

Contents

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

1. Editorial

IT-Security im Auto

Das Fortbewegungsmittel nummer eins unserer Gesellschaft ist das Automobil. Von den einen heissgeliebt, verehrt und gepflegt von den anderen als reines Fortbewegungs- und Nutzmittel titulierte und gesehen. Unabhängig von der Betrachtung, so bestimmt unsere Mobilität, und somit unsere Automobile, doch einen Grossteil unseres Lebens.

Was, wenn externe Personen uns diese Freiheit aus den Händen nehmen können? Nur Illusion?

Ein heutiges Auto beinhaltet eine grosse Fülle an Elektronik. Man denke nur an die diversen Fahrhilfen ESP, ASR, ABS, Spurassistenten, Abstandskontrolle etc. Die Daten der Sensoren dieser Systeme sind zu verarbeiten. Dazu besitzen moderne Autos ausgeklügelte Bordcomputer, welche dem Fahrer auf Knopfdruck den Reifendruck, den nächsten Servicezeitpunkt, den Verbrauch, den approximativen Kilometerradius etc. angeben. Zudem greift die Elektronik anhand der erhaltenen Daten der unterschiedlichen

Datenquellen auch direkt und ohne Einwirken des Fahrers ins Geschehen ein. So werden einzelne Räder gezielt gebremst oder die Motorendrehzahl automatisch gedrosselt.

Der Fortschritt macht nie halt. Von der Erfassung der Daten zur Verarbeitung und der Korrelierung dieser Daten ist nur eine Frage der Zeit. Bereits heute werden die einzelnen Komponenten innerhalb der Fahrzeuge vernetzt. Bei einem Anruf wird automatisch, je nach Einstellung, das Autoradio auf Stumm geschaltet. Zudem können gestohlene Autos, dank GPS, Mobile und Navigationssystem geortet werden. Die ersten Automobile sind bereits dazu in der Lage im Internet zu browsen. Auch sind Bestrebungen im Gange, jedes Auto als Sender und Empfänger von Daten auszurüsten. Somit könnten die erfassten Daten oder Staumeldungen oder Unfallinformationen oder der Internetzugang etc., ohne grossflächigen Ausbau von Sende- und Empfangsanlagen entlang den Autostrassen, versendet werden. Der Vernetzungsgrad ist so auf hohem Niveau und beinahe flächendeckend möglich.



Solange die Kommandos und Befehle physikalisch innerhalb des Automobiles blieben, sowohl die verursachenden als auch die ausführenden, konnten externe Angreifer nur sehr schwer Befehle beeinflussen. Vorallem beim physikalischen Zugriff konnten z.B.

Kilometerstände manipuliert werden oder das Knacken der Wegfahrsperrung in Angriff genommen werden. Den Eingriff in ein sich bewegendes Objekt, ohne zusätzlich integrierte Anlage, war ein Ding der Unmöglichkeit.

Diese Systemgrenzen werden oder sind jedoch bereits ausser Kraft gesetzt. Denken Sie nur an Bluetooth Empfänger innerhalb des Automobiles. Mit dem Einbinden von Datenquellen ausserhalb des Fahrzeuges könnten Angreifern Tür und Tor

geöffnet werden. Nicht zu verachten ist der Aspekt des Betriebssystems, der Vernetzungstechnologie und der verwendeten Applikationen. Die IT-Gesellschaft kennt das Problem. Software ist nie fehlerfrei! Das gilt sowohl für die Benutzerführung als auch für mögliche Manipulationen durch das Ausnutzen von fehlerhaften Codefragmenten. Patches und Updates sind angesagt.

Ist der Preis des Komforts und der Vernetzung, dass wir jede Woche unser Auto zur Garage bringen müssen um die Software zu patchen? Oder machen wir das lieber über automatische Updates oder doch eher „Apt-get“? Wer stellt die Ressourcen zur Verfügung, wer überprüft die Echtheit? Welche Logdaten werden geschrieben und ausgewertet? Bin ich mir sicher, dass der Garagist oder der Autohersteller nicht auch meine persönlichen Angaben mit der Fahrgestellnummer meines Autos verlinkt um damit, sind wir mal positiv, primär mich als Kunden optimal bedienen zu können. Möglicherweise erhalte ich als Vielfahrer plötzlich Werbung von Restaurants welche an meinen Routen stehen... Sind unsere Behörden in der Lage diese Dinge zu überprüfen und Schritte einzuleiten?

Mal abgesehen von diesen vielen Fragezeichen. Die Entwicklung von Software ist rasant. Die Entwicklung von Automobilen ist eine etwas langwierigere Arbeit. Zwischen Autoentwicklung, Fertigstellung und effektivem Verkaufstart vergehen Jahre. Welche Softwareversion wird nun vorinstalliert? Ein beinahe endloses Thema.

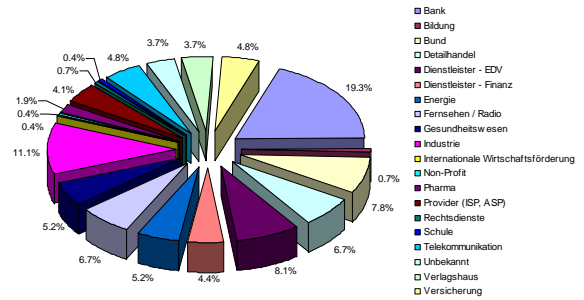
Ich persönlich stehe der Vernetzung der Automobile positiv gegenüber. Ich freue mich auf noch mehr Gimmicks im Auto (wie beim Mobile). Mir ist dabei wichtig, dass der Sicherheit der Autoinsassen oberste Priorität zugeordnet wird. Das beginnt beim Fahrer, dem Reifendruck und der sauberen Scheibe und endet bei der Sicherheit der integrierten Vernetzung und Software. Ich hoffe nur, dass die Industrie aus gemachten Fehlern, als Beispiel seien hier die ersten W-LAN Systeme erwähnt, lernt. Grösse bedeutet nicht Qualität und Sicherheit ist ein Prozess.

