

Contents

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

1. Editorial

Elektronische Einbruchserkennung - Ein missverstandenes Werkzeug

Der erste in erster Linie kommerziell ausgeschlachtete Trend der noch jungen IT Security Branche war das Firewalling. Im Corporate-Bereich wurden Firewall-Systeme gekauft und installiert, wie wenn es kein Morgen gäbe. Jede Firma, die etwas auf sich hielt, musste seinen Internet-Zugang mit einem Paketfilter schützen.

Die Industrie hatte Blut geleckert und versuchte unmittelbar nach dem Erreichen des umsatzstarken Zenits einen neuen Trend zu etablieren. Einen Schritt weiter als die damals als passiv verstandenen Firewalls sollten die Intrusion Detection-Systeme (IDS) gehen. Neben Antivirus und Kryptografie hat sich damit ein weiteres Missverständnis im Bereich der "alltäglichen" Computersicherheit etabliert.

Dies beginnt damit, was ein IDS überhaupt macht. Grundsätzlich kann zwischen Angriffserkennung und Einbruchserkennung unterschieden werden. Zwei strategisch gänzlich unterschiedliche Prozesse, die ebenso unterschiedlich konzipiert werden müssen. Je nachdem wird ein IDS nämlich an exponierter Stelle positioniert, eventuell gar als Teil eines Honeypots/Honeynets betrieben. Oder es wird an zentrale und umfassend geschützte Objekte,

wie zum Beispiel eine interne Kundendatenbank, gebunden. Neben der netzwerktechnischen Positionierung sind ebenfalls die Konfiguration und der Betrieb von diesen Überlegungen abhängig.

Doch was den Untergang der IDS-Lösungen herbeigeführt hat, bevor diese überhaupt das Erbe der Firewall-Kultur antreten konnten, waren die weiterführenden Überlegungen abseits des Produkts ansich. In fast keinem Bereich sollte der Ausspruch "Sicherheit ist kein Produkt, sondern eine Lösung" seine volle Tragweite entfalten. Zur Evaluation, dem Kauf, der Konzeption, Installation und Konfiguration kommen weitere Aspekte, die ein IDS überhaupt nützlich werden lassen.

Intrusion Detection-Systeme sind schlussendlich Software-Lösungen, die durch mehr oder weniger komplexe Verfahren verdächtige/unerwünschte Aktivitäten erkennen und melden sollen. Doch wo werden diese Alerts gemeldet und wer nimmt sich diesen an? Wie im Bereich des Vulnerability Scannings trumpfen die jeweiligen Lösungen nicht gerade mit einer perfekten Zuverlässigkeit auf. False-Positives und False-Negatives sind an der Tagesordnung und so muss ein Spezialist die jeweiligen Resultate analysieren, prüfen und gegebenenfalls erweitern.

In Bezug auf eine IDS-Lösung bedeutet dies, dass Spezialisten als Teil des Monitoring-Teams die jeweiligen Alerts sichten müssen. Doch damit nicht genug. Denn was passiert, wenn ein effektiver Alert ausgelöst wurde? Zum Beispiel ein erfolgreicher Einbruch auf einem betriebskritischen Server? Die Incident Response (IR) regelt als Prozess, wie in einem solchen Fall verfahren werden soll. Die Definition dieser Abläufe ist nicht einfach, sollen sie denn nicht willkürlich oder fahrlässig die Produktivität eines Unternehmens untergraben. Massnahmen müssen klug gewählt und noch kluger angewendet werden.

Da viele Kunden das grundlegende Prinzip von Produkten wie Intrusion Detection-Systemen nicht verstanden haben oder die damit eingeführten Mechanismen mittragen wollten, war das Konzept in einem breitflächig

kommerziellen Sinn zum Scheitern verurteilt. Die meisten Käufer haben ihre teuren Installationen nach nur wenigen Jahren wieder abgebaut. Und auch heute noch finden sich in den wenigsten Unternehmen IDS-Lösungen, die für den Kunden zufriedenstellend, umfassend und flächendeckend eingesetzt werden.

Der Aufwand und die Kosten werden vorgängig falsch kalkuliert und sind im Betrieb einfach zu hoch, wodurch das Risiko eines Blindflugs bei einem drohenden Incident wohl oder übel in Kauf genommen wird.

Marc Rued <maru-at-scip.ch>
Security Consultant
Zürich, 22. Februar 2010

2. scip AG Informationen

2.1 Security Coaching

Das Ziel des Security Coaching ist die direkte Beratung und das unmittelbare Coaching des Kunden in den Bereichen der Information Security zur Sicherstellung nachhaltiger und sicherer Prozesse, Architektur- und Technologieentscheidungen.

Der Kunde bespricht mit uns seine Ziele und Vorgaben. Anhand dessen unterstützen wir den Kunden mit unserer fachmännischen Expertise und langjährigen Erfahrung im Security Bereich. Bei Sitzungen mit Partnern stellen wir das entsprechende Know-How zur Formulierung wichtiger Nachfragen zur Verfügung.

