

Contents

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

1. Editorial

Sicherheit kennt keine Freiheit

Vor wenigen Wochen war ich bei der Niederlassung einer Bank in Basel. Im Rahmen eines überregionalen Penetration Tests wurde ich vom technischen Personal in die Umgebung vor Ort eingeführt. Da werden mir dann Netzwerkdiagramme und IP-Adresslisten vorgezeigt, über eingesetzte Betriebssysteme sowie Applikationen diskutiert.

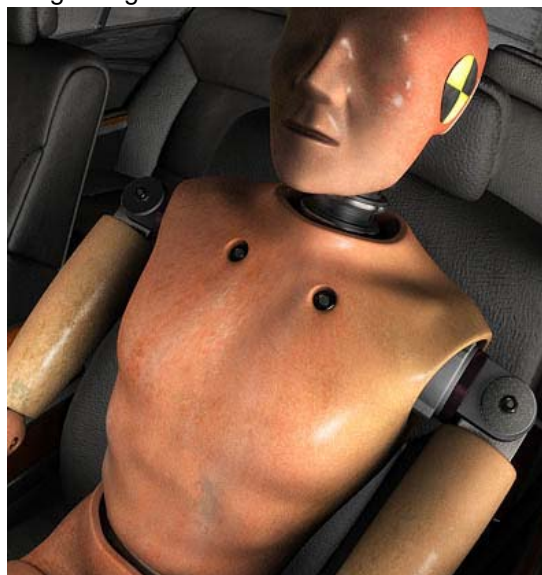
Bei dieser frühen Phase eines Audit Projekts nutze ich oftmals die Gelegenheit, die involvierten Personen auch etwas ausserhalb ihres Berufsbereichs kennenzulernen. Trägt ein Security Officer anstatt Anzug und Krawatte sportliche Fila-Schuhe und finden sich im Regal neben Cisco-Büchern und SuSE-CDs auch eine Schachtel Golfbälle, ist die Frage nach Platzreife und Handicap schon fast ein Muss.

Bei ungezwungenen Gesprächen auf dieser Ebene lernt man oftmals das wahre Naturell ei-

ner Person viel schneller kennen. Ausserdem kann man der Ernsthaftigkeit, die eine Sicherheitsüberprüfung halt so mit sich bringt, ein bisschen entschärfen. Genau so macht es nämlich auch mein Hausarzt, der darin ein wahrer Meister zu sein scheint. Muss ich aufgrund eines neuerlichen oder alten Leidens an ihn herantreten, stehen meine Beschwerden nur selten oder wenigstens kurz im Vordergrund. Politik und Gespräche eines Arztes aus dem Nähkästchen interessieren oftmals mehr weder eine anstehende Magenspiegelung oder dergleichen.

Eine meiner semi-privaten Standard-Fragen ist diejenige nach dem allgemeinen Wohlbefinden mit dem gegenwärtigen Sicherheitsdispositiv. So mancher klagt über schwermütige Prozesse bei der Antragsverarbeitung zu einer neuen Firewall-Komponente oder man ärgert sich über die fehlende Heterogenität/Homogenität der eingesetzten Betriebssystem-Landschaft. Die Sorgen sind alle anders und doch irgendwie gleich.

Auf eben meine Frage erhielt ich jedoch in der Situation eine Antwort, die ich so nicht erwartet hätte. Mein Gegenüber meinte, dass er sich wie ein Verbrecher vorkomme. Und zwar weil in der



Bank extreme Sicherheitsregulierungen und -restriktionen herrschen, wie ich sie selten gesehen habe. Nur eine Bank ist mir bekannt, die da gar noch einen Tick extremer ist. Aber beide Kunden sind auf höchstem Niveau, stellen in manchen Bereichen ungeniert die Sicherheit über die Produktivität. Der Security Consultant in mir will da natürlich jubeln.

Dieses Gespräch zeigte mir aber auf, dass Sicherheit in jeglicher Hinsicht immer auf Kosten der Freiheit geht. Die Gefahr eines Systems, egal ob sozialer oder technischer Natur, liegt in den Risiken der Möglichkeiten. Es verwundert ja niemanden, dass Diktatoren als erstes oppositionelle Gesinnungen verbieten. So minimieren sie das Risiko einer (un-)kalkulierbaren Gegenbewe-

gung, die ihren Standpunkt gefährden könnte.

In der Computersicherheit geht es nicht viel anders zu und her. Da ist der Diktator aber entweder die Gesetzesgebung, die Geschäftsleitung, der Security Officer oder der Administrator, der zur Wahrung seiner Ziele die Möglichkeiten der Opposition einschränkt. Und zur Opposition wird alles gezählt, was irgendwie gefährlich werden könnte. Da Computerkriminalität ein Phänomen, alleine hervorgerufen durch den Menschen, darstellt, wird eben jeglicher Benutzer um seine Freiheiten beraubt werden müssen. Ein System ist sodann nur 100 % sicher, wenn 0 % Freiheiten gegeben sind. Nur bleibt es dann oftmals nicht betreibbar und verliert so seinen eigentlichen Sinn. Da jubelt dann irgendwie auch nicht mehr der Security Consultant in mir.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 07. November 2005

für Computersicherheit wurde Herr Marc Ruef in den Büroräumlichkeiten der scip AG interviewt.

2.2 Computerworld - Developerworld

In der integrierten Beilage für Entwickler (Developerworld) der Computerworld Ausgabe vom 21. Oktober 2005 (<http://www.computerworld.ch>) finden Sie den Artikel: „Social Hacking mit technischen Hilfsmitteln stoppen“ von Marc Ruef der scip AG. Im Artikel werden ausgesuchte Angriffsformen erläutert und konkrete Gegenmassnahmen empfohlen.



Den Artikel finden Sie online als PDF unter <http://www.computec.ch/download.php?view.690>

2. scip AG Informationen

2.1 Phishing in SFDRS Sendung 10 vor 10

Der erneute Phishing Angriff auf die Postfinance im Oktober 2005 veranlasste das Nachrichtenformat 10 vor 10 des staatlichen schweizerischen Fernsehens SFDRS (<http://www.sfdrs.ch>), vergleichbar mit dem Heute Journal des ZDF (<http://www.zdf.de>), einen Beitrag dazu zu erstellen und am 25. Oktober 2005 auszustrahlen.

