

Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Statistiken Verletzbarkeiten
5. Labs
6. Bilderrätsel
7. Impressum

1. Editorial

Cyberwar aus Nordkorea: Artikel richtig lesen

Journalismus und die damit in einen Rechtsstaat verflochtene Transparenz erachtete ich stets als unumstößliche Grundlage eines solchen. Der Umkehrschluss sieht vor, dass in einem Staat, in dem die Journalisten bedrängt werden, nicht frei sein kann. Leider hat die Qualität moderner Medienschaffender spürbar abgenommen. Dies wird mir besonders dann deutlich, wenn ich einmal mehr einen Artikel zum Thema Computersicherheit lese.

Nachfolgend möchte ich den Artikel Hacker attackieren amerikanische und südkoreanische Web-Seiten von Spiegel Online, wie er am 08. Juli 2009 erschienen ist, auseinandernehmen und die Unwahrheiten, Abweichungen und Fehlschlüsse aufzeigen.

"Das Weiße Haus, das Pentagon, die Heimatschutzbehörde: Seit Tagen versuchen Hacker, die Internet-Seiten von US-Behörden durch einen Dauerbeschuss mit Anfragen zu überlasten und lahmzulegen. Auch Server in Südkorea ächzen. Geheimdienste vermuten, dass Nordkorea hinter den Angriffen steckt.

(...)

Einem Bericht des US-Senders Fox News zufolge steckt hinter den massiven Attacken Nordkorea. Der Sender beruft sich auf einen Beamten des US-Verteidigungsministeriums."

Die Schlussfolgerung, dass vermutet wird, dass Nordkorea dahintersteckt, ist (voraussichtlich) unbegründet. Die Systeme, welche für eine Distributed Denial of Service-Attacke (DDoS) eingesetzt werden und den Direktkontakt mit den Zielsystemen herstellen, werden Zombie-Systeme genannt. Hierbei handelt es sich um mit einer Hintertür kompromittierte Rechner, die damit für die Attacken zweckentfremdet wird.

Es ist zwar anzunehmen, dass in Ländern wie Nordkorea eine verhältnismässig hohe Anzahl an schlecht gewarteten und deshalb kompromittierten Systemen vorhanden ist. Aber nur weil diese für einen Angriff missbraucht werden, heisst es nicht, dass das entsprechende Land dahintersteckt. (Gleiches gilt auch für China und Russland.)

Nordkorea wäre sehr unklug, würden sie ein Botnetz im eigenen Land für eine unwichtige DDoS-Attacke hergeben. Ihre Möglichkeiten und die technische Umsetzung wäre unmittelbar preisgegeben. Der Populismus mit einem der momentanen "Lieblingsfeinde der USA" passt jedoch jedoch unbestritten zu Fox News. Tage später nach dem Bekanntwerden der Attacken wurde dann auch darüber berichtet, dass die Täterschaft wohl in Grossbritannien beheimatet ist.

"In den USA seien unter anderem das Weiße Haus, das Pentagon, das Außenministerium und die New Yorker Börse betroffen gewesen. Jedoch seien die Attacken weitgehend wirkungslos geblieben, hieß es. Den Hackern sei es nicht gelungen, die Sicherheitsvorkehrungen der Seiten zu überwinden."

Es ist fragwürdig, ob man im Zusammenhang mit einer DDoS die Phrase "überwinden von Sicherheitsvorkehrungen" nutzen kann, um die fehlende Wirksamkeit der Attacken hervorzuheben. Abgesehen von lückenlosem Whitelisting mittels ACLs auf einer frühzeitigen Ebene gibt es keinen wirksamen Schutz gegen Überlastungsangriffe wie eine DDoS. Zudem widerspricht sich der Artikel hier, da im ersten Absatz die Rede davon ist, dass "[es den Hackern teilweise gelingt], die Seiten vorübergehend lahmzulegen." Dies ist das Ziel der DDoS und damit die Wirksamkeit

(vorübergehend) gewährleistet.

"Im Mai hatten südkoreanische Medien unter Berufung auf Geheimdienstkreise berichtet, das Militär in Nordkorea beschäftige etwa hundert Hacker, die es besonders auf die Computernetze der Streitkräfte Südkoreas und der USA abgesehen hätten."

Es gibt nichts Auffälligeres weder eine Denial of Service-Attacke. Diese mit mehreren Quellsystemen als DDoS, über einen längeren Zeitraum von mehreren Tagen und auf hochgradig exponierte Ziele wie Regierungsseiten umzusetzen erhöht die Auffälligkeit des Angriffs nur noch mehr. Ein solches Vorgehen verfolgt in der Regel kurzfristige Ziele, die jeweiligen Systeme durch die eingeschränkten Zugriffsmöglichkeiten zu schädigen. Einen direkten produktiven Nutzen haben DoS-Attacken in den meisten Fällen nicht (sie werden nur selten als Überdeckungsangriffe im Rahmen konstruktiver Attacken eingesetzt). Es bleibt äusserst zweifelhaft, ob "staatliche Hacker" ihre Ressourcen in derartig plumper und infantiler Weise verschwenden würden.

"Nach Angaben des US-Heimatschutzministeriums drangen Hacker im vergangenen Jahr rund 5500-mal in Regierungscomputer ein, im Jahr davor wurden nur knapp 4000 solcher Zwischenfälle gezählt."

Wir sagen unseren Kunden immer, dass eine Kompromittierung stets eine zuviel ist. Wird sie nämlich geschickt umgesetzt (und weitere Attacken unter Ausnutzung von Vertrauensbeziehungen automatisiert), kann innerhalb weniger Sekunden ein Maximum an Schaden entstehen. Entweder muss man aufgrund der Aussage des Department of Homeland Security unmittelbar das Vertrauen in die Informationssicherheit amerikanischer Behörden verlieren, oder man will mit dieser vermeintlichen Zunahme von Einbrüchen die Verhandlungen für die kommende Budgetrunde einleiten.

"Aus Ermittlerkreisen verlautete jetzt, die Tatsache, dass die Internet-Seiten nach dem aktuellen Angriff noch nach drei Tagen betroffen seien, deute auf eine ungewöhnlich raffinierte Attacke."