- Vorbereitung: Zusammentragen aller vorhandenen Informationen zur anstehenden Aufgabe.
- Research: Einholen von weiteren Informationen (z.B. Erfahrungen von anderen Kunden).
- Diskussion: Besprechung der Aufgabe und der daraus resultierenden Möglichkeiten.
- Empfehlung: Aussprechen und Dokumentieren eines vertretbaren Lösungswegs.

In erster Linie soll in beratender Weise eine direkte Hilfestellung mit konkreten Empfehlungen und Lösungen bereitgestellt werden. Eine Dokumentation (Protokolle, Kommunikationsmatrizen, Statements etc.) erfolgt auf Wunsch des Kunden.

Durch die direkte Beteiligung an einem Projekt kann unmittelbar Einfluss ausgeübt, damit die Etablierung schwerwiegender Fehler verhindert und ein Höchstmass an Sicherheit erreicht werden. Da Sicherheit von Beginn an zur Diskussion steht, lassen sich Schwachstellen von vornherein vermeiden. Aufwendigen Tests und nachträgliche Anpassungen können so vorgebeugt werden.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen konnten wir als scip AG bereits eine grosse Anzahl an Kunden beraten und begleiten.

Zählen auch Sie auf uns!

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

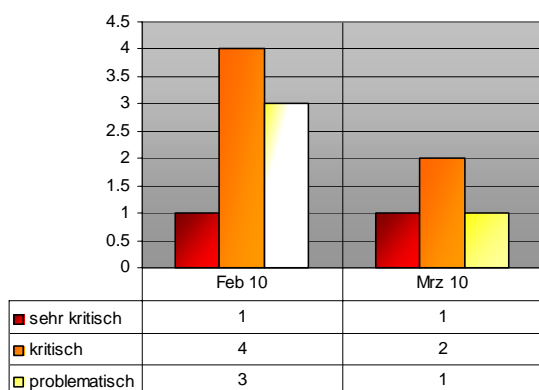
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch.

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:

- 4091 Internet Explorer unspezifizierte Code Execution Schwachstellen
- 4090 Microsoft Office Excel verschiedene Schwachstellen
- 4089 Microsoft Windows Movie Maker Pufferüberlauf
- 4088 Microsoft Windows "MsgBox()" HLP Dateiausführung

3.1 Internet Explorer unspezifizierte Code Execution Schwachstellen

Risiko: **sehr kritisch**

Remote: Ja

Datum: 09.03.2010

scip DB: <http://www.scip.ch/?vuldb.4091>

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. Der integrierte Browser, Internet Explorer, gehört bis heute zu den verbreitetsten Webbrowsern auf dem Markt. Microsoft berichtet in einem Advisory von einer kritischen, jedoch un spezifizierten Schwachstelle, bei der durch eine manipulierte Webseite mittels einer Use-After-Free

Verwundbarkeit beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:

Uns liegen Meldungen vor, dass die vorliegende Schwachstelle derzeit aktiv ausgenutzt wird. Da bislang kein Patch verfügbar ist, sollten betroffene Umgebungen prüfen, ob ein Upgrade auf Internet Explorer 8, der nach aktuellem Ermessen nicht von der Schwachstelle betroffen ist, eventuell machbar und sinnvoll wäre. Das Microsoft Advisory enthält desweiteren einige Hinweise auf mögliche Workarounds, falls dieser Schritt nicht realisierbar ist.

3.2 Microsoft Office Excel verschiedene Schwachstellen

Risiko: **kritisch**

Remote: Ja

Datum: 09.03.2010

scip DB: <http://www.scip.ch/?vuldb.4090>

Microsoft Excel ist das am weitesten verbreitete Tabellenkalkulationsprogramm. Excel gehört zur Microsoft-Office-Suite und ist sowohl für Microsoft Windows als auch für Mac OS verfügbar. Excel entstand als Nachfolger von Microsoft Multiplan. Die aktuelle Version ist für Windows Microsoft Excel 2007 und für Mac OS Microsoft Excel 2008. Microsoft bespricht in einem Advisory verschiedene Schwachstellen in diesen aktuellen Versionen, die es dem Angreifer ermöglichen, beliebigen Code im Kontext der Applikation zur Ausführung zu bringen, was zu einer Kompromittierung führen kann.

Expertenmeinung:

Die vorliegenden Schwachstellen sind grundsätzlich als kritisch zu betrachten und sollten durch das Einspielen des entsprechenden Patches zeitnah geschlossen werden.

3.3 Microsoft Windows Movie Maker Pufferüberlauf

Risiko: **problematisch**

Remote: Ja

Datum: 09.03.2010

scip DB: <http://www.scip.ch/?vuldb.4089>

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.

Damian Frizza identifizierte eine Schwachstelle im integrierten Windows Movies Maker, bei dem durch die Funktion IsValidWMToolsStream() ein Pufferüberlauf provoziert werden kann, der die Ausführung beliebigen Codes erlaubt.

Expertenmeinung:

Die vorliegende Schwachstelle ist grundsätzlich als kritisch zu betrachten, da sie die meisten Standardinstallation der letzten Clientversionen von Windows betrifft. Der freigegebene Patch sollte daher zeitnah installiert werden, um eine Kompromittierung zu vermeiden.