Simon Zumstein <sizu at scip.ch>
Geschäftsleiter
Zürich, 19. Februar 2005

2. scip AG Informationen

2.1 smSS >700 Leser

Ein weiterer Meilenstein ist erreicht. Der scip monthly Security Summary (smSS) zählt nun über **700** registrierte Leser. Dabei ist hervorzuheben, dass sich alle Personen selbstständig eingetragen haben.



Die scip AG bedankt sich für Ihr Vertrauen!

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 F-Secure Antivirus-Produkte ARJ-Archive Pufferüberlauf
- 3.2 Symantec verschiedene Produkte DEC2EXE-Modul UPX-Parsing Pufferüberlauf
- 3.3 Microsoft Internet Explorer 5.01 bis 6.0 OBJECT-Tag codebase-Attribut ?.exe Dateien ausführen
- 3.4 Microsoft Internet Explorer 5.01 bis 6.0 Temporary Internet Files Verzeichnis Zonenkonzept Designfehler
- 3.5 Microsoft Internet Explorer 5.01 bis 6.0 JavaScript createControlRange() Pufferüberlauf
- 3.6 Microsoft Internet Explorer 5.01 bis 6.0 CDF CHANNEL Tag Cross Site Scripting
- 3.7 Microsoft Internet Explorer 5.01 bis 6.0 codierte URLs erweiterte Rechte
- 3.8 Microsoft Windows 98 bis XP und Office OLE-Daten erweiterte Rechte
- 3.9 Microsoft Windows 98 bis XP und Office COM-Dateien erweiterte Rechte
- 3.10 Microsoft Office 2000, 2002 und XP URL Verarbeitung Pufferüberlauf
- 3.11 Microsoft Windows XP Named Pipe Verbindungen gibt Benutzernamen preis
- 3.12 Microsoft Windows 2000, XP und Server 2003 SMB Pufferüberlauf
- 3.13 Netscape bis 7.2 International Domain Name Seiten-Informationen vortäuschen
- 3.14 Mozilla Firefox bis 1.0 International Domain Name Seiten-Informationen vortäuschen
- 3.15 Mozilla bis 1.7.5 International Domain Name Seiten-Informationen vortäuschen
- 3.16 Perl bis 5.8.4-2ubuntu0.3 PERLIO_DEBUG Pufferüberlauf
- 3.17 PostgreSQL bis 8.0.1 plpgsql Cursor Deklaration zu viele Parameter Pufferüberlauf
- 3.18 Cisco IOS 12.0 bis 12.3(8) IPv6 mehrere korrupte Pakete Denial of Service

- 3.19 Cisco IOS 9.x bis 12.1(10) BGP bgp log-neighbor-changes korruptes BGP-Paket Denial of Service
- 3.20 ISC BIND 8.4.4 und 8.4.5 q_usedns Array Pufferüberlauf
- 3.21 ISC BIND 9.3.0 DNSSEC authvalidated() fehlerhaftes DNS-Datagramm Denial of Service

3.1 F-Secure Antivirus-Produkte ARJ-Archive Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 10.02.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1215>

F-Secure stellt eine Antiviren-Lösung für verschiedene Plattformen, darunter auch Linux, zur Verfügung. Wie ISS ursprünglich meldete, existiert in den verschiedenen Antiviren-Produkten von F-Secure eine Pufferüberlauf-Schwachstelle bei der Verarbeitung von ARJ-Archiven. Ein Angreifer kann über eine korrupte ARJ-Datei Programmcode auf einem betroffenen System ausführen. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. F-Secure hat Patches für die betroffenen Produkte zum Download bereitgestellt.

Expertenmeinung:

Zusammen mit der UPX-Schwachstelle in den Symantec-Produkten ist dies die weitere wirklich schwerwiegende da flächendeckende Schwachstelle in diesem Monat. Die Entwickler von Computerviren kommen deshalb in den Genuss, neue Systeme erschliessbar machen zu können. Gegenmassnahmen sind zur Prävention von grossangelegten Viren-Übergriffen von erhöhter Dringlichkeit.

3.2 Symantec verschiedene Produkte DEC2EXE-Modul UPX-Parsing Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 08.02.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1205>

Symantec gilt als einer der grössten Hersteller von Sicherheitslösungen. Die Firma ISS hat einen Fehler im DEC2EXE-Modul gefunden. Durch einen Pufferüberlauf beim Parsen von UPX-Archiven kann beliebiger Programmcode ausgeführt werden. Eine exakte Liste der betroffenen Produkte ist im Symantec-Advisory

unter

<http://www.sarc.com/avcenter/security/Content/2005.02.08.html> zu finden. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Hersteller hat Patches für die betroffenen Produkte zur Verfügung gestellt.

Expertenmeinung:

Für Symantec-Produkte ist dies natürlich der Supergau, denn praktisch alle populären Lösungen - vor allem im Antivirus- und Mail-Bereich - sind davon betroffen. Obschon wenige Details zum Fehler bekannt sind, wird das erhöhte Interesse der Angreifer voraussichtlich schnell technische Daten oder gar ein Exploit zu Tage fördern. Dies mag nur eine Frage von Wochen sein, weshalb man sich umgehend dem Umsetzen von Gegenmassnahmen annehmen sollte.

3.3 Microsoft Internet Explorer 5.01 bis 6.0 OBJECT-Tag codebase-Attribut ?.exe Dateien ausführen

Einstufung: **kritisch**

Remote: Ja

Datum: 08.02.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1203>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Andreas Sandblad des Sicherheits-Dienstleisters Secunia entdeckte eine weitere Schwachstelle in Microsoft Internet Explorer 5.01 bis 6.0. Durch einen Designfehler im codebase-Attribut des OBJECT-Tags kann über den Zusatz ?.exe jede beliebige EXE-Datei aus der lokalen Zone ausgeführt werden. Ein Angreifer könnte so eine Hintertür oder ein Trojanisches Pferd starten. Microsoft hat dem Problem mit einem kumulativen Fix des Patchdays von Februar 2005 Rechnung getragen.

