. Gerade weil die Möglichkeit eine solche Brisanz mit sich bringt, sollte in exponierten Umgebungen über schnellstmögliche Gegenmassnahmen nachgedacht werden. Das Update auf die jüngste Vmware-Version bietet sich an.

3.15 Symantec verschiedene AntiVirus Produkte korruptes RAR-Archiv entpackten Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 20.12.2005
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1931>

Symantec gilt momentan als grösste Security-Firma weltweit. Es gibt praktisch keine Produkt-Richtung, die sie nicht durch eingekaufte oder selber entwickelte Lösungen abdecken. Ein wichtiger Bestandteil spielen dabei die Antiviren-Lösungen, die sich sowohl als Client- als auch als Server-Installationen finden. Wie nun bekannt wurde, existiert in der genutzten Bibliothek Dec2Rar.dll vor den Versionen 3.2.14.3 eine Pufferüberlauf-Schwachstelle beim Entpacken von korrupten RAR-Archiven. Dies kann dazu führen, dass beliebiger Programmcode initiiert

wird. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Als Workaround wird empfohlen, RAR-Dateien frühzeitig mittels Firewalling und Filtern vor der Verarbeitung betroffener Symantec-Produkte zu unterbinden.

Expertenmeinung:

Diese Schwachstelle hat erstaunlicherweise kein grösseres Aufsehen erregt. Dies obschon sämtliche Antiviren-Lösungen von Symantec betroffen sind. Das Problem bei der Verarbeitung korrupter Dateien und vor allem Archiven ist hingegen nichts neues. Es scheint, als müssten die Entwickler von Antiviren-Lösungen in der Hinsicht von weit mehr defensiver programmieren. Es ist nur eine Frage der Zeit, bis aktuelle Schädlinge, vor allem Mail-Viren, die Schwachstelle für sich ausnutzen wollen. Das Umsetzen von Gegenmassnahmen ist deshalb dringendst zu empfehlen.

4. Statistiken Verletzbarkeiten

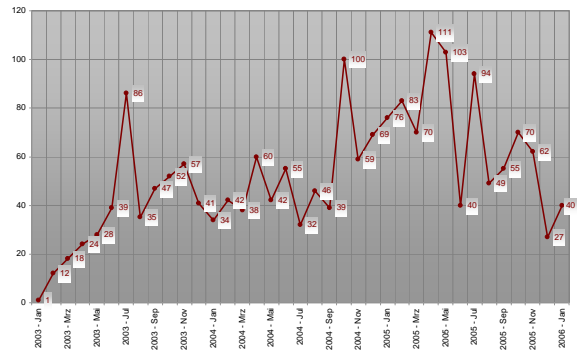
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



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

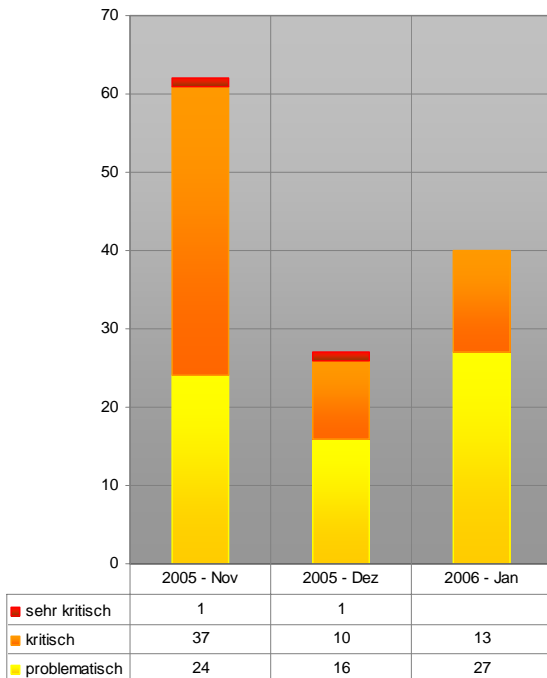
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