Diese Aussage kann ich technisch nicht nachvollziehen. Eine DDoS ist plump und direkt, wodurch sie alles andere als raffiniert ist. Hierzu eingesetzt wurde Mydoom, ein altbekannter Schädling, der erstmals 26. Januar 2004 (vor fast sechs Jahren!) gesichtet wurde. Die scheinbar

lange Zeitdauer des Angriffs ist wohl auf zwei Gründe zurückzuführen: Einerseits wird eine sehr breite Basis an Zombies eingesetzt, andererseits sind die jeweiligen Provider/Administratoren nicht in der Lage, zeitnah auf die unliebsamen Anfragen zu reagieren (z.B. mit ACL/Firewalling). Wie an verschiedenen Stellen zu lesen ist, verhalten sich die Zombies zudem nicht besonders geschickt ("Auffällig sei, dass die DDoS-Angriffe keine Programme benutzen, die eine Entdeckung durch Sicherheitsprogramme erschweren.").

Ich gehe sehr stark davon aus, dass hier eine Einzelperson oder eine kleine Gruppe ein eigens zusammengetragenes, gemietetes oder partiell übernommenes Botnet für ihre politischen Aktivitäten nutzen. Selbstverständlich wird auch Nordkorea begriffen haben, dass im Informationszeitalter grundlegende Prozesse für einen Cyberkrieg eingeleitet werden müssen. Diesen aber auf einer solch plumpen Ebene zelebrieren zu wollen, das traue ich weder Kim Jong-Il noch Muammar al-Gaddafi zu.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 23. November 2009

2. scip AG Informationen

2.1 Frohe Festtage



Die scip AG wünscht an dieser Stelle allen Lesern und Leserinnen des scip monthly Security Summary erholsame Festtage und einen guten Rutsch in eine neues, erfolgreiches und gesundes Jahr 2010.

2.2 OSVDB linkt auf scip VulDB

Die [OSVDB](#) (The Open Source Vulnerability Database) gilt mittlerweile mit über 60'000 Einträgen als grösste öffentliche Verwundbarkeitsdatenbank.



Die jeweiligen Einträge verlinken nun seit dem 14. Dezember 2009 [offiziell](#) auf unsere [scip VulDB](#), die als grösste deutschsprachige Datenbank gilt. Dadurch werden Recherchen nun noch einfacher.

Wir bedanken uns beim OSVDB Team für die angenehme Zusammenarbeit und das hervorragende Projekt.

2.3 Process Review

Prozesse bilden die Grundlage einer sicheren Lösung, wodurch dank einem durchdachten Konzept der Grundstein für den Erfolg einer erfolgreichen Betriebbarkeit gelegt werden kann.

Das Ziel des Prozess Reviews ist die Identifikation von Unschönheiten und Designschwachstellen in bestehenden Prozessen.

Der Kunde stellt uns das bestehende Prozesskonzept sowie alle damit in Verbindung stehenden Dokumente (z.B. Handbücher, Sitzungsprotokolle, etc.) zur Verfügung. Ausserdem werden Mitarbeiter der scip AG die zu prüfenden Prozesse im Betrieb des Kunden mitmachen und somit direkt erleben.

- Vorbereitung: Definition der Ziele sowie Zusammentragen und Diskutieren des bestehenden Konzepts.
- Analyse: Vorort erleben und effektives durchspielen der zu prüfenden Prozesses beim Kunden.
- Review: Durchsicht und Analyse zur Ermittlung von Unschönheiten und Fehlern.
- Diskussion: Dokumentation und Diskussion der identifizierten Fehler sowie der vorgeschlagenen Massnahmen.

Der Kunde erhält ein Dokument, welches die ungeschönen oder falschen Punkte des bestehen der involvierten Prozesse diskutiert. Diese werden analysiert, auf ihre Risiken hingewiesen und weitere Massnahmen zur Reduktion dieser festgehalten. Die so gefunden Punkte werden in gemeinsamen Workshops erläutert und den zuständigen Stellen innerhalb des Kunden nähergebracht.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen haben wir als scip AG bereits eine Vielzahl von Source Code Analysen Projekte durchgeführt.

Zählen auch Sie auf uns!

<http://www.scip.ch/?firma.referenzenalle>

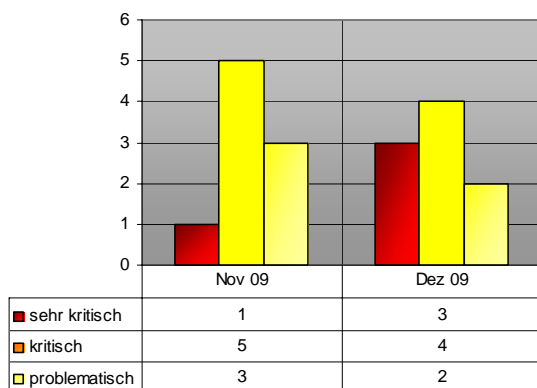
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/?vuldb> einsehbar.



Die Dienstleistungspakete scip(pallas liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.



Contents:

- 4060 Microsoft Windows Win32k Kernel-Mode Driver mehrere Schwachstellen
- 4059 Apple Mac OS X mehrere Schwachstellen
- 4058 Microsoft Windows Active Directory Denial of Service
- 4057 Microsoft Excel verschiedene Schwachstellen
- 4056 Microsoft Office Word File Information Block Parsing Pufferüberlauf
- 4054 Wireshark verschiedene Denial of Service Schwachstellen
- 4053 VMware verschiedene Produkte Host Privilege Escalation
- 4052 Mozilla Firefox mehrere Schwachstellen

3.1 Mozilla Firefox verschiedene Schwachstellen

Risiko: **kritisch**
 Remote: Ja
 Datum: 16.12.2009
 scip DB: <http://www.scip.ch/?vuldb.4073>

Mozilla Firefox (amerikanisch-englische Aussprache) ist ein freier Webbrowser des Mozilla-Projekts. Der seit Mitte 2002 entwickelte Open-Source-Webbrowser bietet die Möglichkeit, eine breite Palette an Erweiterungen zu implementieren. Firefox ist nach dem Internet Explorer der am zweithäufigsten genutzte

Webbrowser. Mozilla adressiert mit einem Update auf Version 3.5.6 eine Vielzahl von Schwachstellen, deren Ausnutzung Denial of Service und/oder Code Executions zur Folge haben.