Expertenmeinung:

Der Microsoft Internet Explorer schafft es einfach nicht, aus der Schusslinie von Sicherheitsexperten zu kommen. Keinen Monat vergeht, an dem nicht eine neue und brisante Schwachstelle im noch immer beliebten Webbrowser publiziert wird. Wie Zahlen belegen, vermag dies langsam aber stetig am Image der Microsoft-Kreation zu kratzen. Die steigenden Download-Zahlen für die freie Alternative Mozilla Firefox sprechen eine eindeutige Sprache. Eine Vielzahl an Unternehmen denken immer lauter daran, einen alternativen Browser zu ihrem Standard zu machen, um das Sicherheitspositiv

für Web zu erhöhen.

3.4 Microsoft Internet Explorer 5.01 bis 6.0 Temporary Internet Files Verzeichnis Zonenkonzept Designfehler

Einstufung: **kritisch**

Remote: Ja

Datum: 08.02.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1202>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Andreas Sandblad des Sicherheits-Dienstleisters Secunia entdeckte eine weitere Schwachstelle in Microsoft Internet Explorer 5.01 bis 6.0. Durch einen Designfehler im Zonenkonzept des Browsers können zwischengespeicherte Dokumente im Temporary Internet Files Verzeichnis eine Selbstreferenzierung durchführen und so in einem anderen Kontext geladen werden. Erweiterte Rechte für die Webdokumente sind die Folge davon. Zur erfolgreichen Umsetzung der Attacke muss der Angreifer den Benutzernamen des angemeldeten Anwenders, die Verzeichnisstruktur und die Dateinamen kennen. Microsoft hat dem Problem mit einem kumulativen Fix des Patchdays von Februar 2005 Rechnung getragen.

Expertenmeinung:

Der Microsoft Internet Explorer schafft es einfach nicht, aus der Schusslinie von Sicherheitsexperten zu kommen. Keinen Monat vergeht, an dem nicht eine neue und brisante Schwachstelle im noch immer beliebten Webbrowser publiziert wird. Wie Zahlen belegen, vermag dies langsam aber stetig am Image der Microsoft-Kreation zu kratzen. Die steigenden Download-Zahlen für die freie Alternative Mozilla Firefox sprechen eine eindeutige Sprache. Eine Vielzahl an Unternehmen denken immer lauter daran, einen alternativen Browser zu ihrem Standard zu machen, um das Sicherheitspositiv für Web zu erhöhen.

3.5 Microsoft Internet Explorer 5.01 bis 6.0 JavaScript createControlRange() Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 08.02.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1200>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Andreas Sandblad des Sicherheits-Dienstleisters Secunia entdeckte eine kritische Schwachstelle in Microsoft Internet Explorer 5.01 bis 6.0. Die JavaScript-Funktion `createControlRange()` ist gegen eine Pufferüberlauf-Attacke anfällig und kann entsprechend für das Ausführen von beliebigem Programmcode genutzt werden. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Microsoft hat dem Problem mit einem kumulativen Fix des Patchdays von Februar 2005 Rechnung getragen.

Expertenmeinung:

Der Microsoft Internet Explorer schafft es einfach nicht, aus der Schusslinie von Sicherheitsexperten zu kommen. Keinen Monat vergeht, an dem nicht eine neue und brisante Schwachstelle im noch immer beliebten Webbrowser publiziert wird. Wie Zahlen belegen, vermag dies langsam aber stetig am Image der Microsoft-Kreation zu kratzen. Die steigenden Download-Zahlen für die freie Alternative Mozilla Firefox sprechen eine eindeutige Sprache. Eine Vielzahl an Unternehmen denken immer lauter daran, einen alternativen Browser zu ihrem Standard zu machen, um das Sicherheitspositiv für Web zu erhöhen.

3.6 Microsoft Internet Explorer 5.01 bis 6.0 CDF CHANNEL Tag Cross Site Scripting

Einstufung: **kritisch**
Remote: Ja
Datum: 08.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1199>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Paul von den greyhats entdeckte eine Schwachstelle in Microsoft Internet Explorer 5.01 bis 6.0. Der CHANNEL Tag des Channel Definition Format (CDF) ist auf Cross Site Scripting-Attacken anfällig und kann entsprechend für das Ausführen von Programmcode genutzt werden. Ein Exploit zur Schwachstelle ist nicht bekannt. Microsoft hat dem Problem mit einem kumulativen Fix des Patchdays von Februar 2005 Rechnung getragen.

Expertenmeinung:

Der Microsoft Internet Explorer schafft es einfach nicht, aus der Schusslinie von Sicherheitsexperten zu kommen. Keinen Monat vergeht, an dem nicht eine neue und brisante Schwachstelle im noch immer beliebten Webbrowser publiziert wird. Wie Zahlen belegen, vermag dies langsam aber stetig am Image der Microsoft-Kreation zu kratzen. Die steigenden Download-Zahlen für die freie Alternative Mozilla Firefox sprechen eine eindeutige Sprache. Eine Vielzahl an Unternehmen denken immer lauter daran, einen alternativen Browser zu ihrem Standard zu machen, um das Sicherheitspositiv für Web zu erhöhen.

3.7 Microsoft Internet Explorer 5.01 bis 6.0 codierte URLs erweiterte Rechte

Einstufung: **kritisch**
Remote: Ja
Datum: 08.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1198>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Jouko Pynnönen eine Schwachstelle in Microsoft Internet Explorer 5.01 bis 6.0. Durch einen Fehler bei der Handhabung von speziell codierten URLs kann ein Angreifer die Adresszeile fälschen und Code im Kontext anderer Seiten ausführen. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Microsoft hat dem Problem mit einem kumulativen Fix des Patchdays von Februar 2005 Rechnung getragen.

Expertenmeinung:

Der Microsoft Internet Explorer schafft es einfach nicht, aus der Schusslinie von Sicherheitsexperten zu kommen. Keinen Monat vergeht, an dem nicht eine neue und brisante Schwachstelle im noch immer beliebten Webbrowser publiziert wird. Wie Zahlen belegen, vermag dies langsam aber stetig am Image der Microsoft-Kreation zu kratzen. Die steigenden Download-Zahlen für die freie Alternative Mozilla Firefox sprechen eine eindeutige Sprache. Eine Vielzahl an Unternehmen denken immer lauter daran, einen alternativen Browser zu ihrem Standard zu machen, um das Sicherheitspositiv für Web zu erhöhen.

