

Contents

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

1. Editorial

IT-Security ist keine Wissenschaft

Die Sicherstellung der Integrität und Vertraulichkeit zu übermittelnder Daten war mit ein ausschlaggender Grund zur Geburt der ersten Computersysteme (Zuse Z1, Enigma etc.). Der Wettlauf hat seinen Anfang genommen. Denn das Prinzip von actio und reactio nach Isaac Newton (1643-1727) besagt, dass auf jede Aktion gleichzeitig eine gleichwertige Reaktion folgt. Dieses physikalische Prinzip gilt, interessanterweise auch bei uns Menschen. Die Reaktion auf die Aktion zur „sicheren“ Übermittlung sensibler Daten war die Suche nach einem potenteren System, welches diese „sicheren“ Daten zu „entsichern“ vermag. Neben diesem direkten Aufeinandertreffen auf gleicher, technischer Ebene wurden auch die Umsysteme angegangen. Welche Informationen können durch Spionage, Personenmanipulation etc. erlangt werden. Ein ganzes Spinnennetz wurde gesponnen. Ganzheitliche IT-Security ist demnach keine Neuheit.

An den Grundzügen hat sich bis heute nichts geändert. Up-to-date Security Richtlinien

beschreiben genau eine solche Landschaft unterschiedlicher Auswirkungen: Physikalische Sicherheit, organisatorische Sicherheit, rechtliche Sicherheit, technische Sicherheit etc.

Eine solche Kontinuität steigert die Möglichkeit einer einheitlichen Auslegung und Beurteilung eines Themengebietes. Im Fall der IT-Security leider zu unrecht. Doch wieso dieser Lapsus? Bestimmt sind unterschiedliche Gründe dafür verantwortlich, weshalb es bis heute noch keine allgemeingültige und einheitliche Bewertung von Sicherheitsfaktoren gibt.

Einer dieser Gründe ist bestimmt die Ausdehnung der in IT-Security Audits betrachteten Regionen. Es gilt die Architektur aufgrund vorhandener Dokumentationen zu beurteilen. Ebenso gilt es die organisatorischen Massnahmen wie Abläufe, Katastrophenvorsorge, Security Awareness Vorkehrungen etc. zu begutachten als auch rechtliche Grundlagen wie Geldwäscherei etc. miteinzubeziehen. Zudem sind die technischen Mechanismen in verschiedenen Tiefen zu analysieren und zu bewerten. Schlussendlich sollten die in den Security Policies, strategischen Dokumenten und Konzepten definierten Muss-Kriterien eingehalten werden. Eine einheitliche und allgemeingültige Beurteilungsmatrix über alle Bereiche ist, nachvollziehbar, nicht vorhanden. Zu unterschiedlich sind die einzelnen Bereiche.



Zu unterschiedlich sind die einzelnen Bereiche.

Versuchen wir es in einem Teilbereich. Betrachten wir die technische Sicherheit gesondert. Hier sollte es möglichst einen seinen gewünschten allgemeingültigen Standard zu definieren. Weit gefehlt, denn IT-Security ist keine Wissenschaft. Damit fehlen die Grunddefinitionen, auf welche man sich abstützen könnte. Anders als z.B. in der Mathematik. Eine Subtraktion zweier Werte läuft dabei immer nach den gleichen definierten und

allgemeingültigen Regeln ab. Durch das Fehlen von Grunddefinitionen können zum Beispiel auch keine vergleichbaren Zuweisungen von Verletzbarkeiten durchgeführt werden. Jede Firma oder jedes Institut definiert ihren eigenen Standard. Da diese Standards in Worten verfasst werden, ist eine genaue Zuweisung von Ereignissen nicht umsetzbar. Der Verfasser kann subjektiv entscheiden, wie er eine Lücke bestimmt. Damit können auf solche Zuweisung bauende Berechnungen des Institut A nicht mit Berechnungen der Firma F verglichen werden. Das Resultat kann Irregularitäten aufweisen.

Selbst in einem homogenen Umfeld einer einzelnen Firma können sich, durch subjektive Einschätzung unterschiedlicher Personen (in z.B. Ferienabwesenheiten), Berechnungsfehler einschleichen. Die Ende Monat an den verantwortlichen Ressortleiter übergebene Auswertung der Security-Vorfälle könnte somit andere Werte enthalten wie wenn der Zuständige keine Ferien hätte.

Ein Traum ist eine Formel, in welcher z.B. die Firewalls die Wurzel, die Zone den Wurzelexponenten stellen und als Radikand eine Multiplikation einer errechneten Verletzbarkeit mit einer Systemvariablen wären. Somit könnte auf technischer Ebene die Sicherheitskotsante eindeutig und wiederlegbar festgesetzt werden.

