

Contents

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

1. Editorial

Kurz- und längerfristige Sicherheit

Regelmässige Leser des scip monthly Security Summary (smSS) kennen die Rubrik „Hintergrundbericht“. In diesem werden spezifische Themen behandelt und durchleuchtet (dieses Mal geht es um Google als Hacking-Instrument; siehe Absatz 4). Ab und an findet sich darin auch ein Interview mit einer Persönlichkeit aus dem Bereich Computersicherheit, wie zum Beispiel mit Matthias Leu, dem Autor des Bestsellers „Check Point Next Generation AI - Das Standardwerk für FireWall-1/VPN-1“ (smSS Ausgabe 19. Juni 2004).

Ich war auf der Suche nach einem neuen Interviewpartner, der die Umsetzung des entsprechenden Absatzes in diesem smSS ermöglichen können sollte. Nach einer Heise Meldung zum Thema der Schliessung neonazistischer Seiten in Amerika stiess ich auf das Shoa-Projekt [Heise 2004]. Dieses war mir schon seit einigen Jahren ein Begriff, denn auf shoa.de wird die Auseinandersetzung mit den Schrecken des Holocaust und ihren Nachwirkungen bis in die Gegenwart behandelt; ein Thema, das wohl jeden geschichtlich interessierten Menschen zum Nachdenken bewegt.



Wahrhaftig eine sehr interessante und Ehrgeizige Initiative, wurde mir beim Durchstöbern des Webauftritts klar. Und mit Sicherheit hätten die Betreiber mit einer Vielzahl an (technischen) Angriffen aus den rechtsextremen Kreisen zu rechnen. Es wäre doch sicher interessant, ein Interview mit den Betreibern der Seite bezüglich Sicherheitsmassnahmen und Angriffe zu führen. So schrieb ich also noch am selben Tag ein Email an die offizielle Adresse des Shoa-Webs. In diesem Schreiben bat ich darum, dass ein potentieller Interviewpartner mit mir via Email ein entsprechendes Gespräch aufnehmen würde.

Einige Tage später erhielt ich sodann auch wirklich eine Rückantwort, die jedoch zu meinem Bedauern und Erstaunen negativ ausfiel. Der Webmaster von shoa.de berichtete mir, dass er nicht für das Hosting zuständig sei, sondern eine entsprechende Firma in Deutschland. Diese habe aber kein Interesse daran, mit mir ein Interview zu führen.

Ein bisschen verduzt, schon fast perplex verharrete ich einige Sekunden vor dem Bildschirm. Ein Interview ist eine einfache und unkomplizierte Sache, bei der man die Möglichkeit einer Plattform erhält, um sich und seine Anliegen zu präsentieren. Jedes freie Projekt und jedes ehrwürdige Unternehmen ist dankbar, wenn es irgendwo in einer Publikation Erwähnung findet – Und das noch ohne Kosten und mit wenig Zeitaufwand. Wieso sollte nun also diese Hosting-Firma kein Interesse an einer solchen Gratis-Werbung haben?

War hier einmal mehr „security by obscurity“ der Fall? Durch das Geheimhalten von Informationen will man die Sicherheit eines eigentlich schwachen Systems aufrecht erhalten? Es kann durchaus sein, dass dieses Hosting-Unternehmen nämlich gar keine speziellen Vorrichtungen gegen Angriffe hat (z.B. Firewalling) und diese eventuell gar nicht protokollieren sowie analysieren kann (z.B. elektronische Einbruchserkennung).

Würden Sie einem Hosting Ihres Webauftritts einwilligen, wenn die offerierende Partnerfirma es verweigert, Auskunft über getroffene Sicherheitsvorkehrungen zu geben? Also ich würde mich dessen definitiv verweigern, denn als potentieller Kunde gilt es mich zu umwerben und dies natürlich mit den grössten Bemühungen, mich auf allen Ebenen zufrieden zu stellen.