Registrierte Schwachstellen by scip AG

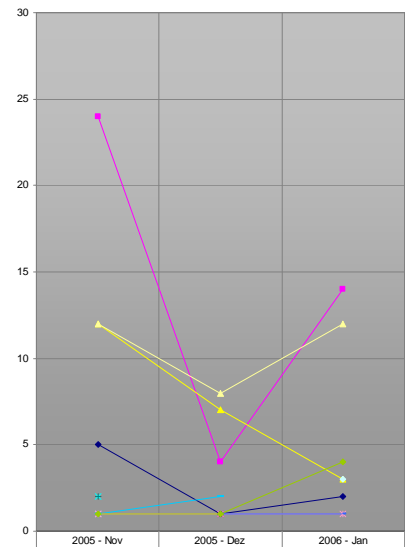


Verlauf der Anzahl Schwachstellen pro Monat

Auswertungsdatum: 19. Januar 2006



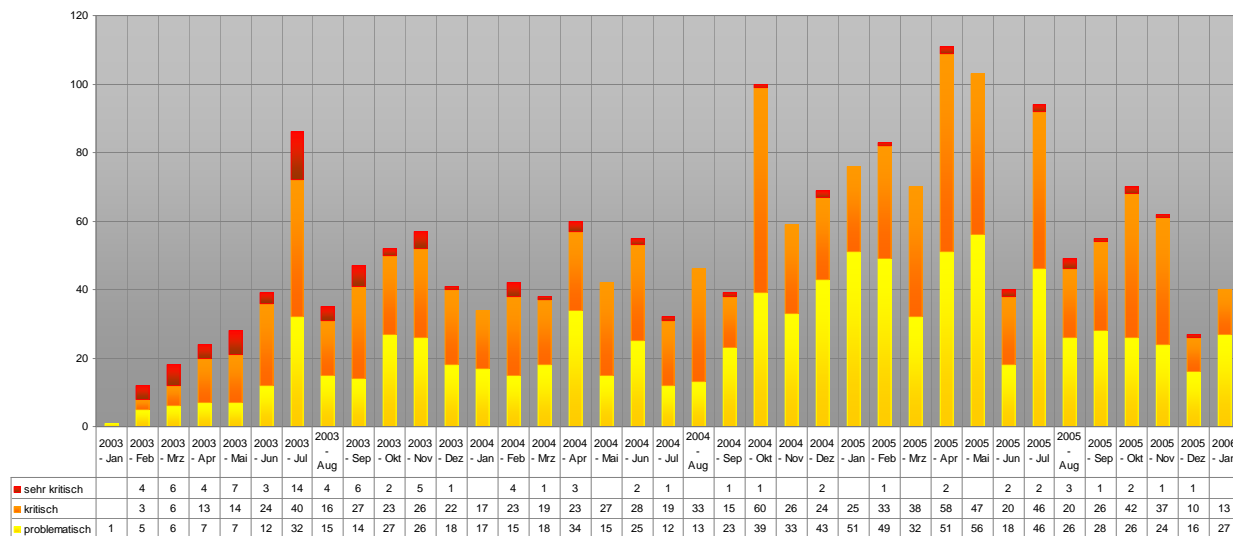
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