Expertenmeinung:

Während diesen Monat Browserschwachstellen relativ rar gesäht waren, adressiert Mozilla mit dem neusten Update einige längst fällige Punkte. Ein zeitnahes Update sei Anwendern wie Administratoren empfohlen.

3.2 Adobe Reader/Acrobat "Doc.media.newPlayer()" Memory Corruption

Risiko: **sehr kritisch**
 Remote: Ja
 Datum: 15.12.2009
 scip DB: <http://www.scip.ch/?vuldb.4072>

Adobe Reader (früher Acrobat Reader) ist ein Computerprogramm der Firma Adobe zum Anzeigen von PDF-Dokumenten, also ein Dateibetrachter. Es ist Teil der Adobe Acrobat-Produktfamilie. Eine (weitere) kritische Schwachstelle in Adobe Reader wird derzeit aktiv ausgenutzt, bei der durch die Funktion Doc.media.newPlayer() bereits freigegebener Speicher erneut aufgerufen wird. Dadurch kann beliebiger Code zur Ausführung gebracht werden.

Expertenmeinung:

Es wird langsam zur Gewohnheit, dass Adobes PDF Betrachter regelmässig zur Angriffsplattform #1 wird, weil erneut eine kritische Schwachstelle über die Scripting Funktionalität einen Pufferüberlauf oder ähnliches zu provozieren vermag. Auch diese Schwachstelle wirft die selben Fragen auf, wie die vorangehenden. Zum Beispiel: Was läuft falsch in Adobes Secure Development Lifecycle? Oder: Warum ist Scripting standardmässig aktiviert? Während die Antworten auf diese Fragen für den Moment offen bleiben müssen, so ist im Hinblick auf die vorliegende Schwachstelle eines klar: Ein Patch ist nach Aussagen Adobes nicht vor Anfang/Mitte Januar zu erwarten. Bis dahin sei es Anwendern wie Administratoren empfohlen, dafür zu sorgen dass Scripting nicht aktiviert ist. Alternativ bietet sich der Wechsel auf eine der zahlreichen Alternativen an.

3.3 Adobe Flash Player verschiedene Schwachstellen

Risiko: **sehr kritisch**
 Remote: Ja



Datum: 09.12.2009
scip DB: <http://www.scip.ch/?vuldb.4071>

Adobe Flash (kurz Flash, ehemals Macromedia Flash) ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte, der Flash-Filme. Die resultierenden Dateien liegen im SWF-Format vor, einem auf Vektorgrafiken (u.a.) basierenden Grafik- und Animationsformat. Das Kürzel SWF steht dabei für Shockwave Flash (nicht für „small web format“, wie mitunter fälschlich angenommen). In einem Advisory beschreibt Adobe verschiedene kritische Schwachstellen im Adobe Flash Player, durch die mittels eines entsprechend manipulierten Flash Files beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:

Adobe schickt sich an gegen Jahresende seine Vorherrschaft in Sachen Schwachstellen für dieses Jahr weiter auszubauen. Mehr als ein halbes Dutzend Schwachstellen adressiert der kumulative Patch, der verschiedene kritische Schwachstellen zu schliessen verspricht. Betroffene Clientsysteme sollten aufgrund der hohen Verbreitung und der öffentlich verfügbaren Exploits zeitnah gepatcht werden.

3.4 Microsoft Windows Indeo Codec verschiedene Schwachstellen

Risiko: **sehr kritisch**
Remote: Ja
Datum: 08.12.2009
scip DB: <http://www.scip.ch/?vuldb.4070>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Verschiedene Researcher berichteten unlängst von Schwachstellen im vorinstallierten Indeo Video Plugin, über die sich beliebiger Code zur Ausführung bringen lässt.

Expertenmeinung:

Die vorliegende Lücke ist daher als sehr kritisch zu werten, weil sie zum jetzigen Zeitpunkt nicht vollständig mitigiert werden kann. Microsoft stellt mit dem vorliegenden Patch zwar sicher, dass Indeo nicht als Codec innerhalb der Internetzone genutzt werden kann. Drittapplikationen verwenden das Plugin jedoch nach wie vor

unverändert, was entsprechende Angriffsvektoren bietet. Das Einspielen des Patches sollte erste Priorität erhalten, dennoch sollte aber das verbleibende Restrisiko weiter beobachtet werden.

3.5 Microsoft Windows MS-CHAP Authentication Umgehungsangriff

Risiko: **problematisch**
Remote: Ja
Datum: 08.12.2009
scip DB: <http://www.scip.ch/?vuldb.4068>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Durch einen Fehler in der Verarbeitung von MS-CHAPv2 Authentisierungsanfragen können Angreifer durch eine speziell bearbeitete Anfrage auf Netzwerkressourcen zugreifen, ohne über entsprechende Authentisierungsmerkmale zu verfügen.

Expertenmeinung:

Die vorliegende Schwachstelle ist vor allem für grosse, interne Netzwerke von Relevanz, die sensitive Daten enthalten. Hier sollte zeitnah mit dem Einspielen entsprechender Patches reagiert werden.

3.6 Windows Active Directory Federation Services verschiedene Schwachstellen

Risiko: **kritisch**
Remote: Ja
Datum: 08.12.2009
scip DB: <http://www.scip.ch/?vuldb.4067>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Microsoft beschreibt in einem Technet Eintrag Schwachstellen in verschiedenen Windows Serverversionen, bei denen Authentication Tokens ausgelesen und beliebiger Code zur Ausführung gebracht werden kann. Dies kann

eine Kompromittierung des Systems zur Folge haben.

Expertenmeinung:

Auch hier sollte für Serveradministratoren eine schnelle Reaktion des Credo sein. Sofern möglich sollte, aufgrund der Gefahr einer Kompromittierung durch Code Execution, eine zeitnahe Installation der entsprechenden Patches erfolgen.