Sicherheit durch Geheimhaltung – wie man den stehenden Begriff ins Deutsche übersetzen kann – mag kurzfristig ein Mehr an Sicherheit bieten. Längerfristig gingen diese Schüsse aber stets nach Hinten los. Populäres Beispiel ist der kryptografische Algorithmus COMP128, der bei GSM – dem heutigen Handy-Netz – Verwendung findet. Dieser Mechanismus zur Verschlüsselung wurde ebenso geheimgehalten, später jedoch durch eine Reihe von Tüftlern geknackt. Das Resultat davon: Die Sicherheit des gesamten GSM-Netzes wurde von einer Sekunde auf die andere durch Leute untergraben, die mit viel Mühe eine Analyse der versteckten Informationen durchführen mussten.

Wie schnell wäre die Kryptoanalyse gegangen, wenn sämtliche Informationen zum Algorithmus uneingeschränkt zugänglich gewesen wäre? Wahrscheinlich wäre der Aufwand viel geringer gewesen und man hätte schon im Vorfeld determinieren können, dass es sich um einen schwachen Algorithmus handelt. Entsprechend hätte man frühzeitig reagieren und eine stärkere Implementierung anstreben können. Aber nein, man wählte lieber den kurzfristigen und „kürzeren“, ja quasi den arroganten Weg des Ignorierens. Und wie Nietzsche schon sagte, holt uns stetig die Ewige Wiederkehr ein, wie uns die Absage für das Interview vermuten lässt.

Marc Ruef <maru@scip.ch>
Security Consultant
Zürich, 19. August 2004

2. scip AG Informationen

2.1 Security Betreuung

Im Verlauf eines Projektes oder während des Betriebs der Infrastruktur kann es vorkommen, dass Sie gerne die Meinung und Unterstützung eines Security Spezialisten in Anspruch nehmen würden. Dazu benötigen Sie keinen Audit oder Review. Sie benötigen in kurzer Zeit eine aussagekräftige Beurteilung der Situation und einen adäquaten Vorschlag zur Weiterführung der Angelegenheit.

Ob dies nun:

- Fragen zur IT-Security
- Kurzanalysen zu spezifischen Themen
- 2nd Opinion Anfragen
- Tracking von identifizierten Schwachstellen
- Management Dokument Erstellung
- Logauswertungen
- Etc.

sind.

Gerne unterstützen Sie die Spezialisten der scip AG dabei. Rufen Sie uns an +41 1 445 1818 oder senden Sie uns eine [Mail](#). Wir freuen uns auf Ihre Kontaktaufnahme.

2.2 Workshops

August 2004	
26.08.2004	Log-Management [LMFT04]
September 2004	
03.09.2004	Zonenkonzeption [ZOFO04]
10.09.2004	IT-Security Overview [ISFO04]
15.09.2004	Attacken [ATVE07]
23.09.2004	Intrusion Prevention [IPVE03]

Das scip AG Workshop-Portfolio finden Sie auf unserer Firmenwebseite <http://www.scip.ch>.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.

Die Dienstleistungspakete [\)scip\(pallas](#) liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.

Contents:

- 3.1 Microsoft Internet Explorer bis 6 verschiedene Kommandos Adresszeile Spoofing
- 3.2 Microsoft Windows XP SP2 Internet cmd.exe sicherer Dateidownload umgehen
- 3.3 Adobe Acrobat Reader für Windows bis 6.0.2 RTLHeapFree() lange URL Pufferüberlauf
- 3.4 Clearswift MIMESweeper for Web bis 5.0.4 Directory Traversal
- 3.5 Microsoft Exchange 5.5 Outlook Web Access HTML Redirection Cross Site Scripting
- 3.6 Microsoft Internet Explorer 6 Protocol Handler erweiterte Rechte
- 3.7 libpng bis 1.0.16rc1 und 1.2.6rc1 PNG-Dateien NULL-Pointer Pufferüberlauf
- 3.8 Putty bis 0.55 SSH-Verbindungsaufbau erweiterte Rechte
- 3.9 Check Point VPN-1 ASN.1 Decodierung Pufferüberlauf

3.1 Microsoft Internet Explorer bis 6 verschiedene Kommandos Adresszeile Spoofing

Einstufung: **kritisch**
 Remote: Ja
 Datum: 15.08.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=793>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Liu Die Yu publizierte eine Schwachstelle, mit deren Hilfe die Adressanzeige im Browser gefälscht werden kann. Dadurch können die zur Zeit von den Medien gerne diskutierten Phishing-Attacken umgesetzt werden. Das Problem besteht im bestimmten Ablauf von Kommandos im Browser, die zu einem entsprechenden Fehler führen können. Ein proof-of-concept Exploit wurde zusammen mit dem Advisory publiziert. Der Fehler lässt sich durch die Installation des

Service Pack 2 für Microsoft Windows XP beheben.