Der nachvollziehbare und gerechtfertigte Wunsch der Verantwortlichen eines Benchmarkings mit vergleichbaren Firmen kann derzeit nur basierend auf Erfahrungswerten und Best-Practice Ansätzen halbwegs befriedigt werden.

In einer auf die Informationstechnologie vertrauenden Gesellschaft (denken Sie nur an die Militärs, Ihre Bank, Ihren Stomversorger oder die medizinischen Präzisionsgerätschaften etc.) ist es an der Zeit, dass die IT-Security den Wandel von Best-Practice Ansätzen zur Wissenschaft in Angriff nimmt.

Im Bereich Organisation darf die subjektive Einschätzung nie umgangen werden. Die Definierung einer entsprechenden Formel ist wohl nie aufzulösen - wobei ich doch einmal in einem Buch die Antwort auf den Wunsch verschiedener Mathematiker, die Lebensformel, respektive das Ergebnis davon gelesen habe: 42!

Simon Zumstein <sizu@scip.ch>
Geschäftsleiter
Zürich, 19. Oktober 2004

2. scip AG Informationen

2.1 scip monthly Security Summary-Redesign

Die scip AG veröffentlicht seit dem 19. Februar 2003 den scip monthly Security Summary (smSS). Wir sind stolz darauf, über **640 Personen** zu unserer Leserschaft zählen zu dürfen.

Wobei es sich ausschliesslich um Personen handelt, welche sich **selbst** angemeldet haben!

SECURITY SUMMARY



Die Form des scip monthly Security Summary ist seit Beginn, am 19. Februar 2003, unverändert. Einzig einige Themenbereiche wurden, aufgrund einer Leserbefragung, angepasst, ersetzt oder entfernt.

Wir planen ein Redesign des smSS auf den 19. Januar 2005. Alle Leserinnen und Leser sind eingeladen, uns Ihre Wünsche und Ideen zukommen zu lassen. Sei dies zu neuen Themenbereichen, Darstellungsform, Versandart etc.

Senden Sie uns Ihre Ideen und Anregungen an info@scip.ch oder nehmen Sie telefonisch Kontakt mit uns auf über +41 1 445 1818 und verlangen Sie Herrn Zumstein oder Herrn Ruef.

Wir freuen uns auf Ihre Anregungen!

3. Neue Sicherheitslücken

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

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

Contents:

- 3.1 Microsoft Windows XP JPEG ActiveX Image Control asycpict.dll Denial of Service
- 3.2 3Com OfficeConnect ADSL Wireless 11g Firewall Router bis 1.05 app_sta.stm fehlende Authentisierung
- 3.3 Microsoft Windows Program Group Converter GRP-Datei Pufferüberlauf
- 3.4 Microsoft Windows Kommandozeile Pufferüberlauf
- 3.5 Microsoft Internet Explorer 5.01 bis 6 SSL-Cache SSL-Seiten vortäuschen
- 3.6 Microsoft Internet Explorer 5.01 bis 6 Install Engine Inseng.dll Pufferüberlauf
- 3.7 Microsoft Internet Explorer 5.01 bis 6 korruptes Cascading Style Sheet Pufferüberlauf
- 3.8 Microsoft Windows NetDDE korruptes NetDDE-Paket Pufferüberlauf
- 3.9 Squid bis 2.5.STABLE7 asn_parse_header() Denial of Service
- 3.10 Samba bis 2.2.11 und bis 3.0.5 unix_clean_name() erweiterte Schreibrechte
- 3.11 Microsoft SQL Server 7.0 bis SP3 Denial of Service
- 3.12 Symantec Firewall/VPN 100/200/200R und Gateway Security 320/360/360R SNMP community nicht veränderbar
- 3.13 Symantec Firewall/VPN 100/200/200R und Gateway Security 320/360/360R udp/53 Filter-Regelwerk umgehen
- 3.14 Symantec Firewall/VPN 100/200/200R UDP-Portscan Denial of Service

3.1 Microsoft Windows XP JPEG ActiveX Image Control asycpict.dll Denial of Service

Einstufung: **kritisch**
 Remote: Ja
 Datum: 18.10.2004
 scip DB: [http://www.scip.ch/cgi-](http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=908)

[bin/smss/showadvf.pl?id=908](http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=908)