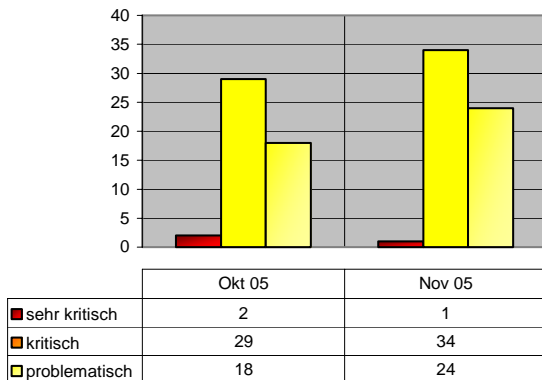


Da die scip AG im Verlauf ihrer Tätigkeiten und Aufträge oft mit den entsprechenden Techniken konfrontiert wird und diese in eigenen Projekten und in Absprache mit den Auftraggeber selbst anwendet wurde sie gebeten die vorliegende Phishing Attacke zu analysieren. Als Spezialist

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 2000 und XP SP1 UPnP GetDeviceList Denial of Service
- 3.2 Cisco IP Phone 7900 Serie SNMP Standardkonten
- 3.3 Microsoft Internet Explorer bis 6.0 Bild mit Link-Verkapselung Destination vortäuschen
- 3.4 CheckPoint Firewall-1 bis R55P IPsec IKEv1 korruptes Paket Denial of Service
- 3.5 Sun Solaris 9 und 10 in.iked IPsec IKEv1 korruptes Paket Denial of Service
- 3.6 Cisco IOS bis 12.4T IPsec IKEv1 korruptes Paket Denial of Service
- 3.7 sudo bis 1.6.8p12 Perl Environment aufräumen Umgebungsvariablen erweiterte Rechte
- 3.8 RealNetworks RealPlayer bis 10.5 DUNZIP32.DLL korrupte RJS Skin-Datei Pufferüberlauf
- 3.9 SAP Web Application Server bis 7.00 fameset.htm sap-syscmd Cross Site Scripting
- 3.10 SpamAssassin bis 3.0.4 Message.pm reguläre Ausdrücke lange Header Denial of Service
- 3.11 Veritas NetBackup bis 5.1 vmd-Bibliothek Pufferüberlauf
- 3.12 Microsoft Windows 2000 und XP korrupte

WMF/EMF-Datei Pufferüberlauf

- 3.13 Macromedia Flash Player bis 8.0.22.0 SWF-Datei Frame Type Identifier Pufferüberlauf
- 3.14 IBM Lotus Domino bis 6.5.4 Fix Pack 2 Domino Web Access fehlerhafte URL Denial of Service
- 3.15 Apache Tomcat bis 5.5.12 Directory Listing Denial of Service
- 3.16 Cisco Wireless LAN Controller LWAPP Verschlüsselung umgehen
- 3.17 NetBSD bis 2.1 setuid-Programme ptrace() erweiterte Rechte
- 3.18 PHP bis 5.0.5 HTTP POST GLOBALS globale Variablen erweiterte Rechte
- 3.19 RSA ACE/Agent bis 5.1.1 webauthentication GetPic Cross Site Scripting
- 3.20 Skype bis 1.4.0.83 skype:// und callto:// URI Pufferüberlauf

3.1 Microsoft Windows 2000 und XP SP1 UPnP GetDeviceList Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 16.11.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1909>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Es existieren Versionen für den Einsatz als Server und solche für den Workstation-Betrieb. Microsoft weist im Security Advisory 911052 auf einen älteren Fehler in UPnP hin. Dort kann mit dem Heranziehen des GetDeviceList-Befehls die CPU-Auslastung von services.exe auf 100 % getrieben und damit eine Denial of Service initiiert werden. Ein Exploit zur Schwachstelle wurde schon öffentlich gemacht. Um das Problem auszunutzen, muss jedoch ein funktionierendes Netzwerkkonto auf dem Zielsystem gegeben sein. Der Fehler betrifft Microsoft Windows 2000 und XP mit installiertem Service Pack 1. Das Problem kann auf XP also mit dem Heranziehen des Service Pack 2 behoben werden. Alternativ wird der Einsatz von Firewalling empfohlen.

Expertenmeinung:

Derlei Implementierung durch Microsoft sind stets ein Sorgenkind der vielen Windows-Anwender. Einmal mehr zeigt sich, dass mit wenig Aufwand ein verwundbares Betriebssystem negativ beeinträchtigt werden

kann. Dieses Mal ist es zum Glück nur eine Denial of Service-Attacke über den UPnP-Dienst. Weitaus schlimmer wären konstruktive Angriffe (z.B. Pufferüberlauf) gewesen. Auch weiterhin sollte man sich dafür einsetzen, unnötigen Datenverkehr zu unterbinden (z.B. durch entsprechende Firewall-Regeln).

3.2 Cisco IP Phone 7900 Serie SNMP Standardkonten

Einstufung: **kritisch**
 Remote: Ja
 Datum: 17.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1907>

Die Firma Cisco hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Cisco liefert zudem ein breites Portfolio an IP-Telefonen, um die Vorteile der IP-basierten Telefonie in allen Geschäftsbereichen nutzen zu können. Wie der Hersteller im Advisory cisco-sa-20051116-7920 eingesteht, bestehen zwei schwerwiegende Probleme in den kabellosen Lösungen der 7900er Serie. Eines der Probleme ist durch Standardkonten für SNMP gegeben. Mit public und private lassen sich über den klassischen Dienst jegliche Konfigurations-Informationen auslesen und gar schreiben. Ein Angreifer kann diesen Umstand nutzen, um das Telefon und sein Verhalten nach Belieben zu manipulieren (z.B. Adressbuch ändern). Cisco hat dedizierte Patches für die betroffenen Modelle herausgegeben. Als Workaround wird der Einsatz von ACLs und Firewalling für den betroffenen SNMP-Ports udp/161 und 162 empfohlen.

Expertenmeinung:

Diese Schwachstelle ist etwas vom kuriosesten, was ich seit langem gesehen habe. Diese SNMP-Möglichkeit ist ein enormes Scheunentor, das sämtliche Umgebungen, die das betroffene Produkt einsetzen, total unsicher machen. Ein alteingesessener Hersteller wie Cisco sollte zudem aus vergangenen Fehlern gelernt haben und endlich auf Standardkonten verzichten. Es zeigt sich hier aber sehr deutlich, dass sich in Bezug auf Voice-over-IP vor allem klassische Sicherheitsprobleme weitertragen. Es ist nämlich ein Problem, das man so schon zu Hauf auf anderen TCP/IP-basierten Plattformen gegeben sah.

3.3 Microsoft Internet Explorer bis 6.0 Bild mit Link-Verkapselung Destination vortäuschen

Einstufung: **kritisch**

Remote: Ja
 Datum: 16.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1906>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Claudio "Sverx" machte eine leicht abgewandelte altbekannte Angriffsform auf den Browser bekannt. Und zwar kann die wahre Link-Destination vorgetäuscht werden, wenn ein mit einem Link versehen Bild mit einem klassischen Anchor-Link verkapselt wird. Sodann wird der "externe" Link in der Status-Zeile des Browsers ausgewiesen. Dieser Umstand kann genutzt werden, um innerhalb eine Social Engineering-Angriffs (z.B. Phishing) Benutzer zum Aufsuchen einer vermeintlich vertrauenswürdigen Quelle zu verleiten. Beispiel-Code wurde schon veröffentlicht. Als Workaround wird empfohlen, sowohl nur vertrauenswürdigen Links zu folgen und nach Möglichkeiten einen alternativen Browser einzusetzen.

Expertenmeinung:

Dieser Angriff ist unter Umständen kritisch, da er zusammen mit anderen Schwachstellen zur effizienten Umsetzung psychologischer oder technischen Attacken führen kann, ohne dass der Benutzer überhaupt etwas davon mitbekommen könnte. Es ist daher umso wichtiger, schnellstmöglich Gegenmassnahmen zu ergreifen und beim Erscheinen eines Patches diesen unverzüglich auf den betroffenen Systemen einzuspielen.