Expertenmeinung:

Angriffe auf Webbrowser sind nach wie vor hoch im Kurs. Diese hier beschriebene Möglichkeit ist vor allem aufgrund der durch die Medien mitgebrachten Popularität interessant. Skript-Kiddies und Anbieter von Dialern werden voraussichtlich die Möglichkeiten nutzen wollen, um einen Vorteil zu erlangen.

3.2 Microsoft Windows XP SP2 Internet cmd.exe sicherer Dateidownload umgehen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 16.08.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=792>

Microsoft Windows XP stellt eine Weiterentwicklung des professionellen Windows 2000 dar. Das lange erwartete Service Pack 2 (SP2) kommt mit einigen wichtigen Sicherheits-Neuerungen daher. Eine davon umfasst die Möglichkeit, dass mittels Microsoft Internet Explorer und Outlook aus dem Internet heruntergeladene Dateien nicht ohne weiteres ausgeführt werden können. Dazu werden die Dateien nach dem Download mit einem entsprechenden ADS-Tag von NTFSv5 versehen, der vermerkt, aus welcher Zone die Datei heruntergeladen wurde. Wie Jürgen Schmidt von heise Security nun in seinem Artikel beweist, wird diese Klassifizierung nicht angewendet, wenn für das Ausführen einer Datei der Kommandozeileninterpreter cmd.exe genutzt wird. Die besagten Dateien lassen sich sodann mit Befehlen wie "cmd /c server.exe" direkt und ohne Warnmeldung ausführen. Die c't hat einen proof-of-concept mit einer vermeintlichen GIF-Datei zum Ausprobieren im Netz bereitgestellt. Als Workaround wird empfohlen, nicht ausschliesslich auf das neue Sicherheitsfeature des SP2 zu setzen. Grundsätzlich sollte noch immer vorsichtig mit Dateien unbekannter oder zweifelhafter Herkunft umgegangen werden. Microsoft weist in ihrem Email vom 12. August 2004 darauf hin, dass sie "keinen Konflikt mit den Designzielen der neuen Schutzfunktionen" sehen und deshalb keine Anpassungen oder Patches diesbezüglich liefern werden.

Expertenmeinung:

Wenige Tage nach der Freigabe der endgültigen Version hat heise Security erste Schwachstellen in einer neuen Sicherheitsfunktion von Service

Pack 2 für Windows XP entdeckt. Es ist nun fragwürdig, ob und inwiefern dies das Einleiten eines Vernichtungszugs gegen das neue SP2 ist. Eine Vielzahl an Angreifern werden sich nämlich mit dem neuesten Update von Microsoft beschäftigen, um dem Branchenriesen aus Redmond einmal mehr eins auszuwischen. Die schon fast arrogant anmutende Antwort des Microsoft Security Response Center wird sie sicher noch dazu anstacheln.

3.3 Adobe Acrobat Reader für Windows bis 6.0.2 RTLHeapFree() lange URL Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 15.08.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=791>

Der Acrobat Reader der Firma Adobe ist eine Software für das Interpretieren, Darstellen und Drucken von PDF-Dokumenten. Besonders in der Geschäftswelt ist dieses Dateiformat sehr gern aufgrund seiner hohen Verbreitung, Kompatibilität und der dargelegten Komprimierung gern genutzt. Adobe Acrobat Reader für Windows bis 6.0.2 besteht eine Pufferüberlauf-Schwachstelle in der Funktion RTLHeapFree(). Diese wird mitunter eingesetzt, wenn aus einem PDF-Dokument ein Link aufgerufen wird. Der Angriff lässt sich mit einer URL wie [http://www.scip.ch/dokument.pdf%00aaa\[...\]aaa](http://www.scip.ch/dokument.pdf%00aaa[...]aaa) umsetzen. Bei dieser wird nach dem Nullzeichen die überlange Zeichenkette an das PDF-Dokument zurückgegeben und überschreibt sodann den Speicher. Als Reaktion auf die Benachrichtigung habe Adobe stillschweigend die Version 6.0.2 veröffentlicht, in der das Problem behoben sein soll. Allerdings stürze auch diese Version mit dem iDefense-Exploit noch ab, was darauf hinweist, dass auch in der aktuellen Version des Readers immer noch ein Pufferüberlauf - jedoch vorwiegend in Form eines Denial of Service - auftreten könnte.