Microsoft ist der weltweit grösste Softwarehersteller mit Hauptsitz in Redmond, einem Vorort von Seattle (US-Bundesstaat Washington). Das Unternehmen wurde 1975 von Bill Gates und Paul Allen gegründet [<http://de.wikipedia.org/wiki/Microsoft>]. Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Microsoft Windows XP stellt eine Weiterentwicklung des professionellen Windows 2000 dar. Es wurde erneut eine Schwachstelle in Windows XP bei der Verarbeitung von JPEG-Dateien gemeldet. Dieses Mal ist die ActiveX-Komponente Image Control betroffen, die bei fehlerhaften Werten in "Image Height" und "Image Width" eine Denial of Service in der Systembibliothek asycpict.dll verursacht. Dadurch wird der komplette Arbeitsspeicher ausgelastet, was einen Reboot des Systems erfordert, um den normalen Betriebszustand wieder herstellen zu können. Dazu reicht im Normalfall das Anzeigen eines korrupten HTML-Dokuments. Diese Sicherheitslücke hat scheinbar nichts mit der bereits bekannten JPEG-Schwachstelle in Microsoft Windows zu tun [scip ID 833, <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=833>]. Laut Bissell sei es auch nicht möglich, über das Sicherheitsloch Code einzuschleusen und auszuführen. Ein Patch gegen das Problem steht bislang nicht zur Verfügung. Windows XP mit Service Pack 2 scheinen jedoch nicht betroffen zu sein, da dort die Bibliothek asycpict.dll nicht vorhanden ist.

Expertenmeinung:

Eine weitere Schwachstelle von Microsoft Windows, die das beliebte Bildformat JPEG betrifft. Dies liess natürlich einmal mehr die Leute aufschrecken, da man die gleichen Ausmasse wie bei der letzten JPEG-Sicherheitslücke vermutete. Es kann jedoch zu einem gewissen Teil Entwarnung gegeben werden, da sich mit der jüngsten Schwachstelle lediglich eine Denial of Service umsetzen lässt. Trotzdem ist dies natürlich ärgerlich und wird den Skript-Kiddies einmal mehr Spass mit dem Abstürzen von Windows bescheren können.

3.2 3Com OfficeConnect ADSL Wireless 11g Firewall Router bis 1.05 app_sta.stm fehlende Authentisierung

Einstufung: **kritisch**
 Remote: Ja

Datum: 15.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=905>

Die OfficeConnect-Reihe der Firma 3com ist eine Appliance Box für Privatanwender und KMUs. Die Geräte bieten in der Regel die Funktionalität eines Hubs/Switches, gewisse Firewalling-Funktionalität und optionale Wireless LAN-Unterstützung. 3Com OfficeConnect ADSL Wireless 11g Firewall Router bietet all dies samt Verbindungsmöglichkeit zu ADSL. Unabhängig von den diese Tage vom Hersteller 3com gemeldeten Schwachstellen im Produkt hat ebenfalls KarbOnOxyde eine Sicherheitslücke bekannt gegeben. Wird über das Web-Interface ein direkter HTTP-Zugriff auf das Dokument `app_sta.stm` umgesetzt, kann ein Angreifer ohne Authentisierung sensitive Informationen wie zum Beispiel den Benutzernamen und das Passwort für die Verbindungen zum ISP auslesen. Die Schwachstelle wurde in der Firmware 1.05 bestätigt, könnte aber auch andere betreffen. Ob das Problem in der jüngsten Firmware 1.27 behoben wurde, ist nicht bekannt. Als Workaround wird empfohlen, den Zugriff auf das Web-Interface zu limitieren.

Expertenmeinung:

Dieser Fehler ist durchaus kritisch, da die 3com-Elemente gerne genutzt sind, der Angriff einfach ausgenutzt werden kann und ein direkter Zugriff auf sensitive Informationen möglich ist. Es ist nur eine Frage der Zeit, bis die gängigen CGI-Scanner den Web-Zugriff automatisiert durchführen können - Und spätestens dann wird ein Mehr an Angriff auf die entsprechenden 3com-Geräte festgestellt werden können.

3.3 Microsoft Windows Program Group Converter GRP-Datei Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 12.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=900>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Der Hersteller macht im kombinierten Microsoft Security Bulletin MS04-037 auf eine Pufferüberlauf-Schwachstelle bezüglich des Group Converters aufmerksam. So sei es möglich, mittels einer korrupten GRP-Datei eine Denial of Service umzusetzen oder beliebigen

Programmcodes auszuführen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Die Schwachstelle kann mitunter mit dem Microsoft Baseline Security Analyzer (MBSA) verifiziert und halb-automatisch behoben werden. Microsoft hat Patches für die betroffenen Windows-Versionen herausgegeben, die sich ebenfalls über das AutoUpdate installieren lassen. Von der Schwachstelle betroffen sind Microsoft Windows 95, 98, 98SE, ME, NT 4.0, 2000, XP und Server 2003. Microsoft Windows XP mit installiertem Service Pack 2 ist ebenso gegen diese Schwachstelle gesichert, wie ein Windows-System nach der Installation des innerhalb des Patchdays herausgegebenen Bugfixes.