3.4 CheckPoint Firewall-1 bis R55P IPsec IKEv1 korruptes Paket Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 14.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1903>

Checkpoint Firewall-1 ist eine populäre Firewall-Lösung aus dem Hause Checkpoint Software Technologies. Das über UDP-Protokoll laufende IKE wird genutzt, um die Schlüssel für gesicherte IPSec-Verbindungen auszutauschen. Die Oulu University Secure Programming Group (OUSPG) hat eine schwerwiegende Schwachstelle in StoneSoft StoneGate bis 2.6.1 im Umgang mit korrupten Paketen bei IKEv1 entdeckt. Dies kann zu einer Denial of Service des Geräts führen. Technische Details oder ein Exploit sind noch nicht bekannt. StoneSoft hat das Problem mit

Patches adressiert.

Expertenmeinung:

Die Verbreitung von CheckPoint-Firewalls im professionellen Bereich sorgt dafür, dass dieser Angriff vor allem für Grossfirmen von Bedeutung werden wird. Da eine Vielzahl an IPsec-Implementierungen betroffen sind, kann man aber durchaus von einem generellen Flächenbrand reden. Gegenmassnahmen tun dringend und zwingend Not.

3.5 Sun Solaris 9 und 10 in.iked IPsec IKEv1 korruptes Paket Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 14.11.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1899>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. Das über UDP-Protokoll laufende IKE wird genutzt, um die Schlüssel für gesicherte IPsec-Verbindungen auszutauschen. Die Oulu University Secure Programming Group (OUSPG) hat eine schwerwiegende Schwachstelle in Sun Solaris 9 und 10 im Umgang mit korrupten Paketen bei IKEv1 entdeckt. Dies kann zu einer Denial of Service des Geräts führen. Technische Details oder ein Exploit sind noch nicht bekannt. Sun hat das Problem mit T-Patches adressiert.

Expertenmeinung:

Solaris-Systeme sind vor allem im professionellen Bereich sehr verbreitet, weshalb diese Angriffsmöglichkeit mit offenen Armen empfangen wurde. Besonders Skript-Kiddies werden nach Erscheinen eines Exploits wahre Freude daran haben. Da eine Vielzahl an IPsec-Implementierungen betroffen sind, kann man aber durchaus von einem generellen Flächenbrand reden. Gegenmassnahmen tun dringend und zwingend Not.

3.6 Cisco IOS bis 12.4T IPsec IKEv1 korruptes Paket Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 14.11.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1895>

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. Das

über UDP-Protokoll laufende IKE wird genutzt, um die Schlüssel für gesicherte IPsec-Verbindungen auszutauschen. Die Oulu University Secure Programming Group (OUSPG) hat eine schwerwiegende Schwachstelle in IOS bis 12.4T im Umgang mit korrupten Paketen bei IKEv1 entdeckt. Dies kann zu einer Denial of Service des Geräts führen. Technische Details oder ein Exploit sind noch nicht bekannt. Cisco hat wie immer das Problem mit dedizierten Patches für die betroffenen Produkte adressiert.

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. Da eine Vielzahl an IPsec-Implementierungen betroffen sind, kann man aber durchaus von einem generellen Flächenbrand reden. Gegenmassnahmen tun dringend und zwingend Not.

3.7 sudo bis 1.6.8p12 Perl Environment aufräumen Umgebungsvariablen erweiterte Rechte

Einstufung: **kritisch**
Remote: Indirekt
Datum: 11.11.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1892>

sudo (Superuser do) ist ein klassischer Befehl unter Unix-Systemen, der dazu benutzt wird, um Prozesse mit den Rechten eines anderen Benutzers zu starten. Charles Morris entdeckte einen Designfehler in den Versionen bis 1.6.8p12. In Bezug auf Perl werden die Umgebungsvariablen PERLLIB, PERL5LIB und PERL5OPT nicht richtig gesäubert, so dass ein lokaler Angreifer erweiterte Rechte erlangen könnte. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Das Problem wurde in der jüngsten sudo-Version behoben.

Expertenmeinung:

Obschon es sich hierbei um eine lokale Schwachstelle handelt, sind die Möglichkeiten einer Rechteübernahme eine existentielle Gefahr. Auf Multiuser-Systemen sollte daher unverzüglich der Patch installiert werden, um das Risiko eines erfolgreichen Angriffs im Keim zu ersticken. Lokale Angriffsmöglichkeiten erreichen



zwar nie die Popularität von Remote-Attacken - Trotzdem dürfte sich aufgrund der hohen Verbreitung des sudo-Kommandos eine Vielzahl von Angreifern für die neue Möglichkeit interessieren.

3.8 RealNetworks RealPlayer bis 10.5 DUNZIP32.DLL korrupte RJS Skin-Datei Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 10.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1890>

Der RealOne Player ist die Weiterentwicklung des altbekannten Real-Players der Firma Real Networks. Er ist in erster Linie für die Wiedergabe von Real-Dateien (Real-Audio und -Video) ausgelegt, kann aber auch andere Formate abspielen (z.B. MP3). Karl Lynn von eEye entdeckte zwei kritische Schwachstellen in den Versionen bis 10.5. Eine davon wird durch eine falsche Längenangabe in einem mit ZIP komprimierten Skin-File provoziert. Durch den gegebenen Pufferüberlauf kann ein Angreifer mittels korrupter Skin-Datei beliebigen Programmcode ausführen lassen. Es sind keine genauen technischen Details oder ein Exploit zur Schwachstelle bekannt. RealNetworks hat dem Problem mit dedizierten Patches für die verwundbaren Software-Versionen Rechnung getragen.

Expertenmeinung:

Diese Verwundbarkeit zeigt einmal mehr, dass harmlose Client-Applikationen für Angriffe missbraucht werden können. Das Einspielen der Patches ist entsprechend - und aufgrund der Möglichkeiten der jüngsten Attacke dringendst - empfohlen. Mit Komplikationen beim Aufspielen der Patches ist nicht zu rechnen.

3.9 SAP Web Application Server bis 7.00 fameset.htm sap-syscmd Cross Site Scripting

Einstufung: **kritisch**
 Remote: Ja
 Datum: 10.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1885>

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. [http://de.wikipedia.org/wiki/SAP_AG] Leandro Meiners von Cybsec S.A. entdeckte gleich mehrere Fehler im SAP Web Application Server bis 7.00. Drei davon sind auf Cross Site Scripting-Schwachstellen zurückzuführen. Eine davon findet sich im sap-syscmd-Parameter von frameset.htm wieder. Ein Angreifer kann diesen Umstand nutzen, um Angriffe im Kontext des Webbrowsers des Opfers durchzuführen. Das Vorgehen für das Umsetzen des Angriffs wurde im Advisory festgehalten. SAP wartet mit einer Lösung auf. Nutzer müssen jedoch den Hersteller kontaktieren, um genaue Details für die Gegenmassnahmen zu erhalten.

Expertenmeinung:

Cross Site Scripting Angriffe erfreuen sich in letzter Zeit grosser Beliebtheit. Viele tun sie als kleines Ärgernis ab - Andere schätzen sie als reelle Bedrohung ein. Gerade bei Angriffen wie diesem, bei dem sämtliche Benutzer einer SAP-Umgebung gefährdet sind, muss man das Risiko als gegeben akzeptieren.