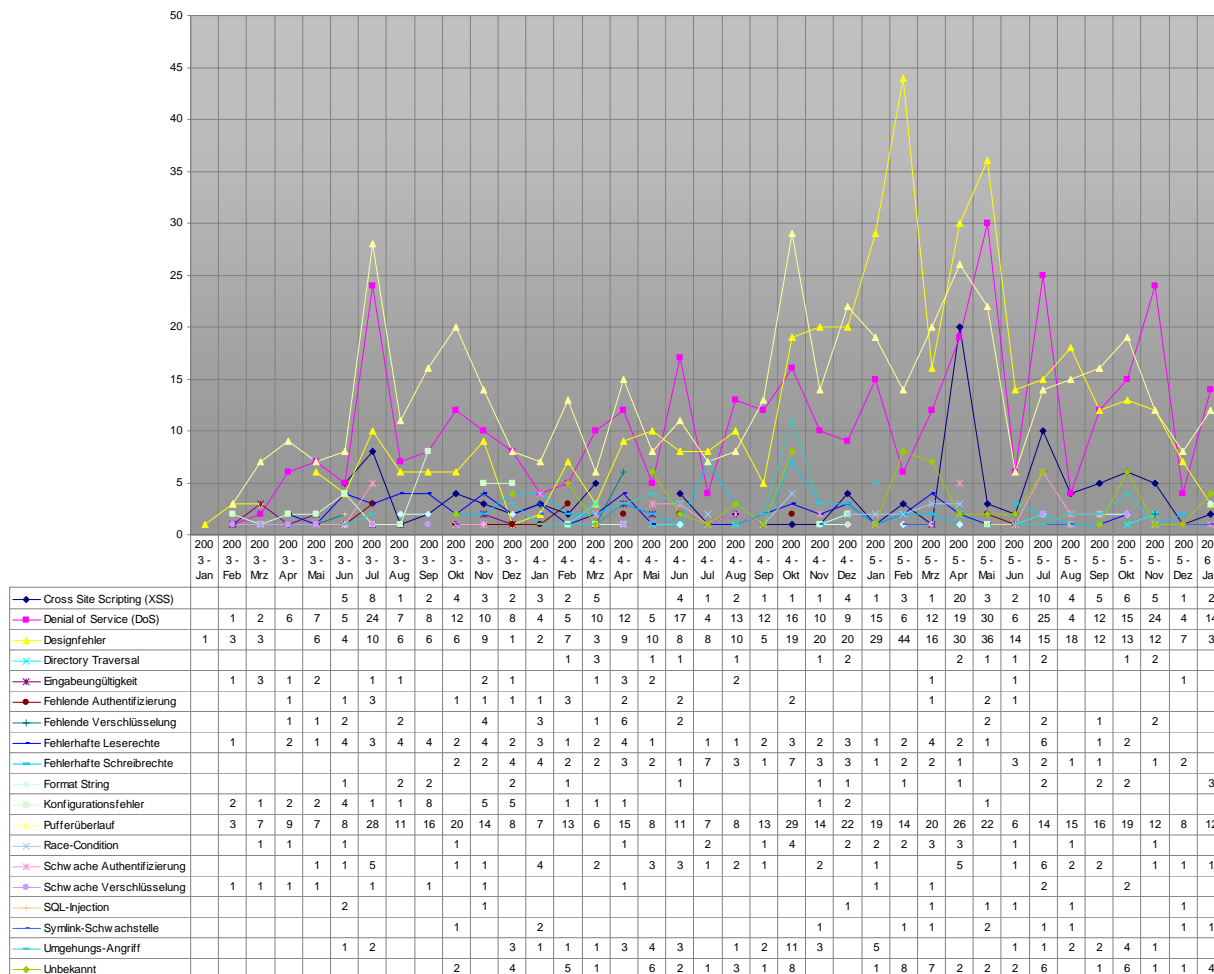
Kategorie	2005 - Nov	2005 - Dez	2006 - Jan
Cross Site Scripting (XSS)	5	1	2
Denial of Service (DoS)	24	4	14
Designfehler	12	7	3
Directory Traversal	2		
Eingabeungültigkeit		1	
Fehlende Authentifizierung			
Fehlende Verschlüsselung	2		
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte	1	2	
Format String			3
Konfigurationsfehler			
Pufferüberlauf	12	8	12
Race-Condition	1		
Schwache Authentifizierung	1	1	1
Schwache Verschlüsselung			
SQL-Injection		1	
Symlink-Schwachstelle		1	1
Umgehungs-Angriff	1		
Unbekannt	1	1	4