3.4 Microsoft Windows "MsgBox()" HLP Dateiausführung

Risiko: **kritisch**

Remote: Ja

Datum: 01.03.2010

scip DB: <http://www.scip.ch/?vuldb.4088>

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. Maurycy Prodeus identifizierte eine Schwachstelle in verschiedenen Windows Versionen, bei der durch die Nutzung der internen Hilfefunktion, normalerweise aufgerufen via F1, die Ausführung beliebiger Kommandos ermöglicht wird. Ein Angreifer könnte dadurch, z.B. über eine manipulierte Webseite beliebigen Code auf dem Zielsystem zur Ausführung bringen.

Expertenmeinung:

Die vorliegende Schwachstelle ist grundsätzlich als kritisch zu betrachten, zumal sie - den nötigen Erfindergeist vorausgesetzt - die Ausführung beliebigen Codes auf dem Zielsystem erlaubt. Microsoft rät zur Mitigation zur Deaktivierung von ActiveScripting oder dem Verzicht auf die Benutzung der Hilfefunktion. Beide Lösungen sind daher eher als unadäquat zu betrachten - es ist daher zu hoffen, dass Microsoft zeitnah mit einem Patch reagieren wird.

4. Statistiken Verletzbarkeiten

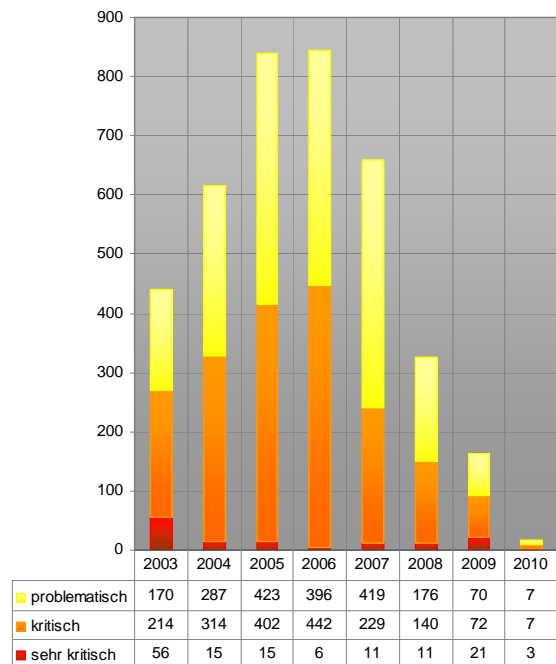
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



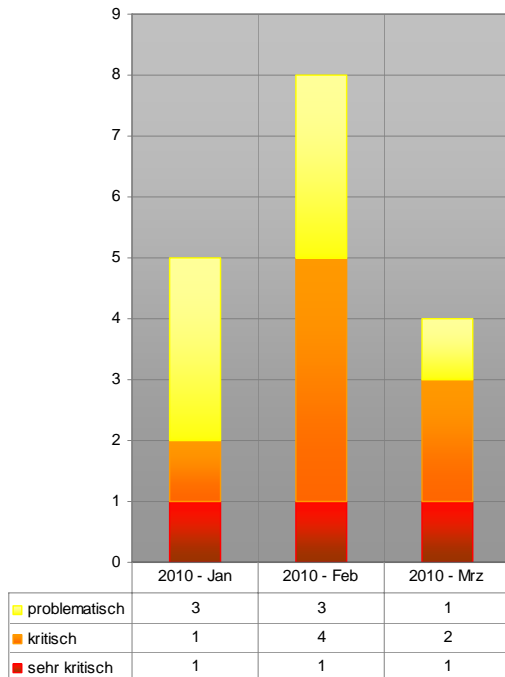
<http://www.scip.ch/?vuldb>

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.