3.7 Microsoft Windows Local Security Authority Subsystem Denial of Service

Risiko: **kritisch**

Remote: Ja

Datum: 08.12.2009

scip DB: <http://www.scip.ch/?vuldb.4066>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Microsoft beschreibt in einem Technet Eintrag eine Schwachstelle in verschiedenen Windowsversionen, bei der durch eine Denial of Service Schwachstelle beim Handling von ISAKMP Nachrichten durch LSASS ein System zu Absturz gebracht werden kann.

Expertenmeinung:

Auch hier handelt es sich wiederum "nur" um eine Denial of Service Attacke. Dennoch: Da auch Serverversionen betroffen sind, sollten vor allem diese zeitnah gepatcht werden, um negative Implikationen zu vermeiden.

3.8 SumatraPDF Shading Pattern Processing Pufferüberlauf

Risiko: **kritisch**

Remote: Ja

Datum: 30.11.2009

scip DB: <http://www.scip.ch/?vuldb.4065>

SumatraPDF ist ein populärer PDF Viewer, der oft als schlanke Alternative zu Adobe Reader betrachtet wird. Christophe Devine identifiziert eine Schwachstelle in der, SumatraPDF zugrunde liegenden, MuPDF Library. Diese enthält eine Pufferüberlauf Schwachstelle, mit der ein Angreifer beliebigen Code zur Ausführung bringen kann.

Expertenmeinung:

Gerade im Moment, wo Adobe Reader unter heftigem Beschuss steht, haben Alternativprodukte Hochkonjunktur. Auch deshalb sollte darauf geachtet werden, dass auch Alternativen nicht vor Schwachstellen gefreit sind und daher stets auf dem neusten Stand gehalten werden sollten.

3.9 Cisco VPN Client "cvpnd" Service Local Denial of Service

Risiko: **problematisch**

Remote: Ja

Datum: 20.11.2009

scip DB: <http://www.scip.ch/?vuldb.4064>

Cisco Systems, Inc. ist ein US-amerikanisches Unternehmen aus der Telekommunikationsbranche. Bekannt ist es vor allem für seine Router und Switches, die einen großen Teil des Internet-Backbones versorgen. Alex Hernandez berichtet in einem Advisory von einer Schwachstelle in Ciscos hauseigenem VPN Client, bei dem innerhalb der Datei cvpnd.exe durch unsauberer Error Handling alle momentanen VPN Sessions terminiert werden können.

Expertenmeinung:

Auch wenn es sich bei der vorliegenden Schwachstelle lediglich um eine relativ unkritische Denial of Service Lücke handelt, sollten betroffene Administratoren, gerade in sensiblen Bereichen, um ein rasches Einspielen des verfügbaren Updates bemüht sein.

3.10 ManageEngine Password Manager Pro searchtext Script Injection

Risiko: **kritisch**

Remote: Ja

Datum: 15.12.2009

scip DB: <http://www.scip.ch/?vuldb.4063>

PasswordManager Pro ist eine Software zur Verwaltung von Passwörtern innerhalb eines Unternehmens. Passwörter können zentral gespeichert und durch authentifizierte Benutzer bei Bedarf abgerufen werden. Stefan Friedli der scip AG identifizierte eine Schwachstelle in aktuellen Versionen (bis Build 6104) der Applikation, bei der durch die fehlende Validierung des GET Parameters "searchtext" beliebiger Scriptcode im Kontext der Applikation zur Ausführung gebracht werden kann. Angreifer können auf diesem Wege in den Besitz sensibler Daten, inklusive Passwörter, gelangen.

Expertenmeinung:

Die vorliegende Lücke ist aufgrund der Kritikalität der zugrundeliegenden Daten als kritisch zu betrachten. Angreifer können durch eine erfolgreiche Attacke in den Besitz sensibler Passwortdaten kommen. Ebenso lässt sich die Lücke problemlos auch für unauthentierte Benutzer im Rahmen einer Phishing Attacke ausnutzen - der Schadcode wird in diesem Fall zwischengespeichert und nach dem erfolgreichen Login zur Ausführung gebracht. Betroffene Benutzer sollten zeitnah um das Einspielen eines entsprechenden Patches bemüht sein.

3.11 Internet Explorer Layout Handling Memory Corruption

Risiko: **kritisch**

Remote: Ja

Datum: 23.11.2009

scip DB: <http://www.scip.ch/?vuldb.4061>

Der Internet Explorer (offiziell Windows Internet Explorer; früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser vom Softwarehersteller Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. securitylab.ir berichtet über eine Schwachstelle, bei der durch das fehlerhafte Parsing von Layouts eine Memory Corruption entsteht. Dies kann über eine dediziert vorbereitete Webseite ausgelöst werden.

Expertenmeinung:

Die vorliegende Schwachstelle ist derzeit ungepatcht, was Benutzer mit IE6/7 grundsätzlich verwundbar macht. ActiveScripting sollte bis zur Verfügbarkeit eines Patches restriktiv gehandhabt werden. Sofern möglich, ist auch der Einsatz von IE8 nach aktuellem Ermessen als Gegenmassnahme in Betracht zu ziehen.

4. Statistiken Verletzbarkeiten

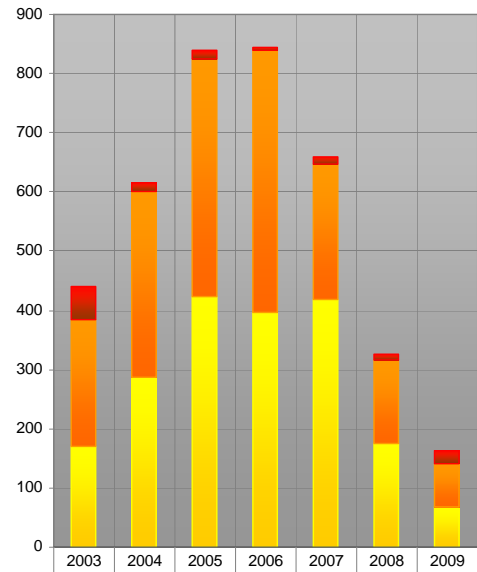
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