Verlauf der letzten drei Monate Schwachstelle/Kategorie





Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat



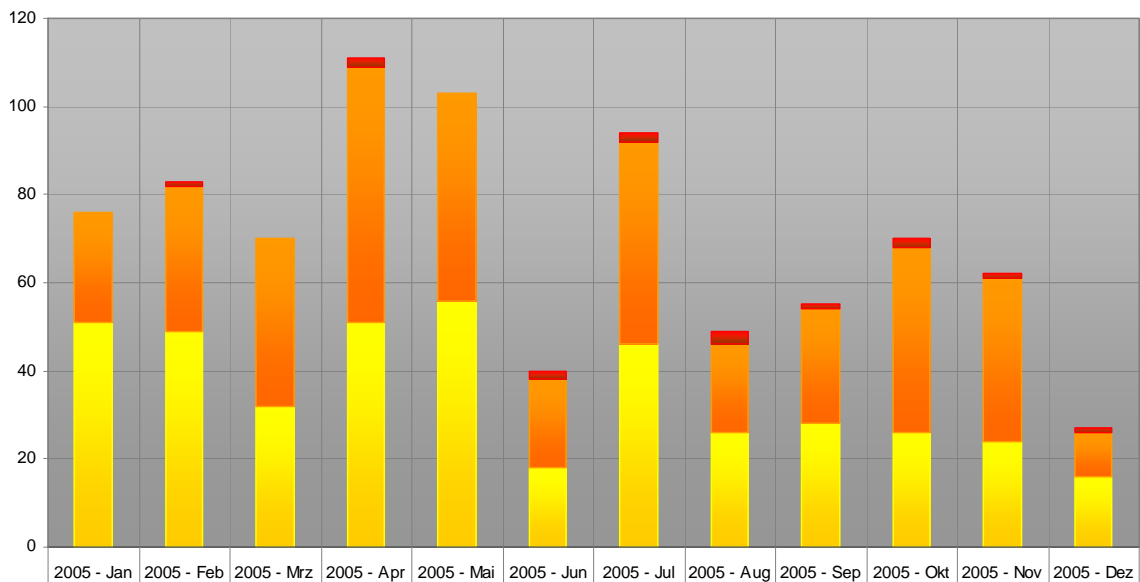
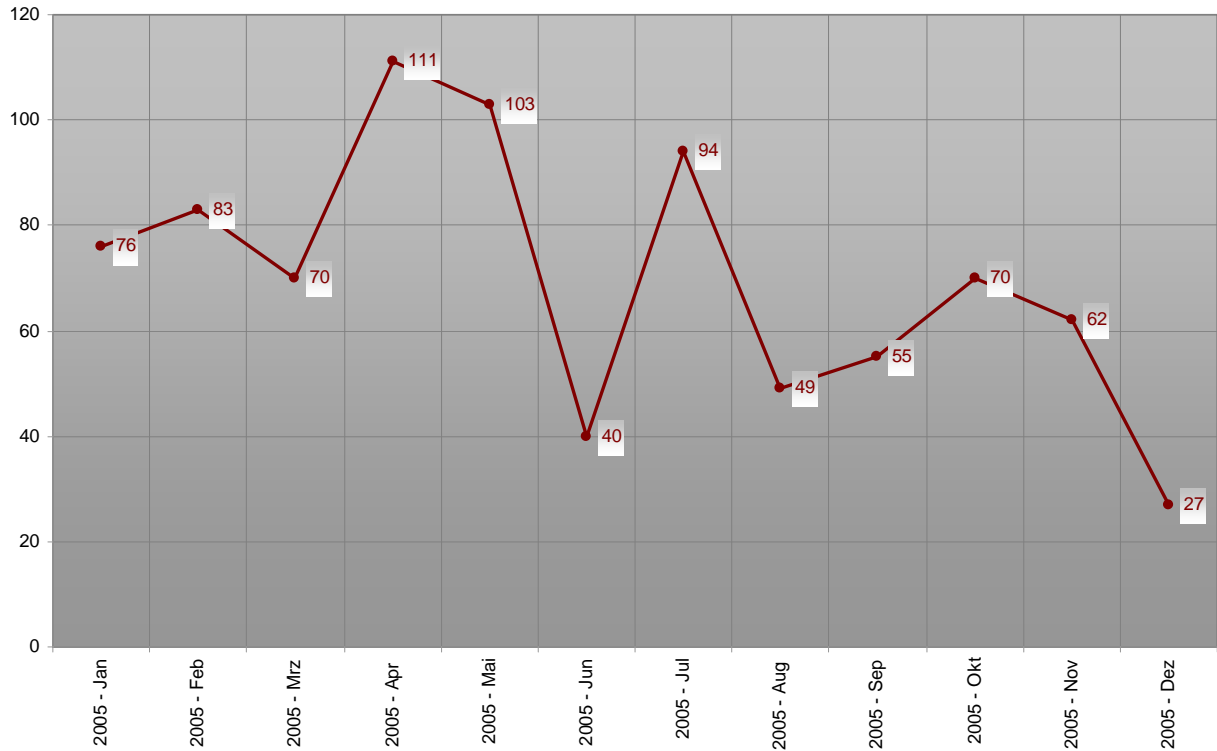
Verlauf der Anzahl Schwachstellen/Kategorie pro Monat