3.10 SpamAssassin bis 3.0.4 Message.pm reguläre Ausdrücke lange Header Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 10.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1881>

SpamAssassin ist eine gern und oft eingesetzte und frei erhältliche AntiSpam Software. Wie das Entwickler-Team meldet, existiert eine Denial of Service-Schwachstelle in den Versionen bis 3.0.4. Die in Message.pm genutzten regulären Ausdrücke versagen bei der Interpretation langer Headerzeilen eines Emails. Dies kann zu einem Absturz der Applikation führen. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Fehler wurde in der jüngsten Software-Version behoben.

Expertenmeinung:

Eine einfache Denial of Service Schwachstelle. Dennoch sehr ärgerlich. Denn wer wurde nicht schon selbst von irgendwelchen Spammails belästigt. Sei dies nun Krawatten, Swissair Besteck, Lotteriegewinne oder zuletzt vor der schweizerischen Schengen Abstimmung.

3.11 Veritas NetBackup bis 5.1 vmd-Bibliothek Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 09.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1878>

Veritas stellt neben dem Cluster Server für die Lastverteilung bzw. Leistungskombinierung ebenfalls eine Backup-Lösung zur Verfügung. Wie iDEFENSE herausgefunden hat, existiert ein Pufferüberlauf in einer Shared Library des vmd in den Versionen bis 5.1 von NetBackup. Ein Angreifer kann diesen Fehler im Volume Manager Daemon nutzen, um eine Denial of Service-Attacke umzusetzen oder gar beliebigen Programmcode ausführen zu können. Es sind keine weiteren Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler wurde innerhalb eines kumulativen Patches behoben.

Expertenmeinung:

Obschon bisher noch keine technischen Informationen zur besagten Verwundbarkeit bekannt sind, sollte man ein Update auf die neueste Version nicht hinausschieben. Es ist nur eine Frage der Zeit, bis die ersten Exploits zur automatisierten Ausnutzung der Schwachstelle die Runde machen. Da Veritas-Produkte vor allem in grösseren Umgebung ihre Verwendung finden, ist diese Schwachstelle doch für den einen oder anderen Angreifer interessant.

3.12 Microsoft Windows 2000 und XP korrupte WMF/EMF-Datei Pufferüberlauf

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 08.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1876>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Es existieren Versionen für den Einsatz als Server und solche für den Workstation-Betrieb. Wie Microsoft in MS05-053 (KB896424) meldet, existiert eine schwerwiegende Pufferüberlauf-Schwachstelle bei der Interpretation korrupter WMF- und EMF-Dateien. Ein Angreifer kann über diese beliebigen Programmcode ausführen lassen. Besonders Problematisch ist der Fehler, da derlei Dateien automatisiert durch populäre Client-Anwendungen wie Microsoft Outlook oder dem Microsoft Internet Explorer interpretiert werden. Das Umsetzen der Übernahme eines

Systems ist entsprechend via korrupter Webseite oder Email denkbar. Genaue technische Details oder ein Exploit sind noch nicht bekannt. Microsoft hat zeitgleich mit der Veröffentlichung der Sicherheitslücke ein Patch für die betroffenen Systeme herausgegeben.

Expertenmeinung:

Eine wahrhaftig kritische Schwachstelle, da der Pufferüberlauf nahezu jedes moderne Windows-System betrifft. Die Interpretation von WMF/EMF-Dateien 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 ausnutzen zu können. Grossflächige Kompromittierungen von Systemen, wie schon damals bei der ähnlichen Problematik in Bezug auf JPEG-Bilder, wird die Folge sein. Gegenmassnahmen sind unverzüglich umzusetzen, um verheerende Ausmasse an Schäden wie im Falle des Blaster-Wurms zu verhindern.

3.13 Macromedia Flash Player bis 8.0.22.0 SWF-Datei Frame Type Identifier Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 05.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1875>

Macromedia Flash (kurz Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erzeugung von Flash-Filmen im SWF-Format, einem auf Vektorgrafiken basierenden Grafik- und Animationsformat der amerikanischen Firma Macromedia. Fang Xing von eEye Digital Security entdeckte einen Fehler, der sämtliche Versionen von Macromedia Flash Player bis 8.0.22.0 betrifft. Und zwar werden bei SWF-Dateien der Frame Type Identifier nicht richtig überprüft, was zu einer Rechtheausweitung über eine korrupte SWF-Datei führen kann. Dies kann für das Ausführen beliebigen Programmcodes missbraucht werden. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Fehler wurde im Macromedia Flash Player 8.0.22.0 behoben.

Expertenmeinung:

Diese Sicherheitslücke birgt ein hohes Risiko in sich. So ist ein entfernter Angreifer mit einem simplen SWF-Dateien in der Lage, über den Webbrowser beliebigen Programmcode ausführen zu lassen. Da ein Beispiel-Exploit für

einen Denial of Service-Angriff aufgrund des erhöhten Interesses bald folgen wird, ist es nur eine Frage der Zeit, bis dieser Angriff erfolgreich im World Wide Web angetroffen werden kann. Vor allem Skript-Kiddies und Anbieter von Dialern werden diese Methode für ihre Zwecke nutzen wollen. Es ist kein Geheimnis, dass aktive Inhalte wie Flash nicht unbedingt den besten Ruf in Bezug auf die Sicherheit genießt. So sollte man bei Nichtgebrauch auf die Interpretation dessen verzichten.

3.14 IBM Lotus Domino bis 6.5.4 Fix Pack 2 Domino Web Access fehlerhafte URL Denial of Service

Einstufung: **kritisch**
 Remote: Teilweise
 Datum: 04.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1872>

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. Mit dem Domino Web Access (DWA) wird eine web-basierte Schnittstelle für das Nutzen von Lotus Domino angeboten. Wie IBM nun mit dem Fix Pack 2 für Lotus Domino 6.5.4 bekanntgegeben hat, existiert eine Denial of Service-Schwachstelle. Und zwar kann das System über eine korrupte URL zum Absturz gebracht werden. Es sind keine weiteren Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler wurde mit dem besagten Fix Pack 2 behoben.

Expertenmeinung:

Vorwiegend verärgerte Mitarbeiter werden diese Denial of Service-Möglichkeit nutzen, um ihrem Arbeitgeber und den zuständigen Administratoren Aufwand zu bereiten. Um das Risiko von derlei Übergriffen zu minimieren, sollte das Fix Pack 2 appliziert werden.

3.15 Apache Tomcat bis 5.5.12 Directory Listing Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 04.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1867>

Apache Tomcat stellt eine Umgebung zur Ausführung von Java-Code auf Webservern bereit, die im Rahmen des Jakarta-Projekts der

Apache Software Foundation entwickelt wird. David Maciejak entdeckte eine Denial of Service-Schwachstelle, die sämtliche Versionen bis 5.5.12 betrifft. Und zwar erzeugen mehrere Anfragen auf Verzeichnisse mit mehreren Dateien als Inhalt und ohne Index-Datei eine hohe CPU-Auslastung. Dies kann dazu führen, dass legitimen Benutzern der Zugriff auf das besagte Verzeichnis, und zwar nur dieses, verwehrt bleibt. Bei den Versionen 5.5.11 ist dies ein konstanter Fehler. Bei der Version 5.5.12 wurde er teilweise adressiert: Dort regeneriert sich das System nach einigen Minuten wieder.