<http://www.scip.ch/?vuldb>

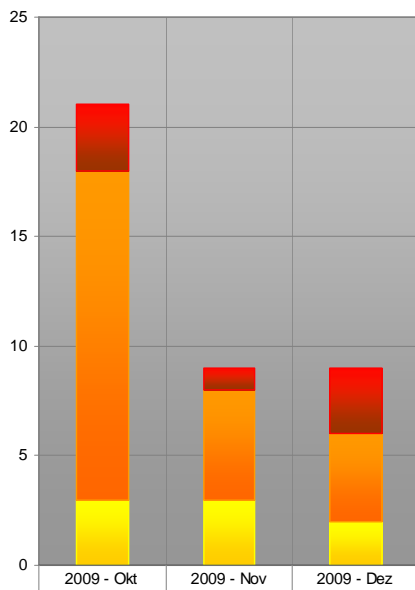
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum: 17. Dezember 2009



| | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 |
|---------------|------|------|------|------|------|------|------|
| sehr kritisch | 56 | 15 | 15 | 6 | 11 | 11 | 21 |
| kritisch | 214 | 314 | 402 | 442 | 229 | 140 | 72 |
| problematisch | 170 | 287 | 423 | 396 | 419 | 176 | 69 |

Verlauf der Anzahl Schwachstellen pro Jahr



| | 2009 - Okt | 2009 - Nov | 2009 - Dez |
|---------------|------------|------------|------------|
| sehr kritisch | 3 | 1 | 3 |
| kritisch | 15 | 5 | 4 |
| problematisch | 3 | 3 | 2 |

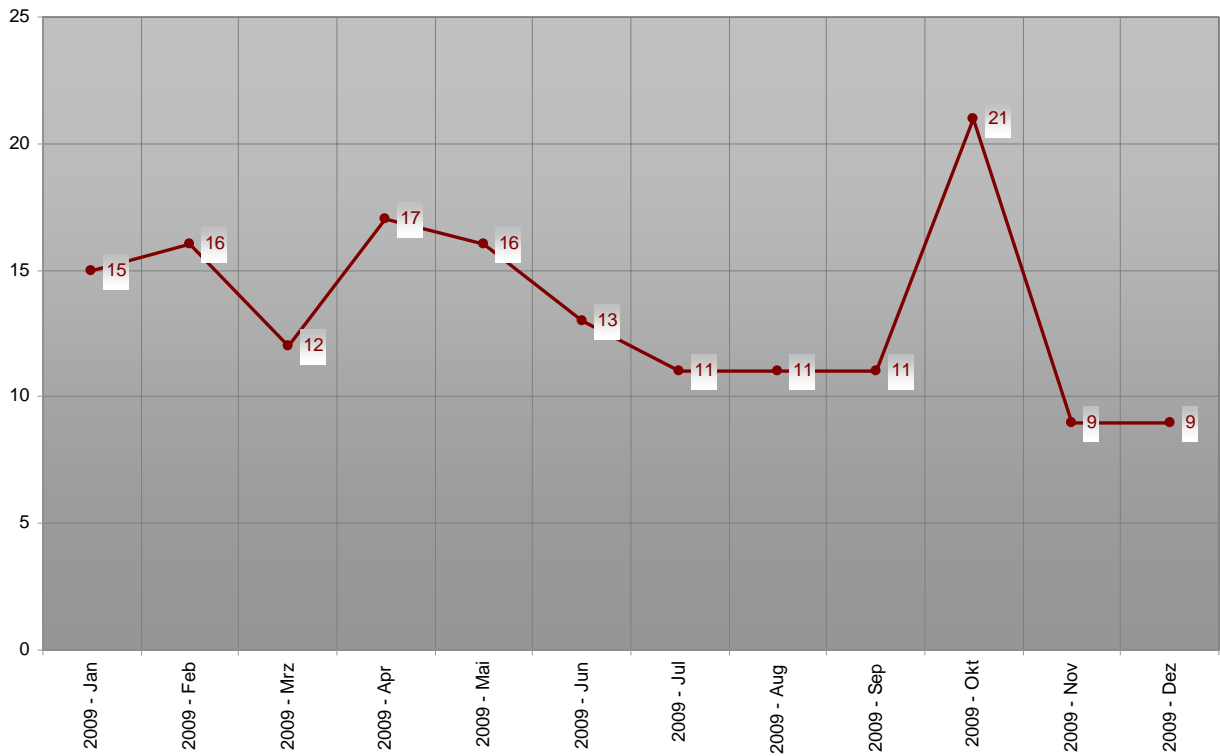
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