scip monthly Security Summary 19.01.2006



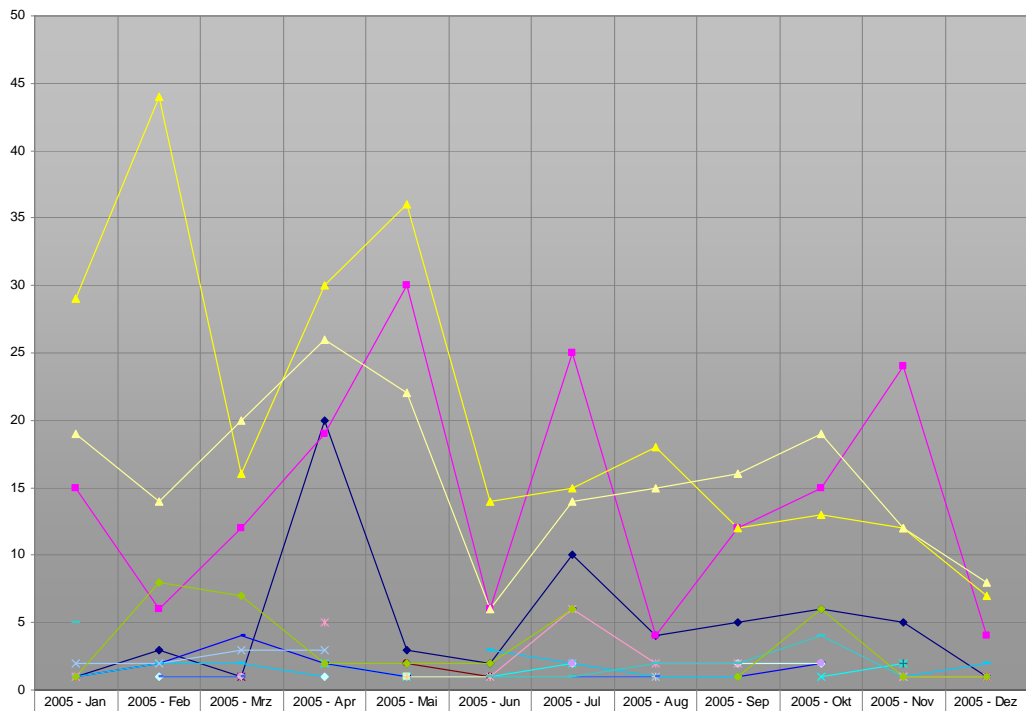
4.1 Verletzbarkeiten 2005

Registrierte Schwachstellen by scip AG



	2005 - Jan	2005 - Feb	2005 - Mrz	2005 - Apr	2005 - Mai	2005 - Jun	2005 - Jul	2005 - Aug	2005 - Sep	2005 - Okt	2005 - Nov	2005 - Dez
■ sehr kritisch		1		2		2	2	3	1	2	1	1
■ kritisch	25	33	38	58	47	20	46	20	26	42	37	10
■ problematisch	51	49	32	51	56	18	46	26	28	26	24	16





	2005 - Jan	2005 - Feb	2005 - Mrz	2005 - Apr	2005 - Mai	2005 - Jun	2005 - Jul	2005 - Aug	2005 - Sep	2005 - Okt	2005 - Nov	2005 - Dez
◆ Cross Site Scripting (XSS)	1	3	1	20	3	2	10	4	5	6	5	1
◆ Denial of Service (DoS)	15	6	12	19	30	6	25	4	12	15	24	4
▲ Designfehler	29	44	16	30	36	14	15	18	12	13	12	7
✕ Directory Traversal				2	1	1	2			1	2	
✕ Eingabeungültigkeit			1			1						1
● Fehlende Authentifizierung			1		2	1					2	
✕ Fehlende Verschlüsselung					2		2		1			
◆ Fehlerhafte Leserechte	1	2	4	2	1		6		1	2		
◆ Fehlerhafte Schreibrechte	1	2	2	1		3	2	1	1		1	2
◆ Format String		1		1			2		2	2		
◆ Konfigurationsfehler					1							
▲ Pufferüberlauf	19	14	20	26	22	6	14	15	16	19	12	8
✕ Race-Condition	2	2	3	3		1		1			1	
✕ Schwache Authentifizierung	1			5		1	6	2	2		1	1
◆ Schwache Verschlüsselung	1		1				2			2		
◆ SQL-Injection			1		1	1		1				1
◆ Symlink-Schwachstelle		1	1		2		1	1				1
◆ Umgehungs-Angriff	5					1	1	2	2	4	1	
◆ Unbekannt	1	8	7	2	2	2	6		1	6	1	1

5. Interview

5.1 Interview mit Lutz Donnerhacke – Mitgründer des Fördervereins Informationstechnik und Gesellschaft (Fitug)

Marc Ruef, <mailto:maru@scip.ch>
Lutz Donnerhacke, <mailto:lutz@iks-jena.de>

scip AG: Hallo Lutz. Vielen Dank, dass Du Dir die Zeit für dieses Interview nimmst. Dein Name ist seit Jahren unweigerlich mit der (deutschsprachigen) "Hacker-Kultur" verbunden. Betrachtet man in diesem Belang Deinen Werdegang, ist er sehr klassisch. Was findest Du, hat sich jedoch seit den Zeiten von C64, Zak McCracken und 5,25"-Floppy-Disks verändert?