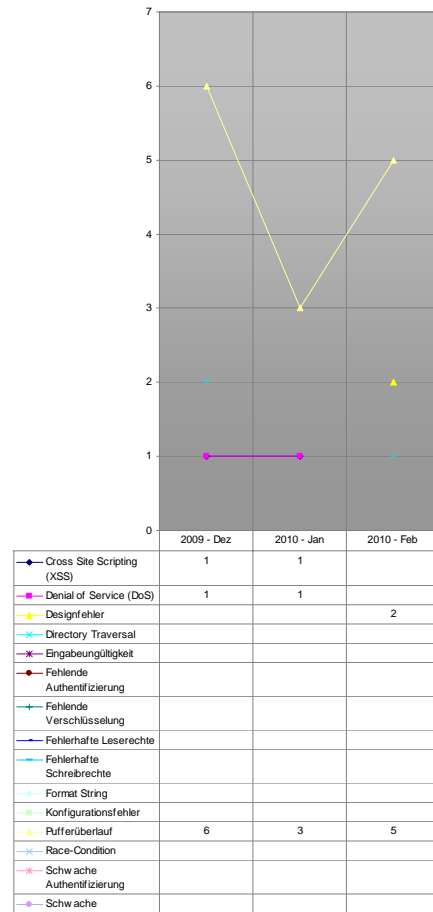
Auswertungsdatum: 19. März 2010



Verlauf der Anzahl Schwachstellen pro Jahr

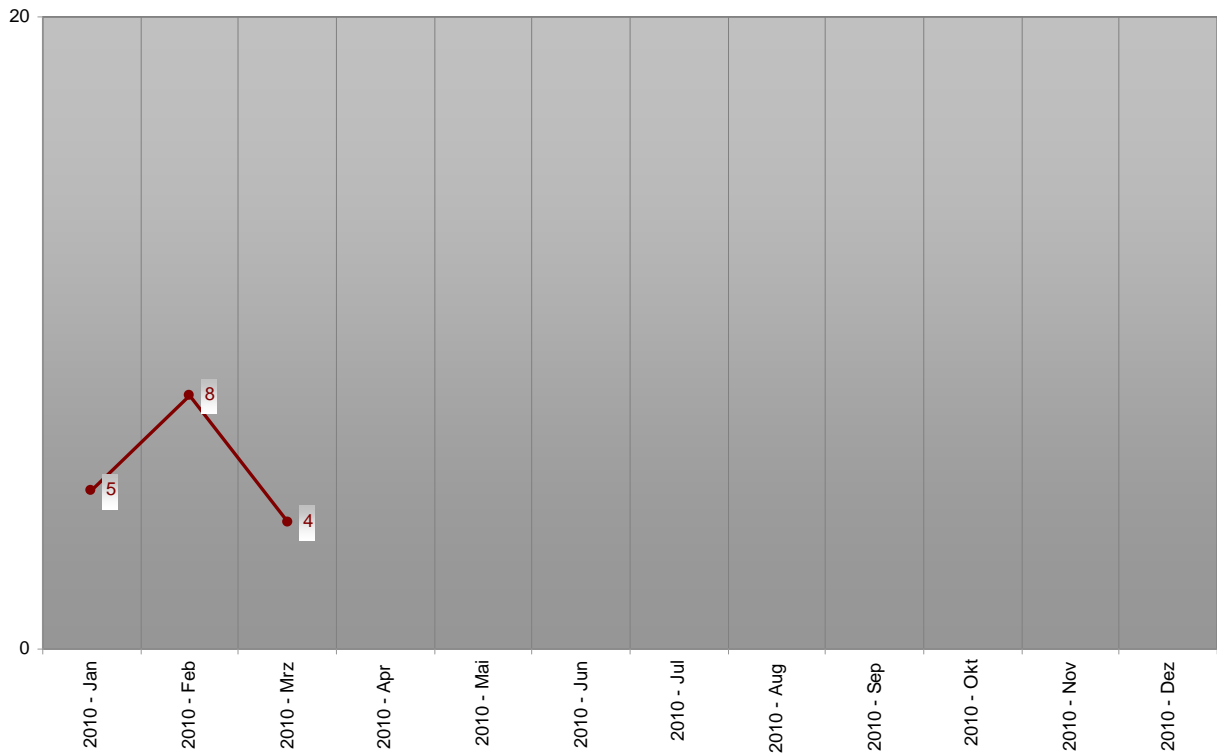


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