Expertenmeinung:

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

Version, sollten also in den kommenden Tagen umgesetzt werden.

3.4 Clearswift MIMESweeper for Web bis 5.0.4 Directory Traversal

Einstufung: **kritisch**
Remote: Ja
Datum: 12.08.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=786>

MIMESweeper der Firma Clearswift ist eine populäre kommerzielle Lösung für das Absichern spezifischer Dienste. Vor allem im SMTP-, aber auch im Web-Bereich werden diese Proxy-Produkte eingesetzt. Wie der Hersteller meldete, existiert eine Directory Traversal-Schwachstelle in Clearswift MIMESweeper for Web bis 5.0.4. Diese ermöglicht es einem Angreifer, weitere Informationen über das Zielsystem oder gar erweiterte Leserechte zu erlangen. Das System ist dabei anfällig auf die klassischen Zeichensequenzen `..\`, `..\\`, `..\^` und `../`. Viele Security und CGI Scanner sind in der Lage, derlei Sicherheitslücken aufzudecken. Zusammen mit dem Advisory wurde ein entsprechender Patch herausgegeben.

Expertenmeinung:

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

3.5 Microsoft Exchange 5.5 Outlook Web Access HTML Redirection Cross Site Scripting

Einstufung: **kritisch**
Remote: Ja
Datum: 10.08.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=783>

Microsoft Exchange ist ein von vielen Unternehmen gern eingesetzter Mailserver für Windows-Umgebungen. In der nicht mehr top-aktuellen Version 5.5 wurde eine Cross Site Scripting-Verwundbarkeit von Amit Klein des Sicherheitsunternehmens Sanctum Inc. gefunden. Einem Angreifer sei es möglich, durch die fehlerhafte Verarbeitung von HTML-Redirects eigene Skripte einzufügen. Dies kann genutzt werden, um indirekt eigener Web-Programmcode auf dem Rechner eines anderen Benutzers ausführen zu lassen. Angeblich sei

nur Microsoft Exchange 5.5 mit Service Pack 4 betroffen. Microsoft hat im Bulletin MS04-026 einen Patch für diese Schwachstelle zur Verfügung gestellt. Der Microsoft Baseline Security Analyzer (MBSA) kann genutzt werden, um die Existenz der Schwachstelle zu verifizieren und mit dem Systems Management Server (SMS) kann das Update eingespielt werden.

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 eine beachtliche Anzahl von Benutzern gefährdet sind - vor allem in KMUs -, muss man das Risiko als gegeben akzeptieren.

3.6 Microsoft Internet Explorer 6 Protocol Handler erweiterte Rechte

Einstufung: **kritisch**
 Remote: Ja
 Datum: 06.08.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=780>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Nicolas Robillard beschreibt in seiner Nachricht an verschiedene Sicherheits-Mailinglisten eine Schwachstelle im Protocol Handler des Microsoft Internet Explorer 6 (andere Versionen könnten jedoch ebenfalls betroffen sein). Diese Protocol Handler werden in der Registry unter HKEY_CLASSES_ROOT definiert und beschreiben die Zuweisung von Applikationen zu bestimmten Protokollen. In der ursprünglichen Nachricht wird der proof-of-concept mit MMS, das unter HKEY_CLASSES_ROOT\MMS\SHELL\OPEN\COMMAND definiert wird, umgesetzt. Dieser ist für das Ausführen des Microsoft Windows Media Players zuständig, wobei der Aufruf über "C:\Program Files\Windows Media Player\wmplayer.exe" "%L" erfolgt. Das %L stellt dabei das Argument für den Programmaufruf dar. Ein Angreifer kann nun beim betroffenen Internet Explorer durch einen Link auf `mms://.%20/layout%20c` das Argument bestimmen. Auf Aufruf lautet nun also aufgeschlüsselt ". /layout c", wodurch der Media Player im Skin Mode gestartet wird. Eine Erweiterung diese Schwachstelle könnte einem Angreifer zusätzliche Rechte einbringen. Microsoft wurde scheinbar nicht frühzeitig oder separat über die Schwachstelle informiert. Die Designschwäche könnte aber im Laufe der

kommenden Monate durch einen Patch behoben werden. Bis dahin wird der Einsatz eines alternativen Browsers empfohlen.