Expertenmeinung:

Grundsätzlich müssen zwei Dinge erfüllt sein, damit dieser Angriff Fuss fassen kann: So auf dem Webserver Index-Listing aktiviert und eine Vielzahl an Dateien in einem solchen Verzeichnis vorhanden sein. Diese Sicherheitskücke ist nicht wirklich akut, denn der Absturz eines solchen Webverzeichnisses ist lediglich lästig und keine wirklich grosse Gefahr.

3.16 Cisco Wireless LAN Controller LWAPP Verschlüsselung umgehen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 03.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1865>

Die Firma Cisco hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Nebenher bieten sie auch einige Produkte für Wireless LAN-Verbindungen an. Wie der Hersteller meldet, existiert eine Designschwachstelle in den Serien 2000 und 4400. Werden diese mit LWAPP (Lightweight Access Point Protocol) betrieben, kann der Einsatz der Verschlüsselung verhindert werden. Ein Angreifer kann dies mittels MAC-Spoofing bei Zugriff auf einen schon authentisierten Client umsetzen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Cisco hat Patches zu den jeweiligen Produkten bereitgestellt.

Expertenmeinung:

Wireless LAN Access Points sind die Stützpfeiler moderner WLAN-Netze. Kann ein solcher Access Point manipuliert werden, fällt damit zeitgleich die Sicherheit des gesamten Funknetzwerks. Da bei fehlender Verschlüsselung schnell sämtliche Elemente in einem WLAN ausgehört werden können, es dann meist nur noch eine Frage der Zeit, bis ein Angreifer eines dieser unter seine Kontrolle zu bringen.



3.17 NetBSD bis 2.1 setuid-Programme ptrace() erweiterte Rechte

Einstufung: **kritisch**
 Remote: Indirekt
 Datum: 02.11.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1860>

NetBSD ist ein Unix-Derivat der BSD-Reihe. Es wird gerne in Umgebungen eingesetzt, in denen Sicherheit und Networking eine übergeordnete Rolle spielen. Wie Tavis Ormandy gemeldet hat, existiert ein schwerwiegender Designfehler in NetBSD bis 2.1. Ein Angreifer kann erweiterte Rechte erlangen, da eine setuid-Software bei der Ausführung von ptrace() die Rechte nicht explizit überprüft. Darüber können eigene System-Calls injiziert werden. Bei betroffenen Versionen kann über CVS ein Patch eingespielt werden.

Expertenmeinung:

Obschon Telnet als veraltet und unsicher gilt, befindet sich dieser Dienst noch vielerorts im Einsatz. Der Grund ist der, dass praktisch ein jedes Betriebssystem mit einem entsprechenden Client ausgeliefert wird, und nicht wie bei SSH zuerst ein solcher installiert und konfiguriert werden muss. Die Verbreitung von BSD im professionellen Umfeld trägt dazu bei, dass dieser Angriff für einige Leute interessant wird.

3.18 PHP bis 5.0.5 HTTP POST GLOBALS globale Variablen erweiterte Rechte

Einstufung: **kritisch**
 Remote: Ja
 Datum: 31.10.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1844>

PHP ist ein frei verfügbares open-source Skripting-Paket, das für sämtliche populären Betriebssysteme zur Verfügung steht. Stefan Esser des Hardened-PHP Project entdeckte eine Reihe von kritischen Schwachstellen in PHP bis 4.4.0 und bis 5.0.5. Eine davon betrifft HTTP POST-Anfragen, über die mit einer multipart/form-data-Codierung auf globale Variablen zugegriffen werden können. Der Fehler ist bei einer Eingabeüberprüfung von GLOBALS gegeben, weshalb ein Angreifer globale Variablen selber schreiben kann. Betroffen sind Umgebungen, die register_globals aktiviert haben und Web-Anwendungen, die zugleich auf Funktionen wie extract() und import_request_variables() zurückgreifen. Einige technische Details finden sich in <http://www.hardened-php.net/index.76.html> - Ein

Exploit zur Schwachstelle ist nicht bekannt. Der Fehler wurde in der aktuellen PHP-Version 4.4.1 behoben. Als Workaround wird empfohlen, die Option register_globals zu deaktivieren bzw. keine POST-Anfragen zuzulassen.

Expertenmeinung:

Werden in einem neuem Software-Release so viele Schwachstellen behoben, wie in dem jüngsten von PHP, 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 PHP eine enorme Verbreitung 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 göttlich tun.

3.19 RSA ACE/Agent bis 5.1.1 webauthentication GetPic Cross Site Scripting

Einstufung: **kritisch**
 Remote: Ja
 Datum: 26.10.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1840>

Die SecureID-Lösung der Firma RSA Security wird für die strenge Authentisierung von Benutzern mittels Token eingesetzt. SEC Consult fand einen Fehler in den Versionen 5.1.1. So ist über die Eingabe einer URL in der Form [http://\[host\]/webauthentication?GetPic?image=\[XSS\]](http://[host]/webauthentication?GetPic?image=[XSS]) das Umsetzen von Cross Site Scripting-Attacken möglich. RSA empfiehlt bis auf weiteres lediglich, diese Angriffsform mit einem Proxy-Element zu verhindern.

Expertenmeinung:

Cross Site Scripting Angriffe erfreuen sich in letzter Zeit grosser Beliebtheit. Viele tun sie als kleines Ärgernis ab - Andere schätzen sie als reelle Bedrohung ein. Gerade bei Angriffen wie diesem, bei dem Benutzer in vermeintlich hochsicheren Umgebungen gefährdet sind, muss man das Risiko als gegeben akzeptieren.

3.20 Skype bis 1.4.0.83 skype:// und callto:// URI Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 25.10.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1836>

Skype ist eine freie Lösung für Online-Telefonie, die vor allem im Jahr 2005 nach der Übernahme von eBay für Aufsehen gesorgt hat. Sie ist für verschiedene Plattformen - von Windows über MacOS X bis Linux - erhältlich. Wie die Entwickler melden, existiert eine Pufferüberlauf-Schwachstelle in den beiden mitregistrierten URIs `skype://` und `callto://`. Ein Angreifer kann scheinbar durch einen speziellen Aufruf dieser eine Denial of Service-Attacke umsetzen oder gar beliebigen Programmcode ausführen lassen - Letzteres ist den Skype-Entwicklern angeblich selbst nicht gelungen. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler betrifft sämtliche aktuellen Versionen bis 1.4.0.83. Für sämtliche Plattformen wurde eine aktualisierte Software-Version herausgegeben, die auch noch andere Fehler behebt.

Expertenmeinung:

Das Mehr an Popularität des jüngsten eBay-Einkaufs bringt einmal mehr ein Mehr an Interesse potentieller Angreifer mit sich. Es erstaunt trotzdem, dass gerade derlei simple Schwachstellen gegeben sind, sollten Entwickler in der heutigen Zeit doch den grundsätzlichen Umgang mit benutzerdefinierten Variablen kennen und können.