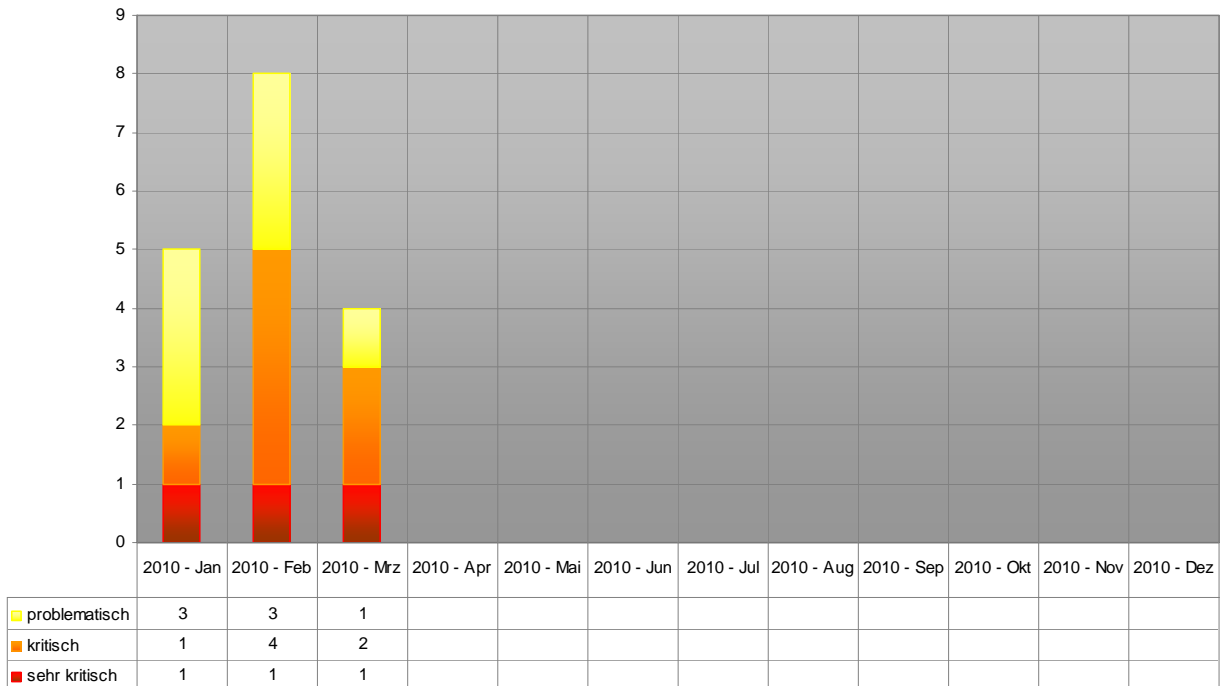


Verlauf der letzten drei Monate Schwachstelle/Kategorie

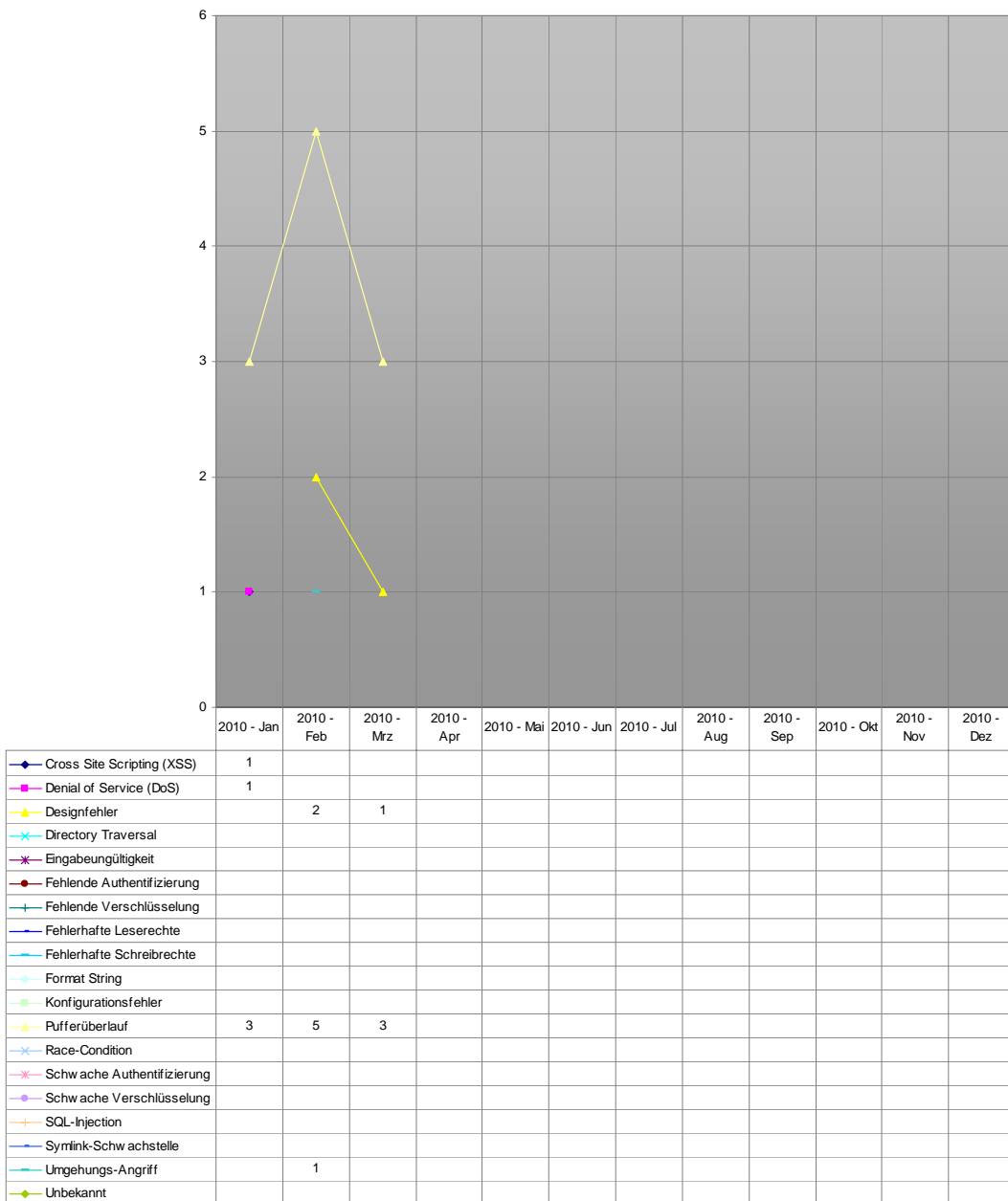
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2010