3.8 Microsoft Windows 98 bis XP und Office OLE-Daten erweiterte Rechte

Einstufung: **kritisch**
Remote: Indirekt
Datum: 08.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1195>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Cesar Cerrudo fand eine Schwachstelle beim Umgang mit OLE-Daten Dateien. Diese kann von einem lokalen Angreifer genutzt werden, um erweiterte Rechte zu erlangen. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Eine Vielzahl an Microsoft Produkten ist betroffen. Dies reicht von Windows 98 bis 2003 über Office bis hin zu einigen Zusatzprodukten. Eine komplette Liste ist dem Microsoft Security Bulletin MS05-012 zu entnehmen. Microsoft hat Patches für die betroffenen Produkte bereitgestellt.

Expertenmeinung:

Es sind zwar keine technischen Details zur Schwachstelle bekannt, jedoch macht diese den Anschein, als könnte sie zu einem Klassiker in der lokalen Übernahme eines Windows-Systems werden. Es ist deshalb nur eine Frage der Zeit, bis weitere Informationen die Runde machen werden.

3.9 Microsoft Windows 98 bis XP und Office COM-Dateien erweiterte Rechte

Einstufung: **kritisch**
Remote: Indirekt
Datum: 08.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1194>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Cesar Cerrudo fand eine Schwachstelle beim Zugriff auf COM-Dateien. Diese kann von einem lokalen Angreifer genutzt werden, um erweiterte Rechte zu erlangen. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Eine Vielzahl an Microsoft Produkten ist betroffen. Dies reicht von Windows 98 bis 2003 über Office bis hin zu

einigen Zusatzprodukten. Eine komplette Liste ist dem Microsoft Security Bulletin MS05-012 zu entnehmen. Microsoft hat Patches für die betroffenen Produkte bereitgestellt.

Expertenmeinung:

Es sind zwar keine technischen Details zur Schwachstelle bekannt, jedoch macht diese den Anschein, als könnte sie zu einem Klassiker in der lokalen Übernahme eines Windows-Systems werden. Es ist deshalb nur eine Frage der Zeit, bis weitere Informationen die Runde machen werden.

3.10 Microsoft Office 2000, 2002 und XP URL Verarbeitung Pufferüberlauf

Einstufung: **kritisch**
Remote: Indirekt
Datum: 08.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1192>

Microsoft Office ist eine sehr populäre kommerzielle Office-Suite der bekannten Firma aus Redmond. Teil dieses Pakets sind beispielsweise die Textverarbeitung Word, die Tabellenkalkulation Excel und die Datenbank Access. Microsoft gibt in MS05-005 (KB873352) eine nicht näher beschriebene Pufferüberlauf-Schwachstelle der Verarbeitung von URLs in Microsoft Office 2000, 2002 und XP bekannt. Ein Angriff kann beispielsweise über das Öffnen eines korrupten Links umgesetzt werden. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Microsoft hat Patches für die betroffenen Betriebssystem-Versionen herausgegeben.

Expertenmeinung:

Eine Einschätzung fällt aufgrund des Fehlens von technischen Details nicht leicht. Die Möglichkeiten eines Angriffs könnten jedoch enorm sein. Sollte sich dies herausstellen, würde die Schwachstelle auf ein "sehr kritisch" heraufgestuft werden. Zwischenzeitlich muss man davon ausgehen, dass eine Interaktion des Benutzers erforderlich ist, um den Angriff umzusetzen.

3.11 Microsoft Windows XP Named Pipe Verbindungen gibt Benutzernamen preis

Einstufung: **kritisch**
Remote: Ja
Datum: 08.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1190>

Microsoft Windows XP stellt eine Weiterentwicklung des professionellen Windows 2000 dar. Microsoft publizierte in MS05-007 (KB888302 eine vom Franzosen Jean-Baptiste Marchand gefundene aber nicht näher beschriebene Design-Schwachstelle in Microsoft Windows XP. Einem Angreifer sei es über Named Pipes möglich, sensitive Informationen zur Benutzern mit bestehender NetBIOS-Verbindung einzuholen. Es sind praktisch keine Details zur Schwachstelle und ebenso kein Exploit bekannt. Microsoft hat einen Patch für die betroffenen Betriebssystem-Versionen herausgegeben. Als Workaround wird empfohlen, NetBIOS-Zugriffe mittels Firewalling zu limitieren.

Expertenmeinung:

Es sind zwar keine technischen Details zur Schwachstelle bekannt, jedoch macht diese den Anschein, als könnte sie zu einem Klassiker in der Windows-Auswertung werden. Es ist deshalb nur eine Frage der Zeit, bis weitere Informationen die Runde machen werden.

3.12 Microsoft Windows 2000, XP und Server 2003 SMB Pufferüberlauf

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 08.02.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1189>

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 publizierte in MS05-011 (KB885250) eine nicht näher beschriebene Pufferüberlauf-Schwachstelle in Microsoft Windows 2000, XP und Server 2003. Einem Angreifer sei es möglich, mittels korruptem SMB-Datenverkehr beliebigen Programmcode auf einem System auszuführen. Es sind praktisch keine Details zur Schwachstelle und ebenso kein Exploit bekannt. Microsoft hat einen Patch für die betroffenen Betriebssystem-Versionen herausgegeben. Als Workaround wird empfohlen, NetBIOS-Zugriffe mittels Firewalling zu limitieren.

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

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.

