

Contents

1. Editorial
2. scip AG Informationen
3. Statistiken Verletzbarkeiten
4. Interview
5. Bilderrätsel
6. Impressum

1. Editorial

Neue alte Anforderungen an die Cyber-Generation

Viele Leute meinen, dass ich nur so von Technomanie strotzen würde. Schliesslich gehöre ich zur Zunft der Informatiker und die haben ja schliesslich nichts anderes im Kopf, als Computer und kleine technische Geräte. Falsch. Ich mag weder Computer noch kleine technische Geräte. Ich bin mir lediglich der Vorteile der effizienten Nutzung dieser zur performanten Erledigung spezifischer Aufgaben bewusst. Eigentlich ein sehr ökonomischer Wesenszug.

Ich besitze seit bald 15 Jahren keinen Drucker. "Wieso das?", werde ich immerwieder gefragt. Ganz einfach: Ich brauch es nicht. Was gibt es auf diesem Planeten, was ich unbedingt aus einer elektronischen Form auf Papier bringen müsste? Eine Adresse oder Telefonnummer kann ich mir auch aufschreiben. Oder ich speichere sie elektronisch(!) in meinem Mobiltelefon. Wahre ich nämlich den digitalen Zustand der Information, kann ich sie unkompliziert weiterverarbeiten. Datenverarbeitung, darum gehts ja mitunter in



"Mit dem Computer lösen wir vorwiegend Probleme, die wir ohne ihn nicht hätten."

Eine Freundin hat mir davon berichtet, was sie von einer Vorlesung eines japanischen KI-Forschers gehört hätte. Dieser habe in vollem Eifer erzählt, dass in absehbarer Zeit Androiden geschaffen werden können. Diese menschenähnlichen Roboter seien in der Lage, auf seine Kinder aufzupassen, während er seiner Arbeit nachgeht. Meines Erachtens zurecht war sie entrüstet, dass sein Schluss nicht umgekehrt (oder wenigstens bidirektional) ausfiel:

"Roboter schaffen, um Arbeiten zu erledigen, damit man Zeit für seine Kinder hat."

Mit all den Computern um uns herum vergessen wir gerne, dass es um den Menschen zu gehen

der Informatik. Und nicht um Drucker und Papier.

Wo wir gerade von Mobiltelefonen sprechen. Ich weigere mich seit eh und je, einen "coolen" Klingelton zu haben. Meine Telefone klingeln immer gleich: Wie Telefone. "Aber das ist doch nicht zeitgemäss, ja gar langweilig", hat man mir auch schon gesagt. Nein. Es lohnt sich nicht, ein MP3 meines Lieblingslieds aufzuspielen, weil ich ja sowieso im besten Fall nur die ersten 10 Sekunden dessen höre (Bei Tool wäre das eine Unsinnigkeit sondergleichen). Es schmerzt mich mehr im Herz, dass ein gutes Lied mittendrin unterbrochen wird, weder dass ich von einem Telefon-Klingelton angeklungelt werde.

Bin ich zudem unterwegs und höre irgendwo mein "Lieblingslied", woher soll ich dann wissen, dass das mein Telefon ist? Es laufen ja eh überall Radios oder TVs. Und meistens hör ich sowieso MP3s auf meiner Sony PSP. Ich müsste mich noch viel mehr darauf konzentrieren, ob mein Telefon nun klingelt oder nicht. Ich kauf mir doch keinen überteuerten Technikschratt, um mich dann auch noch darauf konzentrieren zu müssen, wenn Leute mich stören. Wo kommen wir denn da hin? Es stimmt halt schon:

hat. Ein Computer kann einen Menschen ersetzen. Jedoch nicht in Bezug auf die Menschlichkeit; wieso sollte er überhaupt? Maschinelle Abläufe, für die der Mensch von Natur aus nicht geschaffen wurde (sehr aufwändig, gefährlich oder anstrengend), die sollten durch Roboter übernommen werden. Alles andere hat die Domäne der natürlichen humanoiden Lebensformen zu bleiben.

In einer idealen Welt sollten Roboter ausschliesslich dabei helfen, dass ein jeder Mensch in der Maslow'schen Bedürfnispyramide die Spitze der Selbstverwirklichung erreicht. Dass dies auch noch durch die Roboter abgenommen wird, wäre eine Perversion sondergleichen. Unsere Generation tut gut daran dies zu verinnerlichen und der nächsten Generation weiterzugeben.

Die von Isaac Asimov erstmals in seiner Kurzgeschichte "Runaround" (1942) als Grundregeln des Roboterdienstes beschriebenen Robotergesetze sind und bleiben daher sehr wichtig für die Zukunft. Schliesslich müssen sich Roboter an die Vorgaben halten, um für uns Menschen auch von Vorteil zu sein. Zeitgleich wird es aber umso wichtiger, dass es sogenannte Mensch-Maschinen-Gesetze gibt, die den Verhaltenskodex des Menschen gegenüber Maschinen charakterisieren:

1. Stelle eine Maschine nie über einen Menschen (oder ein anderes Lebewesen).
2. Nutze eine Maschine nach Möglichkeiten immer dann, wenn sich durch sie ein Mensch entlasten lässt.
3. Eine Maschine darf nie zur Schädigung oder Behinderung eines Menschen eingesetzt werden.