Lutz Donnerhacke: Die Grundlagenkenntnisse sind verloren gegangen. Der Einstieg für heutige Technikinteressierte findet auf einem so hohen Niveau statt, dass nur noch in seltenen Ausnahmefällen der Interessent die relevanten Detailkenntnisse erwirbt oder erwerben will.

Dies betrifft besonders die Programmierkenntnisse, aber auch die Kenntnisse von Protokollen. Im Ergebnis sieht man heute viele Leute blind irgendwas probieren, anstatt systematisch Ursachen und Wirkungsweisen abzuklopfen. Es gipfelt darin, dass zufällig funktionierende Handlungsweisen wie Voodoo-Rituale gehandelt und in den verschiedensten Zeitschriften abgedruckt werden.

Besonders schlimm ist jedoch, dass durch das fehlende Verständnis zunehmend wieder unsichere oder schlecht performante Software erstellt wird, ja sogar unsichere Algorithmen und Protokolle neu entwickelt werden.

In Bezug auf Computersicherheit konnte vor allem im Umgang mit neuen Schwachstellen und wie diese Veröffentlicht werden eine Veränderung festgestellt werden: Bugtraq wurde zunehmend unspektakulär und spannende Diskussionen werden immer spärlicher. Hat das Genre IT-Security ein bisschen seinen Reiz verloren?

Nein, im Gegenteil. Der beobachtete Rückgang öffentlicher, sicherheitsrelevanter Informationen ist in der Vermeidung der Öffentlichkeit zu suchen. Sicherheit und selbst Diskussionen darüber sind knallhartes, ökonomisches Geschäft geworden. Das macht das Thema eigentlich nur

noch spannender.

Die Massenmedien pflegen den Begriff "Hacker" in anderen Zusammenhängen zu nutzen, weder er ursprünglich eingeführt wurde. Bedauerst Du dies oder ist es lediglich eine übliche Entwicklung der Popularisierung einer Subkultur? Was verstehst Du unter einem Hacker? Welches sind für Dich die "grossen Hacker"?

Die strenge Unterscheidung zwischen "Hacker", "Cracker" und "Crasher" ist ein typisch deutsches Phänomen. Das Definitionsmonopol des Chaos Computer Clubs erlaubte damals eine positive Konnotation des Wortes "Hacker" einzuführen und zeitweilig in der Sprache zu verankern. Internationales Journalistentum kann und wird eine Gleichschaltung der Bedeutungsebenen solcher Begriffe erreichen, schon allein, um überhaupt zuverlässig kommunizieren zu können.

„Die strenge Unterscheidung zwischen Hacker und Cracker ist ein typisch deutsches Phänomen.“

Der Fachbegriff "Hacker" ist also dabei, sich auf einem Begriffsniveau einzupegeln. Die deutsche Sonderbehandlung führt jedoch auch international zu einer etwas besseren ethischen Einstufung des Begriffs. Viel mehr konnte man nicht erwarten.

Für mich ist ein Hack etwas, das besonders kreativ Technik zweckentfremdet. Meistens verdienen besonders elegante oder besonders effiziente Algorithmen diese Bezeichnung. Sicherheitstechnisch betrachtet sind die Zweckentfremdungen der Hacks schlichte Hintertüren durch gezielte Fehlfunktionen.

Vorbilder zu benennen ist schwer. Neben Wau ist aktuell Florian Weimer zu nennen.

Der Förderverein Informationstechnik und Gesellschaft e.V. propagiert die menschen-nahe "Demokratie im Netz", die auf bürokratische Regelungen verzichten möchte, um ein Höchstmass an Effizienz und Humanismus gewährleisten zu können. Wo hört für Dich aber Meinungsfreiheit auf und wo sind Regulierungen erforderlich?