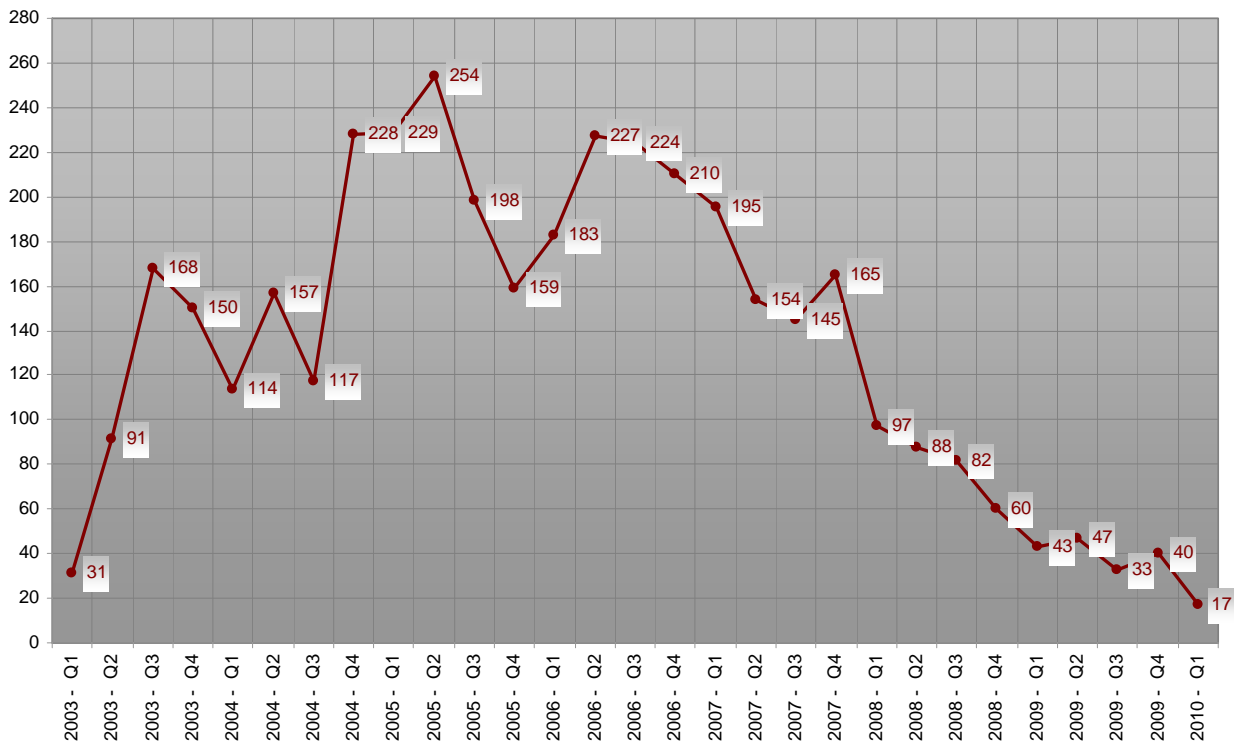


Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2010



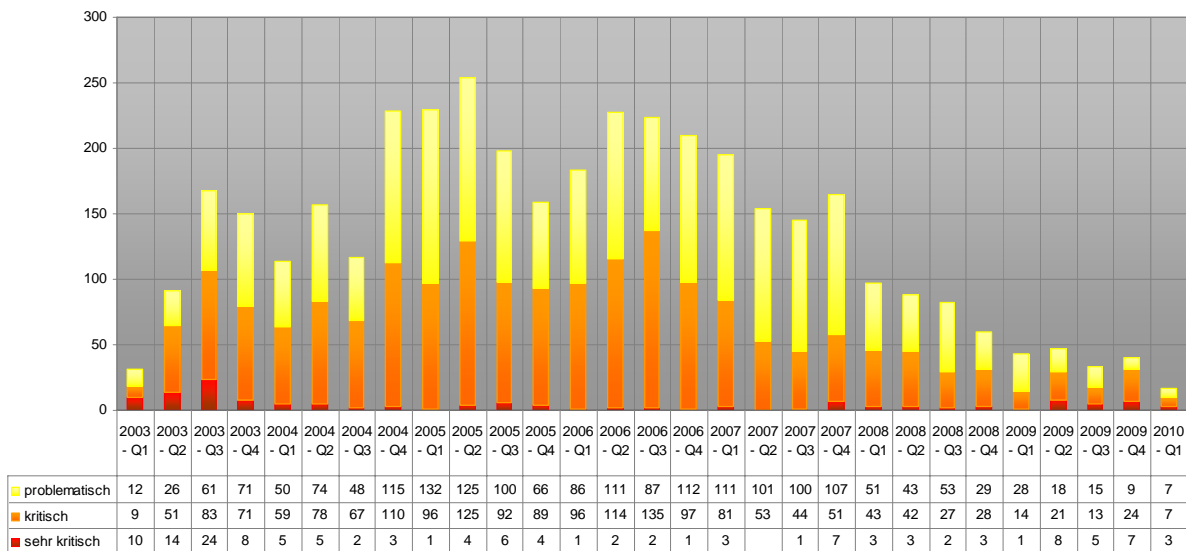
Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2010