4. Statistiken Verletzbarkeiten

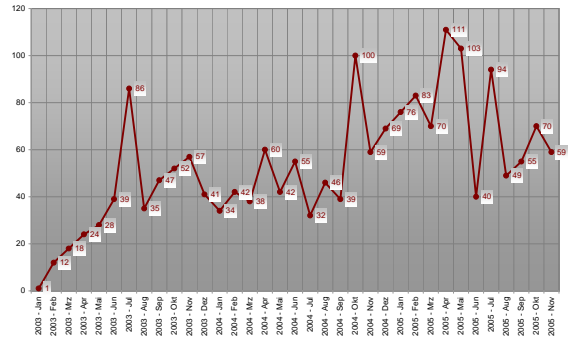
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



<http://www.scip.ch/cgi-bin/sms/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.

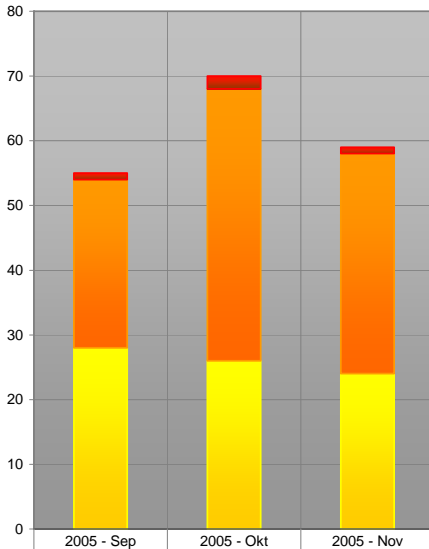
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat

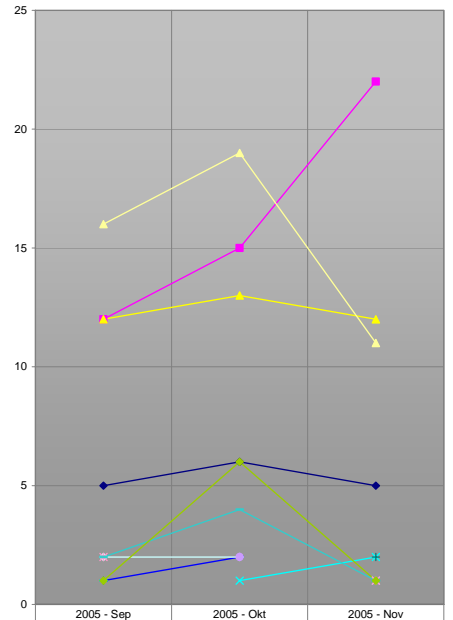
Auswertungsdatum:

19. November 2005



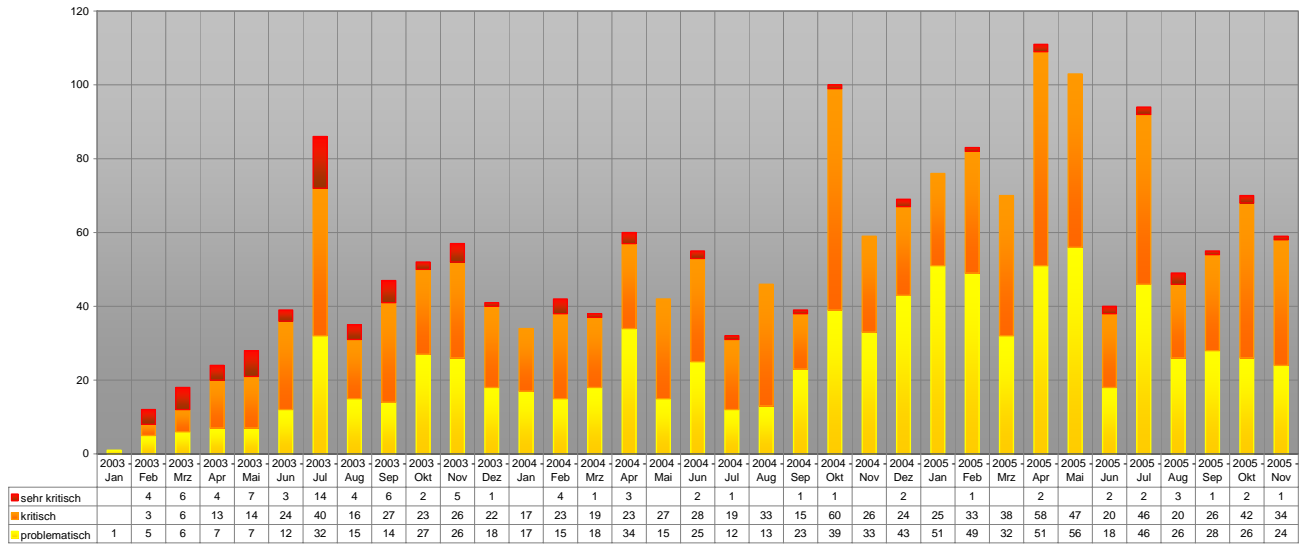
	2005 - Sep	2005 - Okt	2005 - Nov
sehr kritisch	1	2	1
kritisch	26	42	34
problematisch	28	26	24