3.13 Netscape bis 7.2 International Domain Name Seiten-Informationen vortäuschen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 06.02.2005
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1181>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, kann jedoch in Punkto Marktanteile mit den anderen Grössen des Genres noch nicht mithalten. Im Dezember 2001 wurden offiziell internationale Domain-Namen eingeführt, bei denen lokalisierte Sonderzeichen (z.B. Umlaute) genutzt werden können. Zur damaligen Zeit unterstützte noch kein populärer Browser die entsprechenden Zeichen. Viele moderne Webbrowser der mit Gecko/khtml können jedoch mit der neuen Funktionalität aufwarten. Eric Johanson entdeckte nun, dass über spezielle Sonderzeichen die Adressleisten, Statusbars und SSL-Zertifikate vorgetäuscht werden können. Von der Schwachstelle ausgeschlossen ist der Microsoft Internet Explorer (MS IEX). Ein Exploit zur Schwachstelle wurde zusammen mit dem Advisory und durch andere Stellen publiziert [<http://www.shmoo.com/idn/>]. Als Workaround wird empfohlen lediglich Links vertrauenswürdiger Herkunft zu folgen.

Expertenmeinung:

Dies ist eine wahrhaftig ernstzunehmende Schwachstelle. In erster Linie ob der Möglichkeiten der Angreifer, die dadurch Phishing- und Social Engineering-Attacken sehr schön umsetzen können. Zusätzlich ist die Anzahl der betroffenen Browser - auch wenn dieses Mal der Microsoft Internet Explorer nicht betroffen ist - erschreckend. Dies verleiht der Schwachstelle einen schlechten Beigeschmack, dem man unbedingt mit Gegenmassnahmen kontern sollte.

3.14 Mozilla Firefox bis 1.0 International Domain Name Seiten- Informationen vortäuschen

Einstufung: **kritisch**
Remote: Ja
Datum: 06.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1176>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, kann jedoch in Punkto Marktanteile mit den anderen Grössen des Genres noch nicht mithalten. Im Dezember 2001 wurden offiziell internationale Domain-Namen eingeführt, bei denen lokalisierte Sonderzeichen (z.B. Umlaute) genutzt werden können. Zur damaligen Zeit unterstützte noch kein populärer Browser die entsprechenden Zeichen. Viele moderne Webbrowser der mit Gecko/khtml können jedoch mit der neuen Funktionalität aufwarten. Eric Johanson entdeckte nun, dass über spezielle Sonderzeichen die Adressleisten, Statusbars und SSL-Zertifikate vorgetäuscht werden können. Von der Schwachstelle ausgeschlossen ist der Microsoft Internet Explorer (MS IEX). Ein Exploit zur Schwachstelle wurde zusammen mit dem Advisory und durch andere Stellen publiziert [<http://www.shmoo.com/idn/>]. Es wird empfohlen auf den IDN-Support mit der Einstellung von network.enableIDN auf false zu verzichten. Als Workaround wird empfohlen lediglich Links vertrauenswürdiger Herkunft zu folgen.

Expertenmeinung:

Dies ist eine wahrhaftig ernstzunehmende Schwachstelle. In erster Linie ob der Möglichkeiten der Angreifer, die dadurch Phishing- und Social Engineering-Attacken sehr schön umsetzen können. Zusätzlich ist die Anzahl der betroffenen Browser - auch wenn dieses Mal der Microsoft Internet Explorer nicht betroffen ist - erschreckend. Dies verleiht der Schwachstelle einen schlechten Beigeschmack, dem man unbedingt mit Gegenmassnahmen kontern sollte.

3.15 Mozilla bis 1.7.5 International Domain Name Seiten- Informationen vortäuschen

Einstufung: **kritisch**
Remote: Ja
Datum: 06.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1175>

[bin/smss/showadvf.pl?id=1175](http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1175)

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, kann jedoch in Punkto Marktanteile mit den anderen Grössen des Genres noch nicht mithalten. Im Dezember 2001 wurden offiziell internationale Domain-Namen eingeführt, bei denen lokalisierte Sonderzeichen (z.B. Umlaute) genutzt werden können. Zur damaligen Zeit unterstützte noch kein populärer Browser die entsprechenden Zeichen. Viele moderne Webbrowser der mit Gecko/khtml können jedoch mit der neuen Funktionalität aufwarten. Eric Johanson entdeckte nun, dass über spezielle Sonderzeichen die Adressleisten, Statusbars und SSL-Zertifikate vorgetäuscht werden können. Von der Schwachstelle ausgeschlossen ist der Microsoft Internet Explorer (MS IEX). Ein Exploit zur Schwachstelle wurde zusammen mit dem Advisory und durch andere Stellen publiziert [<http://www.shmoo.com/idn/>]. Es wird empfohlen auf den IDN-Support mit der Einstellung von network.enableIDN auf false zu verzichten. Als Workaround wird empfohlen lediglich Links vertrauenswürdiger Herkunft zu folgen.

Expertenmeinung:

Dies ist eine wahrhaftig ernstzunehmende Schwachstelle. In erster Linie ob der Möglichkeiten der Angreifer, die dadurch Phishing- und Social Engineering-Attacken sehr schön umsetzen können. Zusätzlich ist die Anzahl der betroffenen Browser - auch wenn dieses Mal der Microsoft Internet Explorer nicht betroffen ist - erschreckend. Dies verleiht der Schwachstelle einen schlechten Beigeschmack, dem man unbedingt mit Gegenmassnahmen kontern sollte.

3.16 Perl bis 5.8.4-2ubuntu0.3 PERLIO_DEBUG Pufferüberlauf

Einstufung: **kritisch**
Remote: Indirekt
Datum: 02.02.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1172>

Perl ist eine offene und sehr populäre Skript-/Programmiersprache, die vor allem auf Linux-Systemen ihren Einsatz findet. Der Linux-Distribution Ubuntu weist in seiner Security Notice USN-72-1 auf zwei Fehler in Perl 5.x hin. Beide betreffen die Umgebungsvariable PERLIO_DEBUG. Diese weist einen Pufferüberlauf auf und kann deshalb für das

Ausführen beliebigen Programmcodes missbraucht werden. Exakte Details zur Schwachstelle wurden nicht bekannt gegeben. Der Fehler wurde in 5.8.4-2ubuntu0.3 behoben. Als Workaround wird empfohlen, nur vertrauenswürdigen Benutzern Zugriff auf ein gefährdetes System zu gewähren.