Expertenmeinung:

Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Rund 21 neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.4 Microsoft Windows Kommandozeile Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 12.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=899>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. Der Hersteller macht im kombinierten Microsoft Security Bulletin MS04-037 auf eine Pufferüberlauf-Schwachstelle bezüglich der Kommandozeile (engl. shell) aufmerksam. So sei es möglich, mittels speziellen Aufrufen und Kommandos eine Denial of Service umzusetzen oder beliebigen Programmcodes auszuführen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Die Schwachstelle kann mitunter mit dem Microsoft Baseline Security Analyzer (MBSA) verifiziert und halb-automatisch behoben werden. Microsoft hat Patches für die betroffenen Windows-Versionen herausgegeben, die sich

ebenfalls über das AutoUpdate installieren lassen. Von der Schwachstelle betroffen sind Microsoft Windows 95, 98, 98SE, ME, NT 4.0, 2000, XP und Server 2003. Microsoft Windows XP mit installiertem Service Pack 2 ist ebenso gegen diese Schwachstelle gesichert, wie ein Windows-System nach der Installation des innerhalb des Patchdays herausgegebenen Bugfixes.

Expertenmeinung:

Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Rund 21 neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.5 Microsoft Internet Explorer 5.01 bis 6 SSL-Cache SSL-Seiten vortäuschen

Einstufung: **kritisch**
Remote: Ja
Datum: 12.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=896>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Microsoft beschreibt im Microsoft Security Bulletin MS04-038 den kumulativen Patch für den hauseigenen Internet Explorer (834707). So wurde im Rahmen des allmonatlichen Patchdays von Microsoft bekannt gegeben, dass eine Design-Schwachstelle im fortwährend immer stärker kritisierten Microsoft Internet Explorer 5.01 bis 6 besteht. Ein Angreifer kann durch einen Fehler des Caches für durch SSL geschützte Seiten sensitive Informationen von diesen auslesen oder die Darstellung derer manipulieren. Ein solches Vorgehen kann mitunter für die zur Zeit stark in Mode gekommenen Phishing-Attacken genutzt werden. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Die Schwachstelle kann mitunter mit dem Microsoft Baseline Security Analyzer (MBSA) verifiziert und halb-automatisch behoben werden. Microsoft hat Patches für die betroffenen Internet Explorer-Versionen herausgegeben, die sich

ebenfalls über das AutoUpdate installieren lassen.

Expertenmeinung:

Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Rund 21 neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.6 Microsoft Internet Explorer 5.01 bis 6 Install Engine Inseng.dll Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 12.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=893>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Microsoft beschreibt im Microsoft Security Bulletin MS04-038 den kumulativen Patch für den hauseigenen Internet Explorer (834707). So wurde im Rahmen des allmonatlichen Patchdays von Microsoft bekannt gegeben, dass eine Pufferüberlauf-Schwachstelle im fortwährend immer stärker kritisierten Microsoft Internet Explorer 5.01 bis 6 besteht. Ein Angreifer kann durch einen Fehler in der Bibliothek Inseng.dll der Install Engine den Browser zum Absturz bringen und gar beliebigen Programmcode ausführen lassen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Die Schwachstelle kann mitunter mit dem Microsoft Baseline Security Analyzer (MBSA) verifiziert und halb-automatisch behoben werden. Microsoft hat Patches für die betroffenen Internet Explorer-Versionen herausgegeben, die sich ebenfalls über das AutoUpdate installieren lassen.

Expertenmeinung:

Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Rund 21 neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so

manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.7 Microsoft Internet Explorer 5.01 bis 6 korruptes Cascading Style Sheet Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 12.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=892>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Microsoft beschreibt im Microsoft Security Bulletin MS04-038 den kumulativen Patch für den hauseigenen Internet Explorer (834707). So wurde im Rahmen des allmonatlichen Patchdays von Microsoft bekannt gegeben, dass eine Pufferüberlauf-Schwachstelle im fortwährend immer stärker kritisierten Microsoft Internet Explorer 5.01 bis 6 besteht. Ein Angreifer kann durch ein korruptes Cascading Style Sheet (CSS) den Browser zum Absturz bringen und gar beliebigen Programmcode ausführen lassen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Die Schwachstelle kann mitunter mit dem Microsoft Baseline Security Analyzer (MSBA) verifiziert und halb-automatisch behoben werden. Der Angriff ist über sämtliche Komponenten möglich, die auf die Internet Explorer-Funktionalität zurückgreifen - So zum Beispiel auch der Mailclient Microsoft Outlook. Microsoft hat Patches für die betroffenen Internet Explorer-Versionen herausgegeben, die sich ebenfalls über das AutoUpdate installieren lassen.