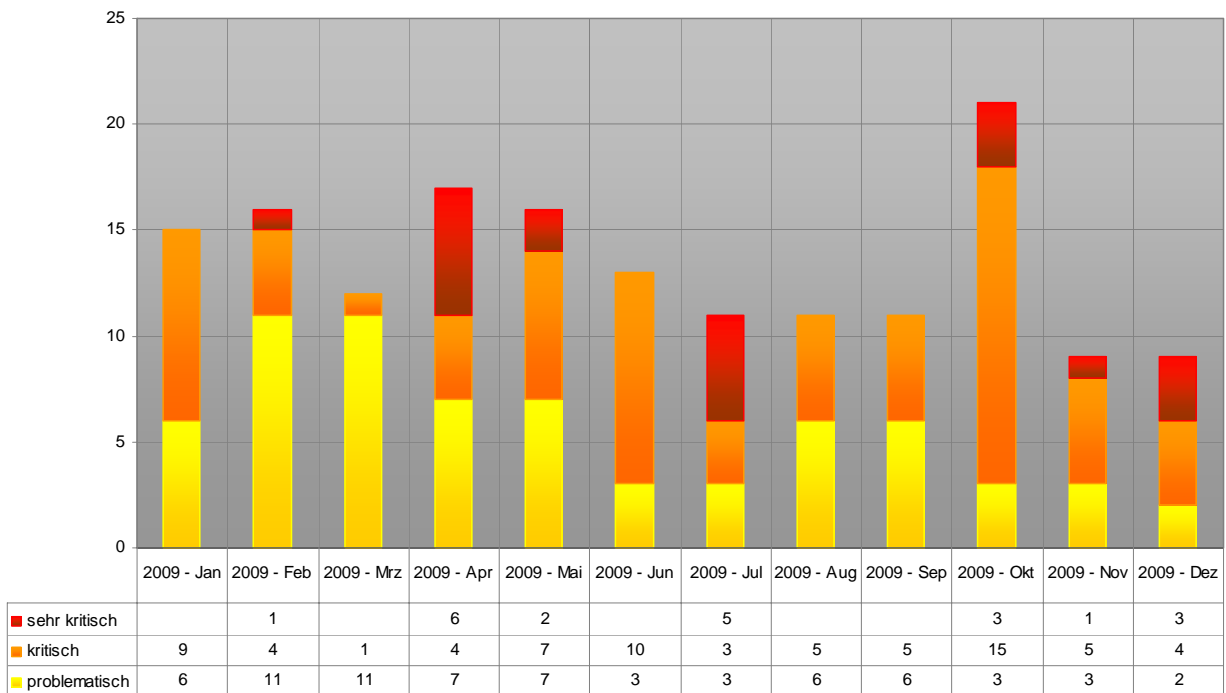
| | 2009 - Okt | 2009 - Nov | 2009 - Dez |
|----------------------------|------------|------------|------------|
| Cross Site Scripting (XSS) | | | 1 |
| Denial of Service (DoS) | 1 | 2 | 1 |
| Designfehler | 2 | | |
| Directory Traversal | | | |
| Eingabeungültigkeit | | | |
| Fehlende Authentifizierung | | | |
| Fehlende Verschlüsselung | | | |
| Fehlerhafte Leserechte | | | |
| Fehlerhafte Schreibrechte | | | |
| Format String | | | |
| Konfigurationsfehler | | | |
| Pufferüberlauf | 18 | 6 | 6 |
| Race-Condition | | 1 | |
| Schwache Authentifizierung | | | |
| Schwache | | | |

Verlauf der letzten drei Monate Schwachstelle/Kategorie

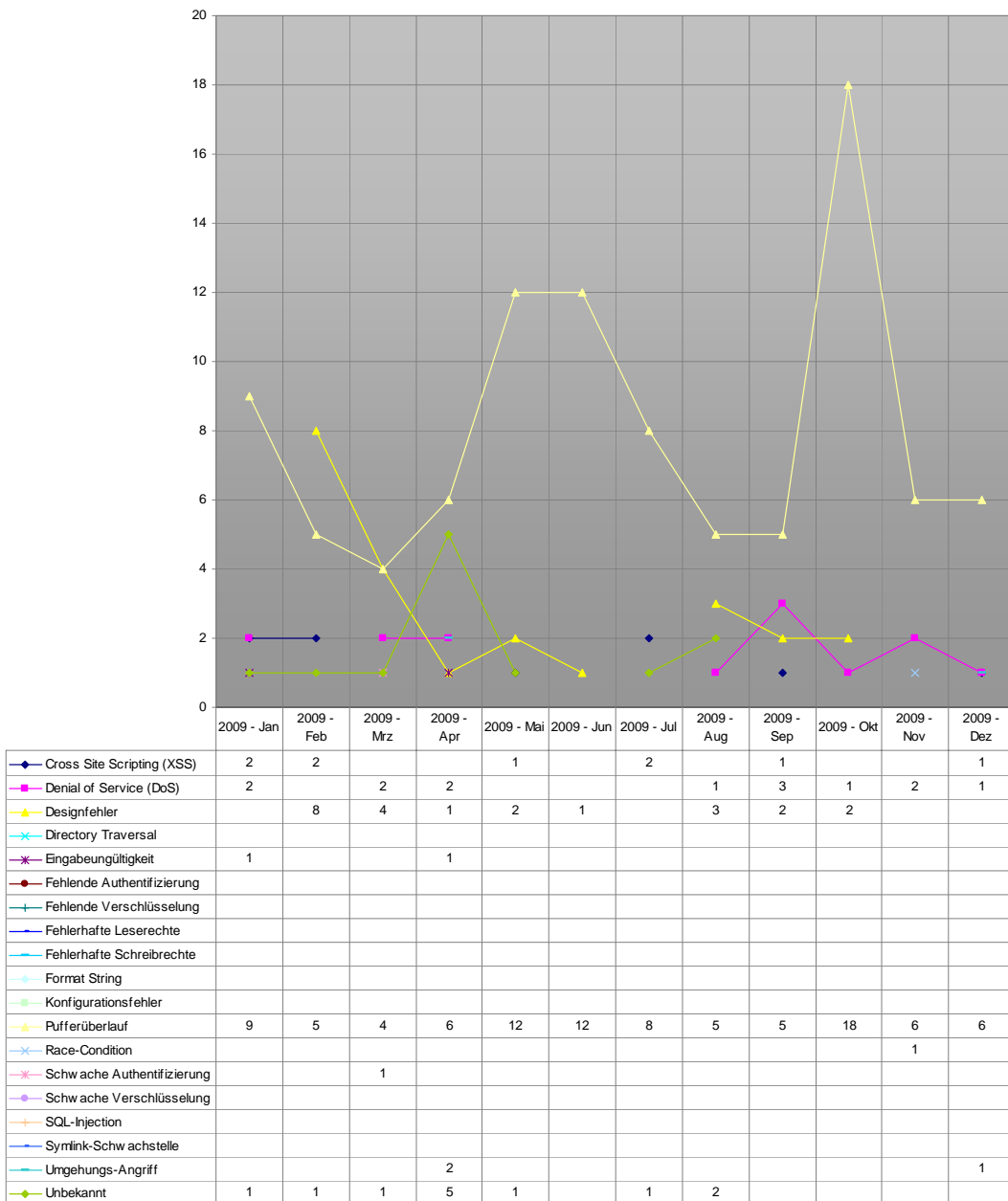
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2009