Expertenmeinung:

Dieser Angriff ist unter Umständen kritisch, da er zusammen mit anderen Schwachstellen zur kompletten Komprimierung des Systems 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.

3.7 libpng bis 1.0.16rc1 und 1.2.6rc1 PNG-Dateien NULL-Pointer Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 04.08.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=779>

PNG ist ein relativ junges Dateiformat für Bilder, das besonders wegen seiner hohen Kompression bei geringem Datenverlust geschätzt wird. Vorwiegend im Linux-Umfeld werden PNG-Dateien gerne als Ersatz für GIF-Dateien eingesetzt und die meisten modernen Webbrowser unterstützen diese ebenfalls. Wie nun auf der Projekt-Webseite gemeldet wurde, existiert ein Pufferüberlauf durch einen NULL-Pointer bei der Verarbeitung von PNG-Dateien durch die Bibliothek. Ein Angreifer sieht sich dadurch in der Lage, beliebigen Programmcode auszuführen. Genaue technische Details oder ein Exploit zur Schwachstelle sind bisher nicht bekannt. Der Fehler wurde in libpng 1.0.16rc1 und 1.2.6rc1 behoben. Hersteller von Applikationen, die ebenfalls auf diese Library zurückgreifen, haben teilweise das Problem schon in ihren Anwendungen gelöst (z.B. Mozilla [<http://www.heise.de/security/news/meldung/49778>]). Die Linux-Distributoren haben in der Regeln innerhalb von 24 Stunden eine Aktualisierung der betroffenen Pakete bereitgestellt.

Expertenmeinung:

Diese Schwachstelle zeigt einmal mehr, dass konstruktive Attacken wie Pufferüberlauf-Angriffe auf passive Weise untergebracht werden können. Schon alleine das Besuchen einer Webseite, die korrupte PNG-Dateien enthält, könnte zum Angriff führen. Dies sollte zum wiederholten Male in unser Gedächtnis rufen, dass Automatismen stets ein Mehr an Gefahr mit sich bringen.

3.8 Putty bis 0.55 SSH- Verbindungsaufbau erweiterte Rechte

Einstufung: **kritisch**
Remote: Ja
Datum: 04.08.2004
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=777>

Putty ist ein freier SSH-, Telnet- und rlogin-Client für Windows. Wie das Entwickler-Team meldet, existiert in den Versionen bis 0.55 eine Schwachstelle bezüglich SSH-Kommunikationen. So sei durch einen böartigen SSH-Server das Ausführen beliebigen Programmcodes auf dem Client möglich. Wird SSH2 eingesetzt, kann dies gar schon vor der Überprüfung des Servers geschehen. Zusammen mit der Meldung wurde die aktualisierte Software-Version zum Download bereitgestellt. Da auch Heise über den Fehler berichtete, war der Putty-Webserver zwischenzeitlich nur sehr schwer erreichbar.

Expertenmeinung:

Der hohe Beliebtheitsgrad von Putty in der Windows-Welt macht diesen Angriff in erster Linie interessant. Dass jedoch ein Opfer dazu bewegt werden muss, auf einen kompromittierten SSH-Server zuzugreifen, ist dann doch eher ein schwieriges Unterfangen. Da deshalb verschiedene Dinge zusammenspielen müssen, wird diese Schwachstelle in der Praxis kein allzu hohes Verbreitungspotenzial erlangen können.