Registrierte Schwachstellen by scip AG



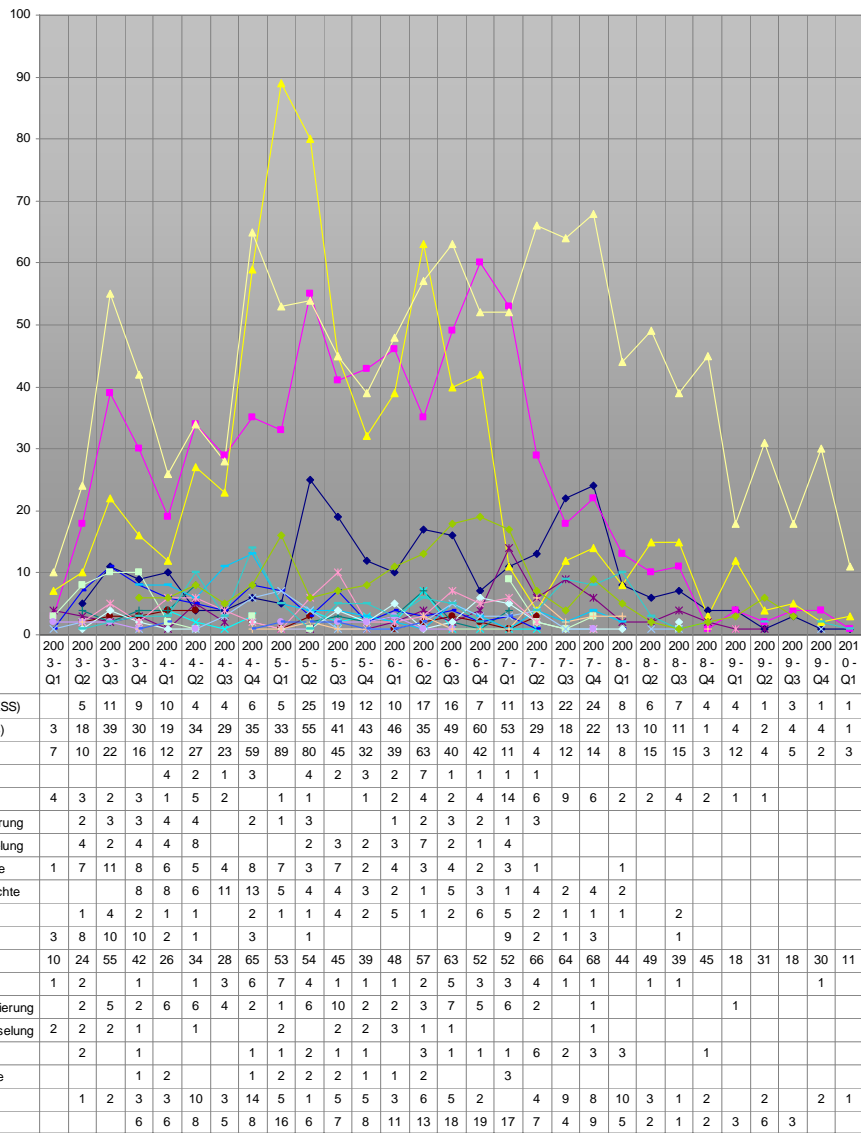
Verlauf der Anzahl Schwachstellen pro Quartal seit 2003 Q1

scip monthly Security Summary 19.03.2010



Verlauf der Anzahl Schwachstellen/Schweregrad pro Quartal seit 2003 Q1





Verlauf der Anzahl Schwachstellen/Kategorie pro Quartal seit 2003 Q1

5. Labs

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

5.1 Nessus generische Plugins für Webapplikationen

12.03.2010 Marc Ruef, maru@scip.ch

Die Entwickler von Nessus haben eine Reihe zusätzlicher generischer Plugins für Web Application Penetration Tests herausgegeben bzw. bestehende Tests erweitert. Das Ziel dieser ist, typische Schwachstellen – wie Cross Site Scripting und SQL-Injection – mittels Fuzzing zu identifizieren. Damit können also nun auch neue und nicht mit dedizierten Plugins abgearbeitete Schwachstellen gefunden werden:

ID	Name
44967	CGI Generic Command Execution Vulnerability (time based)
44136	CGI Generic Cookie Injection Scripting
44135	Web Server Generic Cookie Injection
44134	CGI Generic Unseen Parameters Discovery
43160	CGI Generic SQL Injection (blind, time based)
42872	CGI Generic Local File Inclusion Vulnerability (2nd pass)
42479	CGI Generic SQL Injection Vulnerability (2nd pass)
42427	CGI Generic SQL Injection Vulnerability (HTTP Headers)
42426	CGI Generic SQL Injection Vulnerability (HTTP Cookies)
42425	CGI Generic Persistent Cross-Site Scripting Vulnerability
42424	CGI Generic SQL Injection (blind)
42423	CGI Generic SSI Injection Vulnerability
42056	CGI Generic Local File Inclusion Vulnerability
42055	CGI Generic Format String Vulnerability
42054	CGI Generic SSI Injection Vulnerability
39469	CGI Generic Remote File Inclusion Vulnerability
39468	CGI Generic Header Injection Vulnerability
39467	CGI Generic Path Traversal Vulnerability

ID	Name
39465	CGI Generic Command Execution Vulnerability
11139	CGI Generic SQL Injection Vulnerability

Diese Plugins arbeiten relativ simpel. Das Grundprinzip ist stets das Gleiche:

1. Schnittstellen S zur Übergabe von Parametern werden gesucht.
2. Varianten bössartigen Codes M werden generiert.
3. Pattern P zur Identifikation der erfolgreichen Injektion werden definiert.
4. Die Anfragen der Form S(M) werden abgesetzt und damit die Resultate R generiert.
5. In den erhaltenen Resultaten werden die Pattern (S(M) R) = P gesucht.
6. Ist P in R enthalten, gilt die Schwachstelle als erfolgreich ausgenutzt.