Expertenmeinung:

Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Rund 21 neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.8 Microsoft Windows NetDDE korruptes NetDDE-Paket Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 12.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=891>

Microsoft Windows ist eine sehr beliebte Betriebssystemreihe der redmonder Firma Microsoft. Das grafische Betriebssystem stellt eine Weiterentwicklung des zeilenbasierten MS DOS dar. John Heasman von Next Generation Security Software entdeckte eine Pufferüberlauf-Schwachstelle im NetDDE-Dienst. Wird an diesen ein korruptes NetDDE-Paket geschickt, kann dies zu einer Denial of Service oder gar zum Ausführen beliebigen Programmcodes führen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Von der Schwachstelle betroffen sind Microsoft Windows 95, 98, 98SE, ME, NT 4.0, 2000, XP und Server 2003. Microsoft Windows XP mit installiertem Service Pack 2 ist ebenso gegen diese Schwachstelle gesichert, wie ein Windows-System nach der Installation des innerhalb des Patchdays herausgegebenen Bugfixes.

Expertenmeinung:

Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Rund 21 neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.9 Squid bis 2.5.STABLE7 asn_parse_header() Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 05.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=880>

Squid ist ein open-source Projekt, das einen freien und hochskalierbaren Proxy für Unix-Systeme zur Verfügung stellt. Es werden Protokolle wie HTTP und FTP sowie

Funktionalitäten wie SSL-Unterstützung, Cache-Hierarchien und Zugriffskontrolllisten bereitgestellt. iDEFENSE berichtet in einem scheinbar eingekauften Advisory von einer Denial of Service-Schwachstelle in der Funktion `asn_parse_header()`. Durch ein korruptes SNMP-Paket mit einem negativen Längen-Wert im Header kann der Squid-Server zum Neustart gezwungen werden. Voraussetzung für diese Angreifbarkeit ist das Aktivieren der SNMP-Unterstützung. Mit dem Kommando `"grep snmp_port /usr/local/squid/sbin/squid"` kann verifiziert werden, ob Squid mit der entsprechenden SNMP-Unterstützung kompiliert wurde. Mit der Zeile `"snmp_port 0"` in der Konfigurationsdatei `squid.conf` kann die SNMP-Unterstützung deaktiviert werden. Mit der Zeile `"snmp_incoming_address 127.0.0.1"` in der selbigen lassen sich SNMP-Verbindungen nur auf der loopback-Schnittstelle akzeptieren. Nach den Änderungen ist ein Neustart des Squid-Servers erforderlich. Es wurde zudem ein Patch für Squid-2.5.STABLE6 sowie eine aktualisierte Version Squid-2.5.STABLE7 herausgegeben.

Expertenmeinung:

Diese Schwachstelle ist ärgerlich und gerade aufgrund der hohen Verbreitung von Squid und der Einfachheit der Schwachstelle eben diese als kritisch eingestuft. Aber ebenfalls interessant ist, dass dies einmal mehr eine durch iDEFENSE publizierte Schwachstelle ist, bei der der Finder anonym bleiben möchte. Schon früher habe ich in diesem Zusammenhang den Verdacht geäußert, dass hier ein Mitglied des Squid-Teams nebenbei ein bisschen Geld mit seinem Insider-Wissen verdienen möchte...

3.10 Samba bis 2.2.11 und bis 3.0.5 `unix_clean_name()` erweiterte Schreibrechte

Einstufung: **kritisch**
Remote: Ja
Datum: 30.09.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=858>

Samba ist eine freiverfügbare Applikation für das Freigeben von Ressourcen (Datei- und Druckerfreigabe). iDEFENSE berichtet in ihrem Security Advisory 09.30.04 von einer Schwachstelle in Samba bis 2.2.11 und bis 3.0.5. Die Funktion `unix_clean_name()` ist dafür zuständig, spezielle Zeichenketten bei Dateinamen und Pfadangaben (z.B. `./` und `../`) der Unix-Konvention zu filtern und zu entfernen. Diese Funktion ist in den besagten Versionen nicht korrekt umgesetzt und erlaubt

beispielsweise durch die Angabe `.//////etc` den Lesezugriff auf das Unix-typische Konfigurationsverzeichnis `/etc`. Ein Angreifer kommt so mittels einem Directory Traversal in den Besitz erweiterter Lese- und Schreibrechte. Für die Versionen vor 2.2.12 und vor 3.0.6 wurden Patches herausgegeben. Der Fehler ist in den Versionen 2.2.12 und 3.0.6 behoben worden. Als Workaround wird das Setzen der Funktion `"wide links = no"` empfohlen, die das Ausnutzen der Schwachstelle auf verwundbaren Systemen verhindert.

Expertenmeinung:

Problematisch ist diese Schwachstelle vor allem, weil der Samba-Daemon (`smbd`) meistens mit `root`-Berechtigung ausgeführt wird. Kann ein Angreifer die Schwachstelle ausnutzen, erbt er die Superuser-Privilegien. Grundsätzlich sollten keine Samba-Zugriffe aus unsicheren Netzwerken (z.B. dem Internet) zugelassen werden. Ein Firewall-System sollte die Datei- und Druckerfreigabe lediglich in einem geschützten LAN erlauben. Aber trotzdem gilt es schnellstmöglich auf die aktuellste Samba-Version zu updaten, um mit dieser Sicherheitslücke den Angreifern nicht Tür und Tor zu öffnen.