3.9 Check Point VPN-1 ASN.1 Decodierung Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 28.07.2004
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=772>

Check Point Firewall-1 ist eine populäre Firewall-Lösung aus dem Hause Checkpoint Software Technologies. Wie die bekannte Sicherheitsfirma ISS berichtet, besteht ein Pufferüberlauf im Modul für die Decodierung von ASN.1-Datenverkehr. So ist es deshalb gegeben, dass ein Angreifer durch ein spezielles Paket beim Aufbau eines VPN-Tunnels beliebigen Programmcode auf einem verwundbaren System ausführen kann. Dazu ist keinerlei Authentisierung auf dem Zielsystem erforderlich. Es sind bisher keine genauen technischen Details oder ein Exploit zur Schwachstelle bekannt. Check Point hat entsprechende Patches für die betroffenen Versionen herausgegeben.

Expertenmeinung:

Diese Schwachstelle ist sehr interessant, da CheckPoint-Lösungen vor allem in Finanzbereichen anzutreffen sind. Im Gegensatz zur im Februar bekannt gewordenen Pufferüberlauf-Schwachstelle von ISAKMP sind bei diesem Fehler sämtliche aktuellen Firewall-1 Versionen betroffen. Das Interesse der Angreifer an einem produktiven Exploit ist deshalb nicht zu unterschätzen. Gegenmassnahmen, vor allem am Perimeter, sollten deshalb unverzüglich umgesetzt werden.

4. Hintergrundbericht

4.1 Google als Hacker-Tool – Was steckt wirklich dahinter?

Marc Ruef <maru@scip.ch>

Die verschiedenen Massenmedien und IT-Fachzeitschriften brachten in den letzten Wochen Meldungen mit Titeln wie "Google als Hacker-Tool" [Computerwoche Online 2004] und "Hacker kamen durch Google an Kreditkartennummern" [Yahoo Nachrichten 2004]. In den Artikeln wird darauf verwiesen, dass Google eine Indizierung von Seiten durchführt, die selbst sensitive Informationen enthalten oder gar direkt auf bestehende Sicherheitslücken in einem Webauftritt hinweisen.

Ich war ein bisschen verduzt über diese Meldungen, denn die besagte Problematik ist keineswegs neu. Schon seit Jahren ist in einschlägigen Kreisen bekannt, dass man bei Google mit Eingaben wie „Index of /etc“ zum Beispiel Seiten findet, deren Konfigurations-Verzeichnis /etc öffentlich durch das World Wide Web einsehbar ist [Long 2004a, 2004b]. Selbst im Buch "Hacking Exposed", dessen Erstauflage im Jahr 2000 erschienen ist, sind entsprechende Kapitel enthalten [Scambray et al. 2000].



Den Stein erneut ins Rollen gebracht hat Johnny Long des amerikanischen Sicherheitsunternehmens Computer Security. Bei seiner Präsentation an der diesjährigen Black Hat USA 2004 zeigte er die Möglichkeiten des Google Hackings, wie dieses Vorgehen nun neu genannt wird (obwohl auch andere Suchmaschinen für entsprechende Abfragen herangezogen werden können). [Black Hat USA 2004, BlackHat.Info 2004]

Es fragt sich, wieso nun einmal mehr plötzlich alle zu einem Problem aufschreien, das schon längst bekannt und akzeptiert ist, sowie zudem auf die technischen Grundgegebenheiten von Index-Suchmaschinen zurückzuführen sind. Das

wäre so, wie wenn die Tageszeitungen auf einmal darüber berichten würden, dass man in Autos nach einem schweren Verkehrsunfall eingeklemmt sein könnte. Alex von gray-world.net betreibt seit dem 14. August 2003 ein öffentliches Projekt, das sich mit der statistischen Auswertung dieses Google Hackings beschäftigt [Alex 2003].

Forscht man ein bisschen nach, kommt man zu verschiedenen Lösungen der plötzlich aufflammenden Popularität des Google Hackings. Als erstes ist auffällig, dass Johnny Long im Dezember dieses Jahres ein Buch mit dem Titel "Penetration Testing with Google" veröffentlichen wird (bei Amazon ist jedoch noch keine Ankündigung vorhanden). Sein Vortrag und die daraus resultierenden Medienberichte fördern natürlich die Chancen des erfolgreichen Verkaufs des besagten Buches. Im Security-Bereich war indirekte Werbung schon immer die beliebteste Methode, ein Produkt anzupreisen und dadurch unters Volk zu bringen (z.B. Advisories oder Exploits).