Persönlich halte ich Regulierungen für erforderlich, um Einschränkungen der Meinungsfreiheit zu verhindern. Meinungsfreiheit gliedert sich

dabei in zwei Teilbereiche: Meinungsäusserungsfreiheit und Rezipientenfreiheit.

Die Meinungsäusserungsfreiheit ist mit dem Internet schon weit gediehen, denn praktisch jeder kann seinen eigenen Webserver o.ä. betreiben. Leider ist zunehmend die Einschränkung dieser Meinungsfreiheit zu beobachten: Es ist schwieriger geworden, feste IP-Adressen und ungefilterte Zugänge zu bekommen. Die Access-Provider versuchen durch Einschränkung der eigenbetriebenen Server ein Zusatzgeschäft mit Webpace und co. zu generieren.

Rezipientenfreiheit wird leider zu wenig beachtet. Statt dessen versucht man mittlerweile das Recht auf freien Erhalt von Information auch auf dem Transportweg zu beschneiden. Es werden ganze Teile des Internet ausgeblendet, wenn irgendwo IP-Sperren oder gar Contentfilter zum Einsatz kommen. Bedenklich ist auch die Willkür, mit der Suchmaschinenbetreiber Informationen unterdrücken. Hier tut eine Regulierung hin zu mehr Transparenz not.

Um es platt zu sagen: Die Wiedereinführung des Feindsenderverbots ist Demokratieschädlich.

Kritiker werfen Wissenschaftlern mit Hang zu hypothetischen Betrachtungen gerne vor, dass diese lediglich vor der Wirklichkeit und ihren realen Problemen flüchten wollen. Wie stellst Du als Analytiker und Denker einer solchen Kritik gegenüber?

Kürzlich habe ich Joseph Weizenbaum erlebt und etwas mit ihm reden können. Er ist zu der bemerkenswerten Erkenntnis gelangt, dass die Probleme der Welt quantisiert vorgebracht werden, also in handlichen Bruchstücken ohne grossen Zusammenhang. Dadurch geht die Priorisierung der Probleme verloren, man beschäftigt sich lieber mit unwichtigen Dingen, wie z.B. mit einem Interview.

Aufgrund meiner mathematischen Ausbildung habe ich wenig Schwierigkeiten damit, Probleme gar nicht global zu priorisieren. Es gibt halt verschiedene Halbordnungen und ich benutze die, die mir momentan am besten hilft. Das ändert sich gern auch mehrfach pro Stunde.

Im aktuellen Kontext möchte ich aber anmerken, dass die Probleme der Meinungsfreiheit und des Datenschutzes sehr reale Betrachtungen darstellen.

Die Regierungen und ihre Organe sind seit

jeher darum bemüht, im Falle eines Informationskriegs die Oberhand behalten zu können. Die Folgen davon sind Restriktionen im Umgang mit kryptografischen Methoden. Wie empfindest Du derlei Bestrebungen?

Ich kann derzeit keine Einschränkungen bei kryptografischen Algorithmen feststellen. Ein politischer Hack ist jedoch die französische Regelung, die Krypto verbietet und das Verbot per Durchführungsbestimmung auf irrelevant grosse Schlüssellängen beschränkt. Dies verlagert das Kryptoverbot aus dem Bereich der Legislative in den Bereich der Exekutive. Cool.

Wesentlich mehr Schwierigkeiten machen die Regelungen zum "geistigen Eigentum". Hier wird nachhaltig die Entwicklung und der Fortbestand von Informationsverarbeitungssystemen untergraben.

„Meinungsfreiheit gliedert sich dabei in zwei Teilbereiche: Meinungsäusserungsfreiheit und Rezipientenfreiheit.“

Denkst Du, dass Quantenkryptografie eine Zukunft hat?

Quantenkryptografie im Sinne der öfter besprochenen abhörsicheren Leitungen hat ein sehr begrenztes Einsatzfeld ohne Massenzukunft. Erfolge der Quantencomputer sind dagegen geeignet im Massenmarkt gravierende Umwälzungen anzustossen, ich halte diese in den nächsten zehn Jahren jedoch nicht für sonderlich praxisrelevant.

Wird bei Quantenkryptografie nicht lediglich die Abhörsicherheit gegen die Anfälligkeit von Denial of Service-Attacken mittels Abhören eingetauscht und somit das Verfahren unwirtschaftlich gemacht?