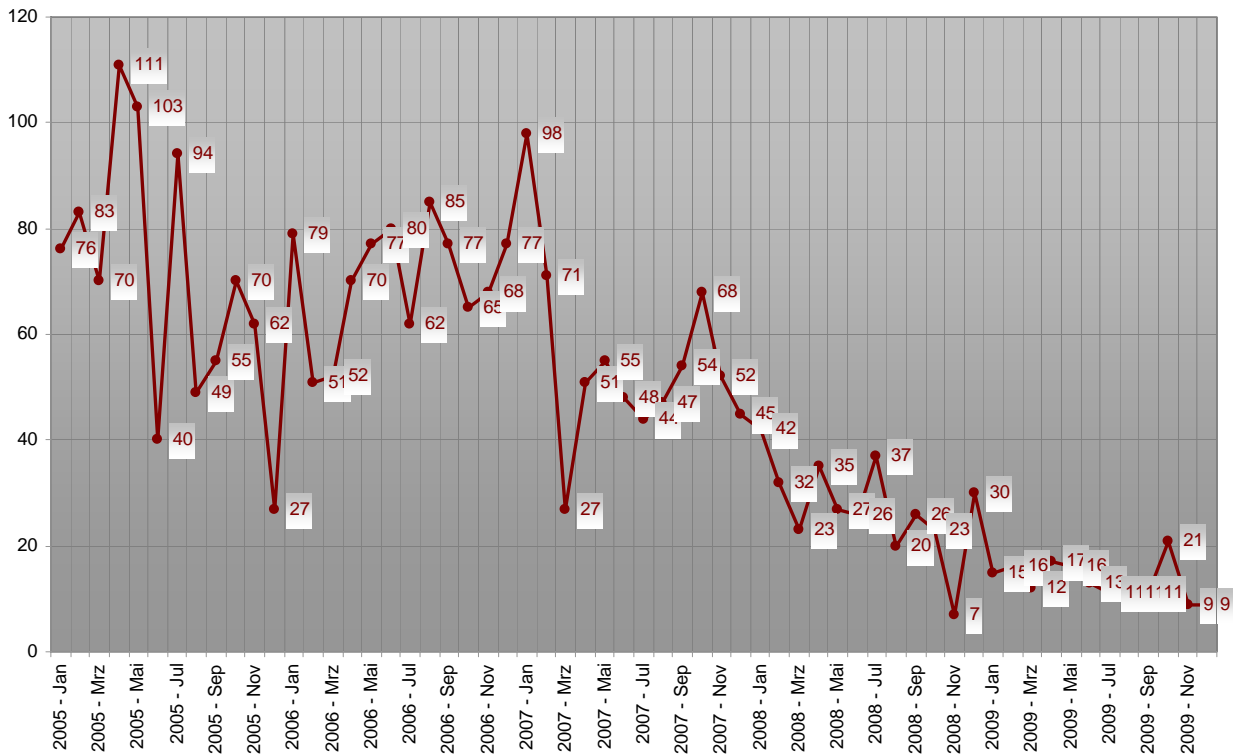


Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2009

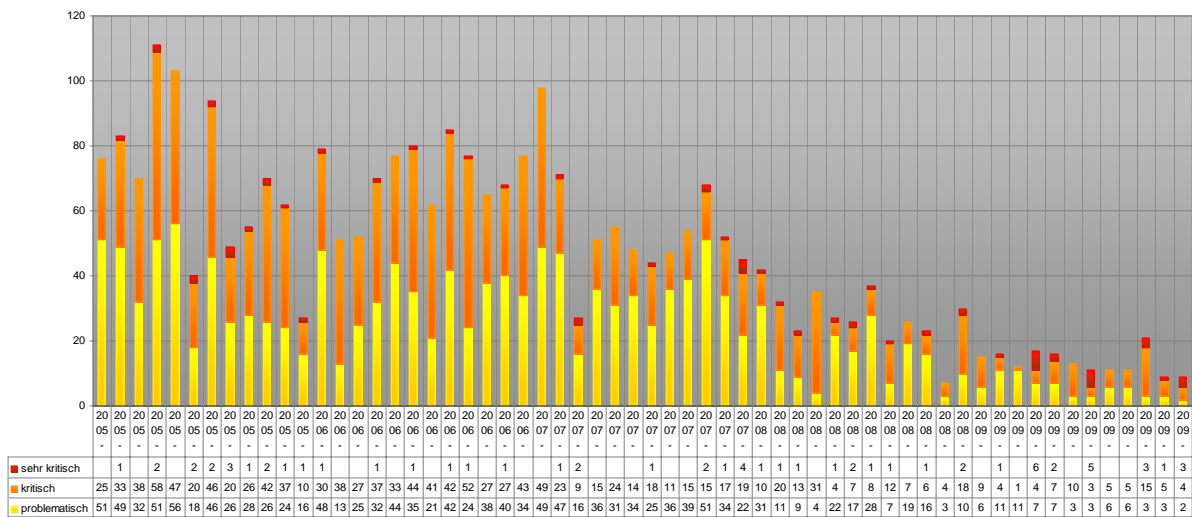


Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2009

Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005

5. Labs

Auf der scip Labs Webseite (<http://www.scip.ch/?labs.archiv>) werden regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

5.1 10 sicherheitsrelevante Gründe gegen Cloud Computing

27.11.2009, Marc Ruef, maru@scip.ch



Im Zuge der anhaltenden Virtualisierung der letzten 10 Jahre bekam ein artverwandtes – aber nicht zwingend neues – Thema immer mehr Aufmerksamkeit: Cloud Computing. Forrester Research fasst das Prinzip dieses Konzepts (es handelt sich nicht um eine Software oder ein Produkt als solches) wie folgt zusammen (Inquiry Spotlight: Cloud Computing, Q2 2009)

Cloud Computing steht für einen Pool aus abstrahierter, hochskalierbarer und verwalteter IT-Infrastruktur, die Kundenanwendungen vorhält und falls erforderlich nach Gebrauch abgerechnet werden kann.