Dies ist aber voraussichtlich nur ein Grund für das scheinbar erhöhte Interesse an der vermeintlich neuen Google-Sicherheitsproblematik. Google will dieses Jahr an die Börse. Mit viel Getöse setzte sich die Kapital-Maschinerie in Bewegung - Natürlich nicht nur zur Freude aller. Auch Google hat seine Feinde und so versuchen diese natürlich mit allen Mitteln die Möglichkeit eines erfolgreichen Börsengangs der populärsten Internet-Suchmaschine zu verhindern. Der Vortrag von Johnny Long - dessen Webseite übrigens Anfangs August veranstaltet wurde [Long 2004c] - kam da gerade Recht, die Gegenpropaganda ins Rollen zu bringen.

Tja, an diesem Beispiel sehen wir, dass auch der Internet-Bereich ein für alle mal erwachsen geworden ist. Und besonders dreckige Spielchen spielen die Erwachsenen: Lug und Betrug, das Aufbringen von Anlegern und das Verunsichern von Kunden ist im Zeitalter von offenen Betriebssystemen und dem Börsen-Gang von grossen Internet-Firmen keine Neuheit mehr (siehe den Gerichtsfall von SCO gegen IBM).

Man sollte also in allen Lebenslagen vorsichtig und kritisch sein. Jede Pressemeldung verfolgt ein mehr oder weniger offensichtliches Ziel. Im Fall des Google Hackings geht es aber eher zweitrangig um den Schutz der potentiellen oder

betroffenen Opfer. Das ist vor allem deshalb auffällig, weil in praktisch keinem einzigen Artikel darauf hingewiesen wird, welche Gegenmassnahmen, egal ob Anbieter, Kunde oder auf der Seite von Google, angestrebt werden könnten.



Empfehlenswert ist es, auf über das Internet direkt ansprechbaren Systemen nach Möglichkeit überhaupt keine sensitiven Daten zu lagern. Müssen diese über das Internet gewissen Personenkreisen zugänglich sein, gilt es die Informationen mittels Zugangsberechtigungen zu schützen. Einfache und effektive Methode bei Webservern ist der Schutz über htaccess, bei dem eine Limitierung anhand von IP-Adressen sowie die Authentisierung mittels Benutzername/Passwort umgesetzt werden kann. Um bei problematischen Webdokumenten eine Indizierung durch die Robots der Suchmaschinen zu verhindern, kann auf den HTML-Tag `META NAME=ROBOTS CONTENT=NONE>` zurückgegriffen werden. Dies ist jedoch nur ein simpler Schutz, da sich die Betreiber von Suchmaschinen nicht zwingend an diesen Meta-Tag zu halten haben.

5. Kreuzworträtsel

Schichtenmodell zur Kommunikation			Nachfolger der PS2-Stecker	UNIX-Variante (4.3)	Konkurrenzlösung zu PHP	Tabelle für Sonderfunktionen bzw. Steuerzeichen		Back Office		Denial of Service	Linux: Kopiert Dateien	
			DOS: Vergleicht den Inhalt von Dateien			Klassischer UNIX-Texteditor		Objektorientierte Programmierung			Bedienoberfläche für OS/2	4
Hersteller von RealSecure						Wagenrückklau		Wer behauptete, Linux hätte Quelltext gestohlen				
Graphische Bedienoberfläche	Webadresse	Internet Protocol			DDoS-Tool	Von NSA herausgegebene Bücherreihe		Künstliche Intelligenz		Populärste deutsche Linux-Distribution		
			optische Platte	Bösewicht im Film "Password Swordfish"			3					
	6		So weit ich weiss					Informationssystem / Mailbox				
Protokoll für Adressumwandlungen		Fehler in einem Computerprogramm		In allen 4 Ecken (Schach)	Tool zum Auslesen NetBIOS-Namens tabellen		So schnell wie möglich		Gruppe mit Ziel sichere Computer-Plattform	Auswertungs Tool für Anwendungsprotokolle	Freundin des Hackers "Neo"	
Unix: Verschieben einer Datei	Virtual Private Network		UNIX Konfigurationsdateien verzeichn.	Engl.: Begriff für "Dingsbums"	Kommando für "keine Operation"							
				Kryptographische Weiterentwicklung von Telnet			Nachrichtendienst der Vereinigten Staaten					5
E-Mail Standard				Anwälte, Steuerberater, Ärzte TLD				Feature-pack von Check point				
Vorgänger von Windows 2000						Lautes Lachen						
Unix: Löschen einer Datei	Rechen geschwindigkeit											
		Emergency v... (scip AG)		2								
Hauptbausteine sicherer HW der TCPA		1		Javascript	Unix: Anzeigen Speicherplatz jeden Verzeichnisses							