Verlauf der letzten drei Monate Schwachstelle/Schweregrad

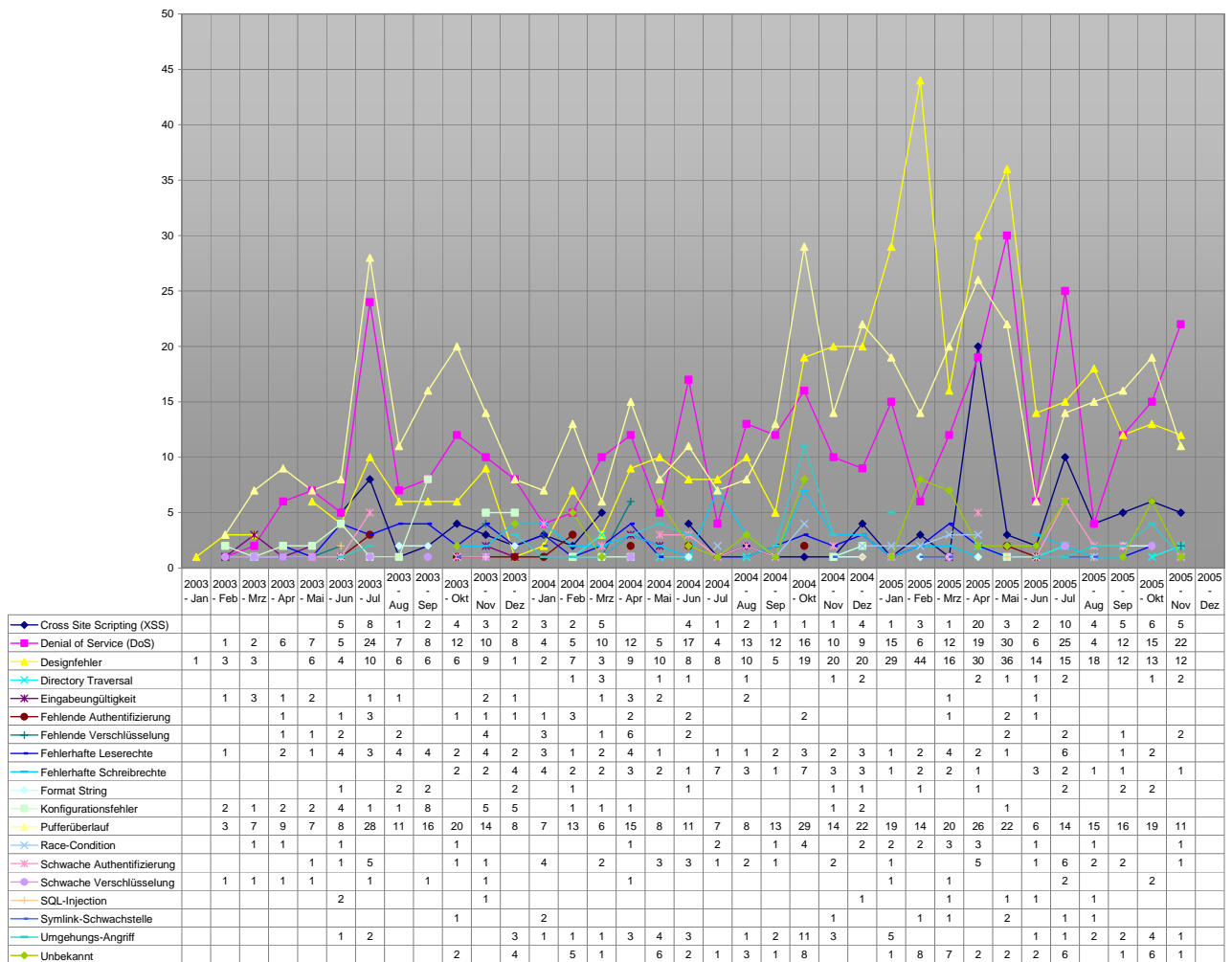


	2005 - Sep	2005 - Okt	2005 - Nov
Cross Site Scripting (XSS)	5	6	5
Denial of Service (DoS)	12	15	22
Designfehler	12	13	12
Directory Traversal		1	2
Eingabeungültigkeit			
Fehlende Authentifizierung			
Fehlende Verschlüsselung	1		2
Fehlerhafte Leserechte	1	2	
Fehlerhafte Schreibrechte	1		1
Format String	2	2	
Konfigurationsfehler			
Pufferüberlauf	16	19	11
Race-Condition			1
Schwache Authentifizierung	2		1
Schwache Verschlüsselung		2	
SQL-Injection			
Symlink-Schwachstelle			
Umgehungs-Angriff	2	4	1
Unbekannt	1	6	1

Verlauf der letzten drei Monate Schwachstelle/Kategorie



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat



Verlauf der Anzahl Schwachstellen/Kategorie pro Monat



5. Erfahrungsbericht

5.1 Ein Tag im Leben eines Social Engineers

Marc Ruef, <mailto:maru@scip.ch>

Obschon ich ein bisschen zwiespältig der Figur Kevin Mitnick gegenüberstehe, habe ich in mancherlei Hinsicht unverhohlene Hochachtung vor seiner Person. So ist es unbestritten, dass er einen beachtlichen Teil dazu geleistet hat, dass Social Engineering salonfähig geworden ist. Ohne seine bekannten Angriffe und die Medienwirksamkeit, die diese erzeugt haben, wäre das Thema Computersicherheit heute wohl noch viel eher ein rein technisches Gebiet - Die menschlichen und psychologischen Elemente würden wohl unweigerlich unterschätzt werden.

So ist es in der Tat gegeben, dass wir ab und an einen Social Engineering-Auftrag umsetzen müssen. Dabei geht es in den meisten Fällen innerhalb eines Penetration Testing-Projekts darum, die menschliche Komponente der Sicherheit zu überprüfen. Das Ziel ist nicht, einzelne Personen blosszustellen oder eine Demonstration umzusetzen, dass der Mensch ansich für Fehlleistungen anfällig ist. Dies ist wohl jedem bewusst. Stattdessen verstehen sich solche Aktionen als Überprüfungen der Prozeduren eines Unternehmens, die eben genau Fehler in der menschlichen Komponente sowie den umgesetzten Prozessen determinieren können soll.

Vor einiger Zeit kontaktierte uns ein Mitbewerber, der ebenfalls im Bereich des technischen Security Auditings tätig ist. Er machte daraus kein Geheimnis und fragte offen an, ob wir einen ihrer Mitarbeiter in Bezug des Penetration Testings auf den neuesten Stand bringen könnten. Ihre Leuten könnten zwar nmap und Nessus bedienen, wissen auch, wie sie ein false positiv erkennen - Aber das effektive Ausnutzen von Schwachstellen und damit der wichtigste Teil eines Penetration Tests ging ihnen abhanden. Weiter soll es sich nicht nur um eine herkömmlich aufgezugene Einzelschulung handeln. Stattdessen soll in dieser direkt einer ihrer Kunden abgearbeitet werden. Das Management wollte wohl mal wieder zwei Fliegen mit einer Klappe schlagen und die Techniker hätten dieses Kunststück dann vollbringen sollen.

Wie ich nunmal bin, riet ich von der Sache ab. Nicht, weil ich nicht wollte, dass der Mitbewerber einen Vorteil im Markt erlangen könnte, indem

wir ihm unsere Herangehensweise zeigen. Nein, stattdessen erschien es für mich sowohl unmöglich, innerhalb eines Arbeitstages sämtliche Kniffe zu zeigen. Und zudem ist es umso schwieriger, eine Sache näher zubringen, wenn diese direkt in einem Projekt verknüpft ist. Die Aktion bleibt zwar sehr realitätsnah, wird jedoch aufgrund fehlender didaktischer Manipulationen umso schwieriger zu verstehen. Dennoch, man einigte sich auf diesen einen Tag.

Der Auditor des Mitbewerbers kam zu mir ins Büro und ich liess ihn mir als erstes erzählen, was er von diesem Tag erwartete. Zudem berichtete er mir, was er bereits innerhalb des Testings,

„So ist es in der Tat gegeben, dass wir ab und an einen Social Engineering-Auftrag umsetzen müssen.“

eine Überprüfung einer Zweigstelle eines Unternehmens in der Ukraine, gefunden hatte. Seine Ausgaben mit nmap, Nessus, nikto, usw. zeigten mir, dass es sich um einen simplen und gut strukturierten Perimeter handelte. Obschon ein ganzer Klasse A-Netzblock auf den Kunden registriert war, schienen nur einige wenige Hosts aus dem Internet direkt erreichbar. Diese - neben einem Mail- und Webserver ebenfalls einen Terminal Server auf Windows Server 2003 - wurden wohl durch eine zentrale Firewall-Komponente (CheckPoint Firewall-1) geroutet.

Erfahrungsgemäss kann ich sagen, dass umso kleiner eine Umgebung ist, umso grösser die Chance ausfällt, dass der Administrator in dieser ein beharrliches Augenmerk auf die Sicherheit dieser richtet. So war es dann auch, denn sämtliche Geräte schienen auf dem neuesten Stand: Aktuellste Software-Versionen und die neuesten Patches machten es praktisch unmöglich, innerhalb dieses einen Tages einen rein elektronischen Einbruch umzusetzen. Andere Möglichkeiten mussten her.