Expertenmeinung:

Problematisch an dieser Schwachstelle ist sicher die sehr hohe Verbreitung von Perl, das praktisch auf jedem Unix/Linux System seinen festen Platz hat. Lokale Angreifer könnten entsprechend den Umstand nutzen, um das System zu kompromittieren. Das Umsetzen von Gegenmassnahmen ist deshalb von erhöhter Wichtigkeit.

3.17 PostgreSQL bis 8.0.1 plpgsql Cursor Deklaration zu viele Parameter Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 01.02.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1169>

PostgreSQL ist eine hoch skalierbare, SQL-kompatible und unter der open-source Lizenz herausgegebene relationale Datenbank. Das PostgreSQL Team meldete drei Sicherheitslücken in ihrer Lösung. Wie das Entwickler-Team in einem Mailing bekannt gab, existiert eine Pufferüberlauf-Schwachstelle bei der Verarbeitung zu vieler Cursor Deklarationen in plpgsql. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Fehler wurde in den Versionen 8.0.1, 7.4.7, 7.3.9 und 7.2.7 behoben. Ein Upgrade ist entsprechend anzuraten.

Expertenmeinung:

Eine unschöne Schwachstelle, die eindeutig auf Nachlässigkeit bei der Entwicklung zurückzuführen ist. Da es sich hierbei schon fast um einen klassischen Fehler handelt, ist das Verstehen und Umsetzen dieses durch Angreifer keiner allzu hohen Hürde unterworfen. In betroffenen Umgebungen sollte man mit dem Einspielen der neuen PostgreSQL Version nicht warten.

3.18 Cisco IOS 12.0 bis 12.3(8) IPv6 mehrere korrupte Pakete Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 26.01.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1164>

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. Jüngere Versionen des Cisco IOS sind in der Lage, das zukünftige IPv6 zu unterstützen. Wie Cisco meldet, existiert eine Denial of Service-Schwachstelle bei der Verarbeitung mehrerer korrupter IPv6-Pakete. Zur erfolgreichen Ausnutzung muss der IPv6-Support entsprechend aktiviert sein, was standardmässig nicht der Fall ist. Eine Anzeige der IPv6 unterstützenden Interfaces kann mit der Eingabe von "show ipv6 interface" gemacht werden. Genaue technische Details oder ein Exploit zum Angriff sind nicht bekannt. Cisco hat einen Patch für die betroffenen IOS-Versionen herausgegeben. Als Workaround kann eine ACL eingesetzt oder das Kommando Deaktivieren von IPv6 umgesetzt werden.

Expertenmeinung:

Angriffe auf Cisco-Elemente sind aufgrund ihrer Verbreitung sehr beliebt. So kann man an dieser Stelle von Glück sprechen, dass sich dieser Remote-Angriff nur durchführen lässt, wenn auf dem verwundbaren System IPv6 aktiviert ist. Wird eines dieser Features nicht benötigt, sollte man es deaktivieren, um möglichst wenig Angriffsfläche zu bieten. Zusätzlich sollte man die neueste Version des IOS einspielen.

3.19 Cisco IOS 9.x bis 12.1(10) BGP bgp log-neighbor-changes korruptes BGP-Paket Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 26.01.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1162>

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 Cisco IOS unterstützt standardmässig das Border Gateway Protocol (BGP), welches zur Propagierung von Verfügbarkeit von Verbindungswegen zwischen Routern genutzt wird [<http://de.wikipedia.org/wiki/BGP>]. Wie Cisco meldet, existiert eine Denial of Service-Schwachstelle bei der Verarbeitung korrupter BGP-Pakete. Zur erfolgreichen Ausnutzung

muss BGP und das Kommando "bgp log-neighbor-changes" am Zielsystem aktiviert sein. Genaue technische Details oder ein Exploit zum Angriff sind nicht bekannt. Cisco hat einen Patch für die betroffenen IOS-Versionen herausgegeben. Als Workaround kann eine ACL eingesetzt oder das Kommando "bgp log-neighbor-changes" entfernt werden. Instruktionen zur Umsetzung des letzteren Lösungsansatzes finden sich online unter http://www.cisco.com/en/US/products/sw/iosswre/ps5187/products_command_reference_chapter09186a008017d026.html#wp1040601

Expertenmeinung:

Angriffe auf Cisco-Elemente sind aufgrund ihrer Verbreitung sehr beliebt. So kann man an dieser Stelle von Glück sprechen, dass sich dieser Remote-Angriff nur durchführen lässt, wenn auf dem verwundbaren System BGP aktiviert ist. Wird eines dieser Features nicht benötigt, sollte man es deaktivieren, um möglichst wenig Angriffsfläche zu bieten. Zusätzlich sollte man die neueste Version des IOS einspielen.

3.20 ISC BIND 8.4.4 und 8.4.5 q_usedns Array Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 25.01.2005
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1159>

BIND ist die mit abstand populärste Nameserver-Implementierung, die von ISC betreut wird. Das Entwickler-Team hat auf der Webseite nun bekanntgegeben, dass eine Denial of Service-Schwachstelle im Array q_usedns besteht. Ein Angreifer kann darüber aber angeblich nur eine Denial of Service umsetzen. Von der Schwachstelle betroffen sind ausschliesslich ISC BIND 8.4.4 und 8.4.5. Sodann wird ein Update auf eine aktualisierte BIND-Version empfohlen.

Expertenmeinung:

Es ist traurig aber wahr: Einmal mehr ist die Sicherheit des Internets durch Schwachstellen in der beliebten BIND-Software gefährdet. Wer ein solches System im Einsatz hat, der sollte unverzüglich die entsprechenden Patches einspielen, um weitreichenden Angriffen vorzubeugen.