3.11 Microsoft SQL Server 7.0 bis SP3 Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 30.09.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=857>

Der Microsoft SQL Server ist ein kommerzieller SQL-Server für die Windows-Betriebssysteme. Auf Bugtraq wurde mehr oder weniger kommentarlos ein in C geschriebener Exploit publiziert. Dieser nutzt eine Denial of Service-Schwachstelle im Microsoft SQL Server 7.0 aus. Der Pufferüberlauf, der den `mssqlserver` Dienst zum Stillstand bringt, verhält sich aber laut Kommentar des Exploit-Codes je nach installiertem Service Pack anders. Für den Angriff muss eine korrupte Anfrage mit mehr als 700'000 Bytes verschickt werden. Verwundbar seien aber alle Systeme bis und mit Service Pack 3. Es ist nicht bekannt, ob und inwiefern Microsoft frühzeitig über das Problem informiert wurde. Auf der MSSQL-Seite konnte jedoch heute noch kein Vermerk zur Schwachstelle und den angestrebten Gegenmassnahmen gefunden werden. Es ist damit zu rechnen, dass das Problem mit einem Patch behoben werden wird.

Expertenmeinung:

Remote Denial of Service-Attacken gegen Server sind sehr beliebt - Vor allem, wenn es sich um eine solch populäre Lösung wie der SQL-Server von Microsoft handelt. Der sofort publizierte Exploit wird das seine tun, um dieser Schwachstelle ein nicht zu unterschätzendes Mass an Popularität zu ermöglichen. Exponierte Systeme sollten deshalb umgehend geschützt werden; beispielsweise mittels restriktivem Firewalling auf den betroffenen SQL-Ports.

3.12 Symantec Firewall/VPN 100/200/200R und Gateway Security 320/360/360R SNMP community nicht veränderbar

Einstufung: **kritisch**
Remote: Ja
Datum: 22.09.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=849>

Die Symantec Firewall/VPN-Lösungen gehören zur Kategorie der immer mehr in Mode kommenden Appliance/SOHO-Lösungen. Die Administration der Geräte findet in erster Linie über ein komfortables Webfrontend statt, weshalb derlei Produkte zunehmend auch für Endanwender ohne tiefeschürfende Firewalling- und Netzwerk-Kenntnisse interessant sind. Mike Sues des Rigel Kent Security & Advisory Team entdeckte drei verschiedene Schwachstellen in Symantec Firewall/VPN 100/200/200R und teilweise ebenfalls Gateway Security 320/360/360R

[http://www.rigelksecurity.com/Services/Svcs_sec_advis.html]. Die SMTP community kann nicht geändert oder der SMTP-Dienst deaktiviert werden. Ein Angreifer ist deshalb mitunter auch über das WAN/Internet in der Lage, manipulative Zugriffe auf der Firewall vorzunehmen. Im Zusammenhang mit dem ebenfalls publik gewordenen Fehler des Nicht-Entdeckens von Zugriffen mit Quellport udp/53 ist dies besonders problematisch. Symantec hat mit einer überarbeiteten Firmware für die betroffenen Firewall-Produkte reagiert.

Expertenmeinung:

Die zeitgleich publizierten Schwachstellen für die kleinen Firewall-Produkte von Symantec sind peinlich für das grosse Sicherheitsunternehmen. Die Fehler sind altbekannt und sollten schon frühzeitig bei der Entwicklung entsprechender Lösungen bedacht werden. Die Popularität von Symantec und ihren Lösungen wird dafür sorgen, dass auch in Zukunft die Angriffsformen von Angreifern genutzt werden. Die Anwender betroffener Systeme sind deshalb angehalten,

diese binnen der nächsten Tage auf den aktuellsten Stand zu bringen.

3.13 Symantec Firewall/VPN 100/200/200R und Gateway Security 320/360/360R udp/53 Filter-Regelwerk umgehen

Einstufung: **kritisch**
Remote: Ja
Datum: 22.09.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=848>

Die Symantec Firewall/VPN-Lösungen gehören zur Kategorie der immer mehr in Mode kommenden Appliance/SOHO-Lösungen. Die Administration der Geräte findet in erster Linie über ein komfortables Webfrontend statt, weshalb derlei Produkte zunehmend auch für Endanwender ohne tiefeschürfende Firewalling- und Netzwerk-Kenntnisse interessant sind. Mike Sues des Rigel Kent Security & Advisory Team entdeckte drei verschiedene Schwachstellen in Symantec Firewall/VPN 100/200/200R und teilweise ebenfalls Gateway Security 320/360/360R

[http://www.rigelksecurity.com/Services/Svcs_sec_advis.html]. Bei einer Standard-Installation werden Zugriffe mit udp/53 als Quellport stets akzeptiert und nicht protokolliert. Ein Angreifer kann diesen Umstand nutzen, um unentdeckt Portscans oder Zugriffe auf Dienste umzusetzen. Symantec hat mit einer überarbeiteten Firmware für die betroffenen Firewall-Produkte reagiert.