Ich wies darauf hin, dass meine Erfahrungen mit Social Engineering sehr gut sind. Ein solide inszenierter Zugriff verspricht bei mindestens 10 % der Benutzer Erfolg. Er willigte ein, dass dies die letzte Möglichkeit im Rahmen des Projekts war, um noch einen Erfolg verbuchen zu können. Nachdem wir ein klassisches technisches Footprinting gemacht hatten, diskutieren wir das Vorgehen. Wir fanden 31 Mailadressen der Benutzer, was natürlich mit einer direkten Querprüfung der jeweiligen Personen einher ging. Vor allem eine Person namens Andrey, er nannte sich im Internet Andy, fiel uns auf. Dieser postete seit

Jahren regelmässig in FreeBSD-Newsgruppen im USENET. Diskutiert dort vor allem Probleme bei Paketen. Da wir bei einem vorgängigen OS-Fingerprinng gesehen hatten, dass sowohl Mail- als auch Webserver auf FreeBSD liefen, vermuteten wir, dass Andy der Administrator dieser Hosts war.

Da wir aufgrund des technischen Information Gatherings sagen konnten, dass der Administrator sehr gute Arbeit in Bezug der Sicherheit des Perimeters geleistet hatte, riet ich davon ab, diesen in einen Social Engineering-Eingriff zu verwickeln. Sein Verständnis für Computersicherheit wäre wohl zu hoch und die ganze Operation könnte auffliegen. Es erschien sodann erfolgsversprechender, wenn wir eine der weiblichen Angestellten angehen würden. Da sich Frauen erfahrungsgemäss weniger für Computer und noch weniger für die Sicherheit dieser interessieren, liess uns ein solches Szenario mehr Handlungsspielraum. Durch einen psychologischen Trick hätten wir beispielsweise mit unserem technischen Wissen Druck aufbauen und so die Zielperson zu einer kompromittierenden Handlung verleiten können.

Ich bin dafür bekannt, dass ich mich bis ins letzte Detail auf solcherlei Operationen vorbereite. So schlug ich vor, dass wir als erstes einige Dinge über die Ukraine lesen sollten. Ein kurzer Abriss historischer und politischer Entwicklungen, Darlegungen in Reiseführern und statistische Angaben zur Population und ihres durchschnittlichen Bildungsstandes würden eine wichtige Stütze werden. So rätselten wir zunächst darüber, wie gross die Chance sei, dass unsere Zielperson aufgrund eines soliden Sicherheitsverständnisses Verdacht schöpfen könnte. Ein bisschen Zahlentheorie - Numb3rs lässt grüssen - konnte uns bei der Beantwortung dieser Frage behilflich sein.

In den Jahren 2002 bis 2004 waren in der Ukraine 10'833'300 Telefonleitungen in Betrieb, 4,4 Millionen Mobiltelefone angemeldet, 3,8 Millionen Internet-Anschlüsse registriert und 94'345 Server mit der landeseigenen Top-Level-Domain .ua positioniert. Die Bevölkerung betrug im Juli 2005 47'425'336. Uns interessieren für die Rechnung aber nur diejenigen im erwerbstätigen Alter von 15 bis 64 Jahren. Dies sind 68 % der Gesamtbevölkerung mit 15'619'989 Männer und 16'992'628 Frauen; also ein Total von 32'612'618 potentiell erwerbstätigen Personen. Sodann besitzen nur jede zehnte Person ein Mobiltelefon und einen Internetanschluss. Und nur jede hundertste Person betreibt einen Server mit der Landesdomain.

Im Vergleich zu den Industriestaaten, zum Beispiel Deutschland, ist das Verhältnis bei Mobiltelefonen zu 120 %, bei Internet-Anschlüssen zu 90 % und Internet-Servern mit DE-Domain zu 100 % grösser. Statistisch gesehen ist die Chance also rund 110 % kleiner, dass eine unserer Zielpersonen Zugriff auf Technologien hat und sich mit diesen auskennt (Für eine Grossstadt wie Kiev wohl nicht ganz so extrem, aber der Trend war dennoch absehbar). Da selbst der Erfolg von Social Engineering-Attacken hierzulande enorm hoch ist, müsste es in der Ukraine noch zig mal höher sein, wie uns die grobe Wahrscheinlichkeitsrechnung zeigte.

Sodann ging es ans Eingemachte. Wir riefen bei der Hauptnummer des Büros in der Ukraine an. Dort meldete sich eine Anya, die wir sogleich darüber informierten, dass im Hauptsitz in der

„Die Aktion nahm jedoch eine unerwartete Wendung. Die Dame wusste nicht, was ein Benutzername ist...“

Schweiz ein technisches Problem vorliegen würde. Unsere Datenbank sei korrupt geworden und einige Benutzerkonten seien nicht mehr zugänglich. Wir würden ihr ein Email schicken, das einen Link auf einen Intranet-Server enthielt. Als sie die durch uns vorbereitete Webseite aufrief wurde sie von uns angehalten, dort zur Überprüfung ihre Mailadresse, den Benutzernamen und das Passwort einzugeben. Der Trick bestand darin, dass diese sensitiven Benutzerdaten nach dem Abschicken des Formulars an uns gesendet werden würden und wir so in den Besitz dieser kommen würden. Halt das typische Phishing.

Die Aktion nahm jedoch eine unerwartete Wendung. Die Dame wusste nicht, was ein Benutzername ist - Sie würden sowas nicht nutzen. Ich musste mich wirklich beherrschen, dass ich nicht in schallendes Gelächter ausbrach, denn das Ganze schien an der Unwissenheit der Benutzer zu scheitern. Wir wiesen Anya an, dass sie im Büro nachfragen sollte, ob jemand einen Benutzernamen und ein Passwort kennen würde. Schön artig las sie das Mail, das wir ihr geschickt hatten und die Instruktionen für unsere Phishing-Attacke enthielt, im Grossraumbüro vor. Ich musste zeitweilig das Mikrofon des Telefons ausschalten, denn diese absurde Situation amüsierte mich ungemain. Diese unendliche Unbeholfenheit führte dazu, dass mir Anya schon fast ein bisschen leid tat, klang sie doch sehr sympathisch und hilfsbereit am Telefon.

Und in der Tat scheiterte das Ganze. Die Dame

und ihre Kollegen waren nicht in der Lage, uns auch nur irgendeinen Benutzernamen nennen zu können. Sowa's gäbe es da nicht. Analysen des Webzugriffs haben uns ebenfalls gezeigt, dass sie uralte Windows-Versionen im Einsatz haben, die gar nicht auf den Multiuser-Betrieb und sichere Authentisierungen ausgelegt waren. Uns blieb nichts anderes übrig als Anya zu sagen, dass wir der Sache nachgehen und uns wieder bei ihr melden würden. Eines hat mich die Geschichte gelehrt: Fehlendes Verständnis oder Wissen muss nicht zwingend ein Nachteil für die Sicherheit einer Umgebung sein!

7. Literaturverzeichnis

scip AG, 2005, scip monthly Security Summary, Ausgabe April 2005

http://www.scip.ch/publikationen/smss/scip_mss-19_04_2005-1.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 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. 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 Summary's finden Sie online.

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