Zum einen ist die Abhörsicherheit entgegen der ursprünglichen Versprechungen nicht zu halten. Zum anderen ist der Einsatzbereich so speziell, dass die betroffenen Strecken ausreichend überwacht werden können, d.h. das Erkennen des Lauschers zu einer schnellen Ergreifung führt.

Zu DDR Zeiten hatte die Rote Armee Kabel in Druckluftrohren verlegt. Beim Anbohren eines solchen Rohres konnte man durch Frequenzmessung der auftretenden stehenden Wellen (wie bei einer Flöte) den Ort des Angriffs sofort

ermitteln und den Zugriff organisieren. Sehr effektiv, ziemlich teuer und nur für Spezialfälle geeignet. Wie Quantenkryptografie.

IPv6 schimmert seit Jahren am Horizont. Was denkst Du, welche Auswirkungen wird die Einführung der neuen Protokollgeneration auf die Welt und ihre digitale Sicherheit haben?

IPv6 ist ein wesentlicher Beitrag zur Meinungsäusserungsfreiheit. Damit wird es möglich, Informationen direkt und ungefiltert anzubieten. Wir (als ISP) haben sehr positive Erfahrungen mit IPv6 im Backbone, für Server und Arbeitsplätze gemacht.

Seitens der Sicherheit ist hervorzuheben, dass man deutlich leichter das verwurmete Endgerät ermitteln kann, als im klassischen PAT Fall. Dies ermöglicht schnellere und genauere Reaktionen. Ebenso sind Filterlisten deutlich besser gerätebezogen definierbar, insbesondere für Laptops.

RFID ist in aller Munde. Über Risiken wird jedoch, wie gewohnt, in den Massenmedien wenig debattiert. Wird sich das Wardriving in Zukunft nicht mehr nur auf WLANs beschränken, sondern vorwiegend auf die kontaktlosen Chipkarten abzielen? Ist es dann wohl schon zu spät?

Es ist zu spät. RFID ist allerdings nur eines von vielen Trackingsystemen, die die Privatsphäre der Bürger ausspionieren. Solange jedoch die Bürger selbst immer weiter ausspioniert werden wollen (siehe Payback), ist ein Aufbegehren gegen die Industrie sinnfrei. Mündigen Bürgern folgt die Industrie von allein: Man sehe sich nur an, dass UnCDs in England kein Thema sind, weil sie nicht akzeptiert werden.

Computerkritiker wie Joseph Weizenbaum postulieren, dass sich der moderne Mensch kritisch mit der Technik, den Medien und Informationen auseinandersetzen hat, um damit quasi die Mündigkeit in einem technokratischen Zeitalter zu erreichen. Denkst Du, dass dies überhaupt von einer Konsumgesellschaft wie der unseren verlangt werden kann? Falls ja, bleibt dieses Ziel überhaupt erreichbar?

Es kann und muss verlangt werden. Medienkompetenz ist gerade im Rahmen der Meinungsfreiheit wichtig. Menschen, die nicht in der Lage sind, Informationen abzuwägen, ziehen ein re-

daktionell bearbeitetes "Internet" vor, also befürworten Einschränkungen der Rezipientenfreiheit.

Und zum Schluss noch die etwas andere Frage: Wenn Du einen eigenen Staat gründen würdest, welche drei Dinge würdest Du dem Volk frei oder möglichst billig zur Verfügung stellen wollen?

Wir (Thüringen Netz e.V.) hatten vor nunmehr 10 Jahren mal einen Staatsgründung des Internets mit den entsprechenden Juristen durchdiskutiert. Es geht. Es würde Spass machen. Es macht unheimlich viel Arbeit. Man muss vielzuviel "unwichtigen" Kram erledigen. Es macht keinen Spass.

„Medienkompetenz ist gerade im Rahmen der Meinungsfreiheit wichtig.“

Das, was an der Staatsgründung keinen Spass macht, ist die umfassende Verantwortung für den Bürger. Deswegen hat Vatikanstadt keine Staatsangehörigen. Ohne Bürger ist die Frage jedoch auch wieder sinnfrei. (*lacht*)

Vielen Dank für Deine Zeit sowie das interessante Interview. Und viel Glück für die Zukunft Deiner interessanten Projekte.

Danke.

7. Literaturverzeichnis

scip AG, 2003, scip monthly Security Summary, Ausgabe Oktober 2003

http://www.scip.ch/publikationen/smss/scip_mss-19_10_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 Ruef

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 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. 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.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das **Errata** (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summaries finden Sie online.

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