3.21 ISC BIND 9.3.0 DNSSEC authvalidated() fehlerhaftes DNS- Datagramm Denial of Service

Einstufung: **kritisch**
Remote: Ja

Datum: 25.01.2005
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1158>

BIND ist die mit abstand populärste Nameserver-Implementierung, die von ISC betreut wird. Das Entwickler-Team hat auf der Webseite nun bekanntgegeben, dass eine Denial of Service-Schwachstelle in der Funktion authvalidated() besteht. Ein Angreifer kann mittels einem fehlerhaften DNS-Datagramm den internen Konsistenz-Test zu einem Absturz bewegen. Sodann beendet sich der named-Daemon. Um den Angriff erfolgreich umzusetzen, muss auf dem Zielsystem DNSSEC aktiviert sein, was standardmässig nicht der Fall ist. ISC hat eine aktualisierte Version von BIND herausgegeben. Als Workaround kann entsprechend DNSSEC mittels "dnssec-enable no" deaktiviert werden.

Expertenmeinung:

Es ist traurig aber wahr: Einmal mehr ist die Sicherheit des Internets durch Schwachstellen in der beliebten BIND-Software gefährdet. Wer ein solches System im Einsatz hat, der sollte unverzüglich die entsprechenden Patches einspielen, um weitreichenden Angriffen vorzubeugen.

4. Fachartikel

4.1 Phishing im Zentrum von Penetration Tests

Marc Ruef

Penetration Tests, das zielgerichtete und „aggressive“ Überprüfen der Sicherheit von Systemen, wird auch zunehmend in unseren Breitengraden in Sicherheitsprozesse eingebunden. Dass dabei die technologische Angriffsfläche bei weitem nicht das meiste Gefahrenpotential in sich birgt, wird oft vergessen oder schlicht nicht wahrgenommen.



Bei Penetration Tests (Abk. PenTest oder PT) wird versucht, zielgerichtet die Sicherheit eines Systems zu untergraben, um in der Praxis die bestehenden Sicherheitslücken und die realen Gefahren dieser zu bestimmen. Als Erweiterung zu einem breitflächigen Security Audit können so die letzten Schlupflöcher ausgemacht und vermeintliche Sicherheitslücken zweifelsfrei festgestellt werden.

Penetration Testing ist dabei für viele Sicherheitsdienstleister und Kunden eine rein technische Disziplin: Security Scanner und Exploits sollen innert kürzester Zeit für Erfolge sorgen, in Systeme einbrechen und sensitive Daten zusammentragen. Dabei wird übersehen, dass die Sicherheit einer Umgebung eben auch und vor allem ganz besonders von menschlichen Faktoren abhängt. Falsches Verhalten von Administratoren, Benutzern und Kunden kann fatale Folgen für ein System haben – Nicht selten haben ein kleiner Fauxpas viel mehr Durchschlagskraft, weder der hundertste Remote-Exploit zu einer Webserver-Sicherheitslücke.

Die Gefahren von Social Engineering

Die Geschichte der Computerkriminalität lehrt uns, dass eine Vielzahl an Einbrüchen durch psychologische Tricks initiiert oder gar umgesetzt wurden. Kevin Mitnick, er galt als einer von Amerikas Superhackern, gelang mitunter durch einige simple Telefonanrufe der Einbruch in „hochsichere Computernetze“ bekannter Firmen: Oftmals wurde einfach nach den sensitiven Informationen „gefragt“.

Nachdem er 1995 inhaftiert (eine erste Anhörung

wurde ihm jedoch erst zwei Jahre später zuteil!) und im Januar 2002 vorzeitig entlassen wurde, publizierte er ein Buch mit dem Titel „The Art of Deception: Controlling the Human Element of Security“ – Eine ausgezeichnete Abhandlung darüber, wie effizient Social Hacking sein kann und wie sich derlei Angriffe umsetzen lassen. Der Erfolg des Buches in der Fachwelt und das noch dieses Jahr erscheinende Nachfolgewerk „The Art Of Intrusion: The Real Stories Behind The Exploits Of Hackers, Intruders, And Deceivers“ (11. Februar 2005) geben Mitnick Recht.

Ein praxisorientiertes Fallbeispiel

Kann man den Kunden vom Nutzen von Social Engineering in einem Penetration Test-Projekt überzeugen, gilt es natürlich einen entsprechenden und vor allem realistischen Fall zu konstruieren. Ich möchte hier eine Phishing-Attacke, die wir für einen unserer Kunden umgesetzt haben, kurz dokumentieren.

Im Rahmen des regulären Penetration Tests, bei dem nach wie vor die technischen Aspekte im Mittelpunkt standen, wurden in einer ersten Footprinting-Phase durch verschiedene Medien die Mailadressen der Mitarbeiter der Organisation zusammengetragen. Eine Vielzahl an Adressen waren öffentlich auf der Unternehmens-Webseite zugänglich. Aber auch klassische Abfragen bei Google (z.B. @scip.ch) liessen die Liste der Mitarbeiter und ihrer Mailadressen anwachsen. Diese Daten sind die grundlegende Ausgangslage für einen entsprechenden Social Hacking-Angriff via Email (sie können jedoch auch bei einem Telefonat Verwendung finden).

Der Honigtopf lockt

Unsere Absicht eines Phishing-Angriffs war es, sämtlichen Mitarbeitern ein Email mit gefälschter Absenderadresse von der IT-Administration zu schicken. In unserem Schreiben wiesen wir darauf hin, dass eine Erweiterung der Kommunikationsplattform im Unternehmen geplant sei. Unter anderem sei eine Messageing-Lösung samt Webcams geplant. Die Test-Phasen seien am Anlaufen und wer Interesse an einer Teilnahme habe, der solle seine Kontaktdaten auf einem extra dafür eingerichteten Webserver eingeben, damit die entsprechenden administrativen und technischen Schritte eingeleitet werden können.

Der Trick bestand nun darin, dass der vermeintlich interne Webserver gar nicht zur Firma gehörte, sondern unabhängig von dieser

aufgesetzt wurde. Die Benutzer, die also dort ihre Namen, Mailadressen, Benutzernamen und Passwörter eingaben, stellten eben diese Daten externen Personen – unserem Auditoren-Team - zur Verfügung. Als Begründung, warum die sensitiven Kontoinformationen übertragen werden müssen, können verschiedene herhalten. So hat sich der Benutzer auf dem Formular zweifelsfrei zu identifizieren – Oder die Installation der Webcam soll ausserhalb der Arbeitszeiten durch das IT-Personal umgesetzt werden. Viele Anwender werden sich sowieso nicht darum kümmern ob und inwiefern sie nun ihre Passwörter angeben müssen.