Wettbewerb

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

Einsendeschluss ist der **15.09.2004**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

Gewinnen Sie die Teilnahme am scip AG Workshop: [Attacken](#) [ATVE07] vom 15.09.2004 im Technopark Zürich.

WORKSHOPS



6. Literaturverzeichnis

Alex, 14. August 2003, gray-world.net honey page, <http://gray-world.net/etc/passwd/#wtf>

Black Hat USA 2004, 2004, <http://www.blackhat.com/html/bh-usa-04/bh-usa-04-speakers.html>

BlackHat.Info, 1. August 2004, Is Google the hacker's best friend?, <http://www.blackhat.info/live/modules.php?op=modload&name=News&file=article&sid=4832>

Computerwoche Online, 30. Juli 2004, Google als Hacker-Tool, Computerwoche Online, <http://www.computerwoche.de/index.cfm?pageid=254&artid=63637>

Heise, 27. Juli 2004, Neonazistische Websites in den USA geschlossen, Heise News, <http://www.heise.de/newsticker/meldung/49460>

Long, Johnny, 7. Mai 2004, Google Hacking Mini-Guide, informIT, <http://www.informit.com/articles/article.asp?p=170880>

Long, Johnny, 1. Juli 2004, The Google Hacker's Guide, SecurityManagement Online, http://www.securitymanagement.com/library/Google_Hacker0704.pdf

Long, Johnny, 4. August 2004, WWJH?, <http://johnny.ihackstuff.com>

Scambray, Joel, McClure, Stuart, Kurtz George, 2000, Hacking Exposed, McGraw-Hill Osborne Media, ISBN 0072127481 (zweite Auflage, 2001), <http://www.amazon.de/exec/obidos/ASIN/0072127481/>, deutsche Übersetzung, Ian Travis, Das Anti-Hacker-Buch, Februar 2002 (dritte Auflage), MITP, ISBN 3826608453, <http://www.amazon.de/exec/obidos/ASIN/3826608453/>

Silicon.de, Google ist ein beliebtes Hacker-Tool - Alter Hund mit neuen Tricks, <http://www.silicon.de/cpo/news-itsecurity/detail.php?nr=15727>

Yahoo Nachrichten, 4. August 2004, Hacker kamen durch Google an Kreditkartennummern, Yahoo, <http://de.news.yahoo.com/040804/286/45ek0.html>

7. Impressum

Herausgeber:
scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 1 445 1818
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:
Marc Ruef
Security Consultant
T +41 1 445 1812
<mailto:maru@scip.ch>
PGP:
http://www.scip.ch/firma/facts/maru_scip_ch.asc

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserung möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch.

Die ausgewiesenen IT-Security Spezialisten der scip AG verfügen, in diesem sehr komplexen sowie breitgefächerten Spezialgebiet, über jahrelang erarbeitetes und angewandtes Wissen. Wir sind der **effiziente** und **persönliche** Partner im Sektor IT-Sicherheit. Bei Fragen, Schulungen, Assessments und Projekten im Bezug zur IT-Security finden Sie eine kompetente Anlaufstelle in uns.

Nutzen Sie unsere Dienstleistungen!

Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online unter <http://www.scip.ch/publikationen/smss/>.

Der Bezug des scip monthly Security Summary ist **kostenlos**. Sie können sich mit einer Email an die Adresse smss-subscribe@scip.ch eintragen. Um sich auszutragen, senden Sie Ihr Email an die Adresse smss-unsubscribe@scip.ch