Expertenmeinung:

Die zeitgleich publizierten Schwachstellen für die kleinen Firewall-Produkte von Symantec sind peinlich für das grosse Sicherheitsunternehmen. Die Fehler sind altbekannt und sollten schon frühzeitig bei der Entwicklung entsprechender Lösungen bedacht werden. Vor allen diese Schwachstelle ist nicht neu, denn so hatte das gleiche Problem vor vielen Jahren auch schon in ZoneLabs ZoneAlarm für Aufsehen gesorgt. Die Popularität von Symantec und ihren Lösungen wird dafür sorgen, dass auch in Zukunft die Angriffsformen von Angreifern genutzt werden. Die Anwender betroffener Systeme sind deshalb angehalten, diese binnen der nächsten Tage auf den aktuellsten Stand zu bringen.

3.14 Symantec Firewall/VPN 100/200/200R UDP-Portscan Denial of Service

Einstufung: **kritisch**
Remote: Ja

Datum: 22.09.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=847>

Die Symantec Firewall/VPN-Lösungen gehören zur Kategorie der immer mehr in Mode kommenden Appliance/SOHO-Lösungen. Die Administration der Geräte findet in erster Linie über ein komfortables Webfrontend statt, weshalb derlei Produkte zunehmend auch für Endanwender ohne tiefeschürfende Firewalling- und Netzwerk-Kenntnisse interessant sind. Mike Sues des Rigel Kent Security & Advisory Team entdeckte drei verschiedene Schwachstellen in Symantec Firewall/VPN 100/200/200R und teilweise ebenfalls Gateway Security 320/360/360R

[http://www.rigelksecurity.com/Services/Svcs_sec_advis.html]. Ein Angreifer kann über einen externen UDP-Portscan auf sämtliche UDP-Ports des WAN-Interfaces das Ziel zum Abstürzen bringen. Aus den Meldungen geht nicht hervor, ob dazu ein normaler UDP-Portscan ausreicht oder ob bestimmte Bedingungen gegeben sein müssen. Symantec hat mit einer überarbeiteten Firmware für die betroffenen Firewall-Produkte reagiert.

Expertenmeinung:

Die zeitgleich publizierten Schwachstellen für die kleinen Firewall-Produkte von Symantec sind peinlich für das grosse Sicherheitsunternehmen. Die Fehler sind altbekannt und sollten schon frühzeitig bei der Entwicklung entsprechender Lösungen bedacht werden. Vor allem die Popularität von Symantec und ihren Lösungen wird dafür sorgen, dass auch in Zukunft die Angriffsformen von Angreifern genutzt werden. Die Anwender betroffener Systeme sind deshalb angehalten, diese binnen der nächsten Tage auf den aktuellsten Stand zu bringen.

4. Hintergrundbericht

4.1 Das Risiko Trusted Computing für die deutsche Versicherungswirtschaft

Von Dr. Philipp Kramer/Marko Rogge

Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V.

Das Positionspapier des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. fasst prägnant und dennoch umfassend zusammen, welche wirtschaftlichen und weiteren Interessen bei der Einführung von Trusted Computing auf dem Spiel stehen und zu berücksichtigen sind.

Trusted Computing (auch Trustworthy Computing), initiiert von wichtigen Hard- und Softwareherstellern (Promoter sind AMD, Hewlett-Packard, IBM, Intel Corporation, Microsoft, Sony Corporation, Sun Microsystems), bedeutet Absicherung von Hardware und der auf ihr gespeicherten Daten mittels Hardwarechip. Dieser Chip ist einer fest eingebauten Smartcard vergleichbar. Zum Trusted Computing gehören auch softwarebasierte Datensicherheitsmaßnahmen. Es geht um das Ziel, sicherzustellen, ob die Trägerplattform, das Betriebssystem und die ablaufenden Anwendungen trusted (vertrauenswürdig) sind. Damit sollen die Ziele der Datensicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Prüfbarkeit, umgesetzt werden.



Zugleich handelt es sich damit um eine Technik, die verhindert, dass User die laufenden Anwendungen manipulieren können, die wiederum abgesichert mit dem Softwarehersteller und untereinander kommunizieren können. Dahinter steckt ursprünglich in erster Linie Digital Right Management.