Modularität ist ein wichtiger Aspekt von Cloud Computing. Denn nur dadurch kann die transparente Abstrahierung und dynamische Skalierbarkeit – die mittlerweile auch von Botnet-Betreibern und Crackern entdeckt wurde – erlangt werden. Im Rahmen von Cloud Computing werden jedoch grundlegende Risiken aufgetan, die im Zuge wirtschaftlicher Aspekte gerne abgewiegt oder gänzlich ignoriert werden:

1. Fehlende Transparenz: Durch die Abstrahierung wird es für einen Kunden nicht mehr möglich zu erkennen, wo sich seine Daten genau befinden und wie mit diesen umgegangen wird. Branchenspezifische Anforderungen an Sicherheitsüberprüfungen werden nur sehr schwer umsetzbar. Damit wird die Grundlage für alle weiter genannten Probleme geschaffen. Dieser Aspekt wird massgeblich dem bis dato umfangreichsten Kreditkartenrückruf angelastet.
2. Vermengung von Kunden/Diensten/Daten: Durch das Teilen von Ressourcen findet eine Vermengung von Kunden, Diensten und Daten statt, wodurch ungleich klassifizierte Assets in gleicher Weise behandelt werden. Verliert ein Asset seine Integrität, kann sich dies unmittelbar auf die anderen Assets auswirken. Beteuerungen eines Anbieters, einen

sicheren und geschützten Umgang der Daten durchzusetzen, können oftmals auf Grund der fehlenden Transparenz nicht verifiziert werden.

3. Verlust der Kontrolle über Daten/Prozesse: Die fehlende Transparenz und das Teilen der Ressourcen führen dazu, dass ein Verlust über die Nutzdaten und Aktivitäten stattfindet. Ein Anbieter könnte diese unerlaubt selbst weiterverwenden oder an einen Mitbewerber oder eine Behörde weiterreichen. Dies ist das zentrale Argument, welches Whitfield Diffie in einem Interview mit Technology Review anführt.
4. Abhängigkeit vom Anbieter: Man ist in direkter Weise vom Angebot und der Qualität des Dienstleisters abhängig. Ausfälle des Dienstes können sich als sofortige Einbusse der Produktivität auswirken (siehe den Datenverlust des Sidekick-Dienstes im Oktober 2009; heise online, fefe).
5. Schwierigkeit von Backups: Das Erstellen von Backups könnte massgeblich erschwert sein. Nur mit erheblichem Aufwand lassen sich diese selbstständig umsetzen. Will man diesen nicht in Kauf nehmen, ist man bezüglich derer erneut vom Anbieter abhängig. Die kompetente Umsetzung dieses Prozesses sowie unter Einhaltung branchen-/unternehmensspezifischer Vorhaben lässt sich oftmals nur schwer durchsetzen.
6. Schwierigkeit bei Migration: Durch komplexe Abhängigkeiten und Inkompatibilitäten kann ein Wechsel zu einem anderen Anbieter nur mit sehr viel Aufwand möglich sein. Die Abhängigkeit zum Partner führt eine ständige Trägheit mit sich. Bei Differenzen in der Zusammenarbeit ist man lange Zeit der Willkür des Partners unterworfen.
7. Juristische Konflikte bezüglich Datenschutz: Es ist denkbar, dass sich eine Cloud über verschiedene Länder erstreckt. Diese können ihrerseits unterschiedliche Rechtsgrundlagen aufweisen. Durch ein dynamisches Verteilen eines Dienstes ins Ausland können juristische Probleme auftreten (z.B. bei Exportverbot oder bezüglich Datenschutz). Amazon versucht diesem Problem auf technischer Ebene mit den Availability Zones und Finjan mit Vital Cloud Herr zu werden.
8. Juristische Eigenverantwortung: Ein Unternehmen kann sich durch das Auslagern von Daten und Prozessen nicht gänzlich von der Eigenverantwortung lossprechen. Selbst eine strukturierte Evaluation und Prüfung des Partners sowie eine solide vertragliche Vereinbarung lassen ein derartiges Abtreten von

Verantwortung nicht zu.

9. Einbusse bei Knowhow: Das Auslagern von Prozessen und Technologien wird meist umgesetzt, um bezüglich internen Ressourcen eine Kostenersparnis zu erreichen. Der Abbau von ausgebildetem Personal hat längerfristig die Einbusse von Knowhow und Kompetenzen zur Folge. Im schlimmsten Fall ist bei Verhandlungen und Problemen nicht einmal mehr jemand intern anwesend, der dem Sachverhalt ansatzweise ein Verständnis entgegenbringen kann. Ein etwaiges In-sourcing gestaltet sich dann als Neuaufbau einer gesamten Abteilung (inkl. Personal, Prozesse, Strukturen).
10. Zentraler Angriffspunkt: Obschon Cloud Computing als Distributed Computing verstanden wird, wird damit ein zentraler Angriffspunkt geschaffen. Je mehr Mechanismen in eine spezifische Cloud ausgelagert werden, desto fokussierter kann sich ein Angreifer eben diesem Konstrukt annehmen. Eine Kompromittierung der Cloud hat theoretisch die Kompromittierung sämtlicher ausgelagerter Mechanismen zur Folge.

Cloud Computing kombiniert die unliebsamen Risiken von Virtualisierung und Outsourcing. Von der pauschalen Nutzung von Cloud Computing ist deshalb in Umgebungen mit hohen Ansprüchen an die Sicherheit abzusehen. Zu gross sind die Risiken, die sich bisweilen nur sehr schwer ausmachen und eliminieren lassen. Hilfestellung bei einer entsprechenden Risikokalkulation gewährt die umfangreiche aber auch nicht unumstrittene ENISA-Studie. Und mögliche Ansätze für ein sicheres Cloud Computing werden von RSA zusammengefasst.

6. Bilderrätsel



| GESUCHTE BEGRIFFE | | |
|-------------------|-------------|-------------|
| 6 (english) | 4 (english) | 7 (english) |

LÖSUNGSWORT

scip monthly Security Summary 19.12.2009

Wettbewerb

Mailen Sie uns das erarbeitete Lösungswort 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 **15.01.2010**. 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 des Bilderrätsel finden Sie jeweils online auf <http://www.scip.ch>.

Gewinnen Sie einen Monat des [Securitytracker](#) Dienstes)pallas{.

SECURITYTRACKER



7. Impressum

Herausgeber:



scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:



Marc Ruff
Security Consultant
T +41 44 404 13 13
<mailto:maru@scip.ch>

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich Information Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, Trend-Micro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)