Konnte also eine Reaktion provoziert werden, die auf einen erfolgreichen Angriff hindeuten, wird die Schwachstelle als gegeben ausgewiesen. Dabei wird jenem Muster gefolgt, wie es auch bei manuellen Tests herangezogen wird:

Technik	Resultat	Beispiel
Cross Site Scripting	Injizierten Code	BODY ONLOAD=alert(\$URL\$)
SQL-Injection	SQL-Fehlermeldungen	supplied argument is not a valid MySQL result

Der Pseudocode für die Implementierung eines Plugins, das SQL-Injection in HTTP-Headern prüft, sieht wie folgt aus. Neben der Definition der einzelnen Elemente in Arrays sind die verschachtelten Schleifen für das Ausprobieren der jeweiligen Anfragen verantwortlich:

```
function findXssIn-Header($target='127.0.0.1', $port=80){
    // Pre-defined arrays (some examples)
    $headerarr = array('User-Agent', 'Referer', 'Accept');
    $maliciousarr = array('"%22', '-+');
    $patternarr = array('Incorrect column name', 'Unknown table');

    // Generation of test requests
    foreach($headerarr as $header){
        foreach($maliciousarr as
```

```

$malicious){
    // Sending dedicated test
    request
    $response =
    http_get_request($target, $port,
    $header, $malicious);

    // Identification of pat-
    terns
    foreach($patternarr as
    $pattern){
        if(find($response,
    $pattern) == TRUE){
            return 1;
            exit;
        }
    }
}
return 0;
}

```

Links:

<http://community.nstalker.com/n-stalker-security-scanner-2009-is-released>

<http://nstalker.com/products>

<http://pages.cs.wisc.edu/~bart/fuzz/>

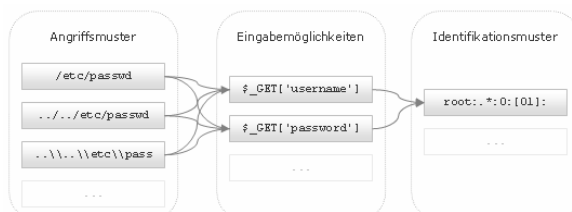
<http://www.compute.ch/download.php?view.713>

<http://www.compute.ch/projekte/tractatus/?s=tractatus&m=liste&h=5.3.2.1.2&l=6>

<http://www.nessus.org>

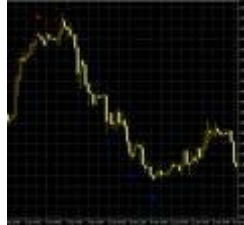
http://www.scip.ch/publikationen/fachartikel/scip_cross_site_scripting.pdf

Ein solcher Ansatz ist theoretisch für jede Schwachstelle umsetzbar, die sich durch eine korrupte Eingabe oder einen korrupten Programmablauf provozieren und anhand eines spezifischen Verhaltens (z.B. Rückgabewert einer typischen Struktur) ermitteln lässt. Eine erste Fokussierung von Nessus auf Webapplikationen liegt wohl darin begründet, dass das genutzte Anwendungsprotokoll relativ simpel ist (Klartext und umfassend dokumentiert), die Kombinationen aus Reiz/Reaktion gut erforscht sind sowie Webapplikationen eine sehr hohe Verbreitung finden. Weiterführende Implementierungen für anderweitige Angriffstechniken – wie zum Beispiel LDAP-Injection oder OS Command Injection – liessen sich nach dem selben Prinzip implementieren.



Diese Weiterentwicklung von Nessus ist wichtig und war dringend nötig. Der kommerzielle HTTP-Scanner N-Stalker hatte den exakt gleichen Schritt beispielsweise ebenfalls im umfassenden Rewrite der Version 2009 vollzogen. Denn nur damit kann den grundlegenden Schwächen des Produkts, das auf Reaktionen statt Aktionen setzt (auch ein grundlegendes Problem von Antivirus), entgegengetreten werden. Damit werden nun auch individuelle Applikationen, für die keine dedizierten Produkte-Plugin zur Verfügung stehen, erfolgreich angegriffen werden.

6. Bilderrätsel



GESUCHTE BEGRIFFE		
3 (english)	11 (english)	9 (english)

LÖSUNGSWORT

Wettbewerb

Mailen Sie uns das 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 **15.04.2010**.

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.

Gewinnen Sie ein Exemplar des Buches „Die Kunst des Penetration Testing“ von Marc Ruef. Dem meistverkauften deutschsprachigen Penetration Testing Fachbuch auf dem Markt.



<http://www.computec.ch/mruef/?s=dkdpt>
 911 Buchseiten, ISBN 3-936546-49-5

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 Ruef
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!](#)