Die Beurteilung des Positionspapiers fällt sehr kritisch aus. Zunächst ist schon die Datenschutzkonformität dieser Technik zweifelhaft. Die Einführung von Trusted Computing öffnet den Herstellern unter

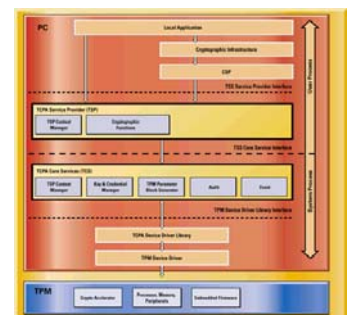
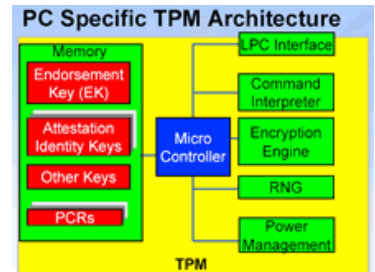
Umständen Zugriff auf die Daten des Unternehmens. Handelt es sich um personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes, hängt die Übermittlung an den Dritten, den betreffenden Hard- und Softwarehersteller, nur noch davon ab, ob dieser bestimmte Daten

tatsächlich abruft. Denn ein Übermitteln liegt bereits vor, wenn ein Dritter zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft (§ 3 Absatz 4 Nr. 3 Buchstabe b BDSG). Für diese Übermittlung liegt jedoch kein rechtfertigender Tatbestand vor. Schon für das betroffene Unternehmen ist überhaupt nicht transparent, ob ein solcher Abruf erfolgt. Das gilt erst recht für den betroffenen Dateninhaber. Ein Rechtfertigungsgrund im Sinne der allgemeinen Rechtfertigungsnorm des § 28 BDSG ist nicht ohne weiteres ersichtlich.

Erfolgt tatsächlich ein Abruf von personenbezogenen Daten durch den betreffenden Hard- und Softwarehersteller, bedeutet dieser Abruf im Zweifel daher eine unrechtmäßige Datenübermittlung durch das Unternehmen, welches die personenbezogenen Daten sonst rechtmäßig verwaltet. Die auf den ersten Blick der Datensicherheit des Unternehmens dienende Technik des Trusted Computing kann sich also bei genauerer Betrachtung schnell als eine mit einem Bussgeld von EUR 250.000 bewehrte Datenübermittlung darstellen.

Das Positionspapier zeigt sehr deutlich und übersichtlich die Einstiegsgeschichte in die Thematik des Trusted Computing. Die technischen Beschreibungen helfen dem Leser, schnell die

Bedeutungen von Worten wie Palladium (Microsofts Standard für die Software-Implementation), NGSCB (Microsofts neuer Standard) und Safer Computing und LaGrande (Intel) zu verstehen, so sie sie noch nicht kennen. Die Autoren haben mit viel Mühe Details recherchiert, die aufzeigen, wie gering der Sicherheitsgewinn und wie hoch die Sicherheitsrisiken und der Kontrollverlust für die



Versicherungswirtschaft sind. Die technische Umstellung bei Hard- und Software setzen nach Ansicht der Autoren ein hohes Maß an Vertrauen gegenüber den Initiatoren voraus.

In den einzelnen Abschnitten dieses Papiers wird die Gefahr von Abhängigkeiten gegenüber den Produkten und der Verantwortung der Initiatoren aufgezeigt. Im einzelnen werden neue Plattformen geschaffen, die Trusted Computing unterstützen und fördern. Hierdurch werden Versicherungsunternehmen zu neuen Investitionen gezwungen. Auch ein Zugewinn an Sicherheit, der an sich mittels Trusted Computing erreicht werden soll, wird aufgezeigt. Jedoch ist derzeit eine effektive Steigerung der Sicherheit nicht erkennbar, so die Autoren. Durch Ausweitung unterschiedlicher Technologien aus dem Bereich Trusted Computing ist es kaum noch möglich, eine effiziente Kontrolle über eigene Systeme zu erhalten.

Die Autoren kommen zu dem Schluss, dass eine Umsetzung von Trusted Computing in der aktuellen Form aus Datenschutz- und Datensicherheitsaspekten nicht zu rechtfertigen ist. Es besteht die begründete Gefahr, dass Trusted Computing dazu führt, dass die Kontrolle über einen Rechner von seinem Inhaber auf denjenigen übergeht, dessen System und/oder Software der User verwendet. Zudem droht die Verletzung von Datenschutzvorschriften verletzt.

Die Broschüre, auch für anderen Unternehmen hilfreich, ist unentgeltlich erhältlich beim Gesamtverband der Deutschen Versicherungswirtschaft e.V. in Berlin (per E-Mail h.borchardt@gdv.org, per Fax 030-2020-6628 oder - vom GDV angekündigt - per Download unter www.gdv-online.de). Weitere Informationen der Trusted Computing Kampagne finden sich unter „www.trus-tedcomputinggroup.org“.

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 Rued

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