Es galt nun also, eine Webseite mit Formular im Stil des Zielunternehmens zu erstellen. Dabei wurde sich eng an die Aufmachung der öffentlich zugänglichen Homepage der Organisation gehalten. Das HTML-Gerüst und die Bilder wurden übernommen und nur geringfügig den eigenen Zwecken angepasst. Auf den ersten Blick sah es also wirklich so aus, als handle es sich um eine offizielle Intranet-Seite.

Die vermeintlich echte Nachricht

Der Kommunikationsaustausch, der das Opfer zu einer (ersten) Aktion bewegen soll, will gut überlegt und mindestens so akribisch vorbereitet sein. So muss die Nachricht – in unserem Fall ein Email – ein Maximum an Authentizität aufweisen. Dies beginnt beim Wortlaut des Schreibens, das höflich aber bestimmend ausfallen hat. Der Mitarbeiter soll schon allein am Klang der Worte das Gefühl haben, als sei das Vorgehen durch das oberste Management bewilligt und unterstützt.

Zusätze wie eine griffige Betreffzeile und eine echt erscheinende Signatur sind ebenfalls von enormer Wichtigkeit. Ein Email erscheint automatisch vertrauenswürdiger, wenn an diesem eine Disclaimer- oder Antiviren-Nachricht angefügt wird.

Ebenfalls gilt es eine Nachricht technisch so authentisch wie möglich erscheinen zu lassen. Das in RFC 821 spezifizierte Simple Mail Transport Protocol zur Übermittlung von Emails kann sehr einfach zur Fälschung von Absenderadressen bewegt werden. Die wahre Herkunft eines Schreibens kann nur mit erweiterten technischen Kenntnissen, die eine Vielzahl der normalen Computerbenutzer nicht mitbringen, herausgefunden werden.

“Thanks for all the Fish...”

Nachdem die Mailadressen zusammengetragen, scip monthly Security Summary
Marc Ruef & Simon Zumstein
scip_mss-19_02_2005-1.doc

eine gefälschte Webseite aufgesetzt und das vermeintliche echte Email an die Mitarbeiter verschickt wurde, heisst es nun nur noch: Abwarten und Tee trinken, bis ein Fisch ins Netz geht...

Es verging nur wenige Minuten, bis ein erster Benutzer, sich eben für die Webcam interessierend, seine Daten auf dem gefälschten Web-Formular eingegeben hat - Benutzername und Kennwort inklusive! Der Beweis war erbracht: Die Mitarbeiter des Unternehmens sind sich der fehlenden Authentizität von elektronischen Nachrichten nicht bewusst. Das Anstreben von entsprechenden Awareness-Schulungen sollte ein zentraler Punkt bei der Verbesserung der Unternehmenssicherheit sein.

Fazit

Phishing war in den letzten Monaten einer der meist genutzten Mode-Begriffe der Massenmedien. Social Hacking ist aber mindestens so alt wie die Menschheit selbst. Doch nur weil eine Angriffsform längst bekannt ist, heisst es noch lange nicht, dass wir sie akzeptieren oder gar ignorieren dürfen. Gerade in unserer technokratischen Gesellschaft sind psychologische Tricks, die durch die schillernde Technik imposant in Szene gesetzt wurden, das mitunter grösste Risiko für Dienstleister und Nutzer.

5. Kreuzworträtsel

DOS: Löscht Dateien	↓	TCP-Flagge für das abrupte Beenden einer Sitzung	DOS: Zeigt die Uhrzeit an	Freeware Security Scanner	↓	Verbindungsloses Transportprotokoll	↓	DOS: Kopiert Dateien	Liste für Zugangskontrolle	↓	Gleitkomma-Processor	↓	DOS: Vergleicht den Inhalt von Dateien	Übertragungsgeschwindigkeit
↻ 4				Featurepack von Checkpoint				Advanced Program-to-Program Communication					Laufzeitbibliothek	
Computer Emergency Response Team								Umarmung und Küsse			Virtual Private Network	UNIX-Kommando äquivalent zu dir unter DOS		
Künstliche Intelligenz			↻ 1							Bezeichnung für einen Computer-Freak				
↵		Soll den Data Encryption Standard ablösen		Niedliche Nennung weiblicher Hacker		32-Bit-Bus	Europ. Institut für Normung		Wer behauptete, Linux hätte Quelltext gestohlen					
Internationales Standardisierungsinstitut			Weiterentwicklung der SMS	↵					↻ 8			Digital-Analog-Wandler	TCP-Flagge für Bestätigung	
↵		↻ 5		Aho, Weinberger, Kernighan	↻ 3			Wagenrücklauf			Datenfernbürgung	↻ 6		
Vorgänger von Windows 2000								Korrektur des Programmcodes			Datensync			
↵		E-Mail Standard		AES Auswahl Endspiel Teilnehmer					Elektronische Datenverarbeitung	Einmal pro Schachpartie & Partei				
Internet Protocol			Projekt: Suche nach ausserirdischem Leben		Gedruckte Schaltung					Name server-Implementierung				
Privatpersonen TLD				Linux: Kopiert Dateien		Graphische Bedienoberfläche								
↵			↻ 7	Javascript										
↵				Unix: Löschen einer Datei										
Top-Level-Domain von Schweden														
										↻ 2				

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 **15.03.2004**. 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 einen Monat des [Securitytracker](#) Dienstes **)pallas(**.

SECURITYTRACKER



6. Impressum

Herausgeber:

scip AG

Technoparkstrasse 1

CH-8005 Zürich

T +41 1 445 1818

<mailto:info@scip.ch>

<http://www.scip.ch>

Zuständige Person:

Marc Ruef

Security Consultant

T +41 1 445 1812

<mailto:maru@scip.ch>

PGP:

http://www.scip.ch/firma/facts/maru_scip_ch.asc

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Nutzen Sie unsere Dienstleistungen!

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

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!](#)