Eine der grössten Herausforderungen der nächsten Generation wird es sein, sich in ethisch-moralisch richtiger Weise auf diese Aufgabe einzustimmen. Vielleicht sollten die Prinzipien dessen in einem neuen Schulfach "Robotismus" oder allgemein "Ethik" gelehrt werden: Wann nutze ich eine Maschine und wann arbeite ich lieber selbst? Für viele scheint diese Frage nämlich Sehr schwierig "richtig" zu beantworten zu sein.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 5. November 2007

2. scip AG Informationen

2.1 Log Analyse

Die Nachvollziehbarkeit durchgeführter elektronischer Aktionen wie z.B. das ändern des Passwortes oder der Aufruf der Applikation X mit dem Benutzernamen Q, werden je länger je mehr durch anstehende Gesetze respektive quasi Regulatorien (SOX 404, Basel II etc.) gefordert oder durch die interne Revision beanstandet.

Um einen echten Mehrwert zu erreichen, besteht die Herausforderung darin aus der immensen Anzahl an Logdaten, nach der Sammlung, die relevanten Daten auszufiltern und entsprechend zu Reporten.

Nebst der Einstellung der entsprechenden Logdetails der Applikationen und Betriebssysteme, deren Sammlung, deren sicherer Transportierung, der adäquaten Archivierung ist der Analyse und Korrelierung der Daten höchste Priorität zuzuweisen. Der Nutzen einer Umgebung ist erst gegeben, wenn die zuständigen Stellen mit den erhobenen Daten die geforderten Ansprüche erfüllen können.

Die Definierung des Projektumfangs ist hier einer der Schlüssel zum Erfolg. Je nach Kunde und dessen Anforderungen sind unterschiedliche Schritte zu priorisieren.

Dank unserem ausgewiesenen Expertenwissen in diesem sehr dedizierten Gebiet haben wir als scip AG die Ehre bereits namhafte nationale und internationale Unternehmungen in den Belangen des Eventmonitoring und der Log Analyse unterstützen und begleiten zu können.

Zählen auch Sie auf uns:

- Analyse, Evaluation und Beratung
- Event Correlation, Handling und Alerting
- Ganzheitliche Konzeption
- Integration Know-How Partner
- Konzept Review
- Second Opinion
-)SELROSY(SEcureLOgReoprtngSYstem

Kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail auf chris.widmer@scip.ch

3. Statistiken Verletzbarkeiten

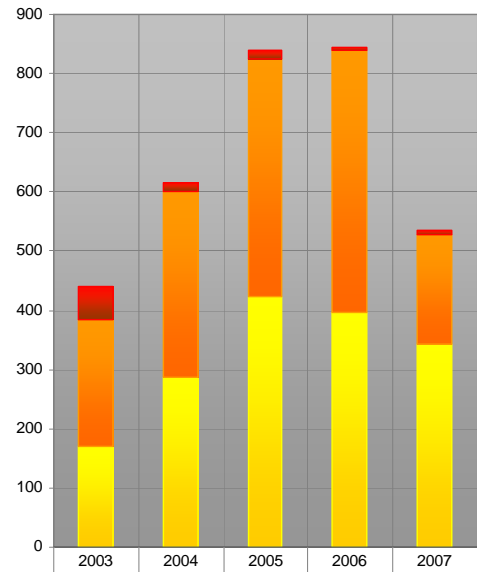
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

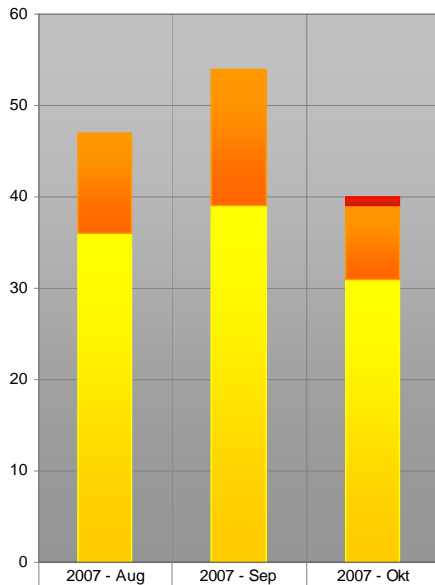
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum: 19. Oktober 2007



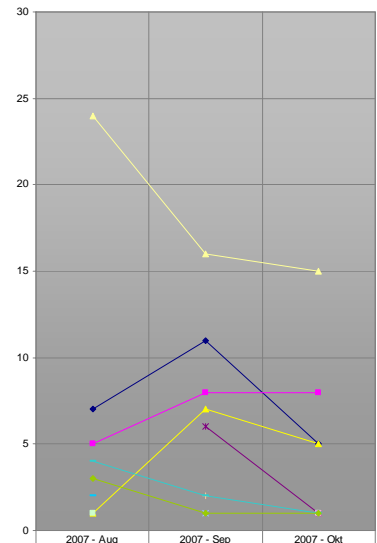
	2003	2004	2005	2006	2007
sehr kritisch	56	15	15	6	5
kritisch	214	314	402	442	186
problematisch	170	287	423	396	343

Verlauf der Anzahl Schwachstellen pro Jahr



	2007 - Aug	2007 - Sep	2007 - Okt
sehr kritisch	0	0	1
kritisch	11	15	8
problematisch	36	39	31

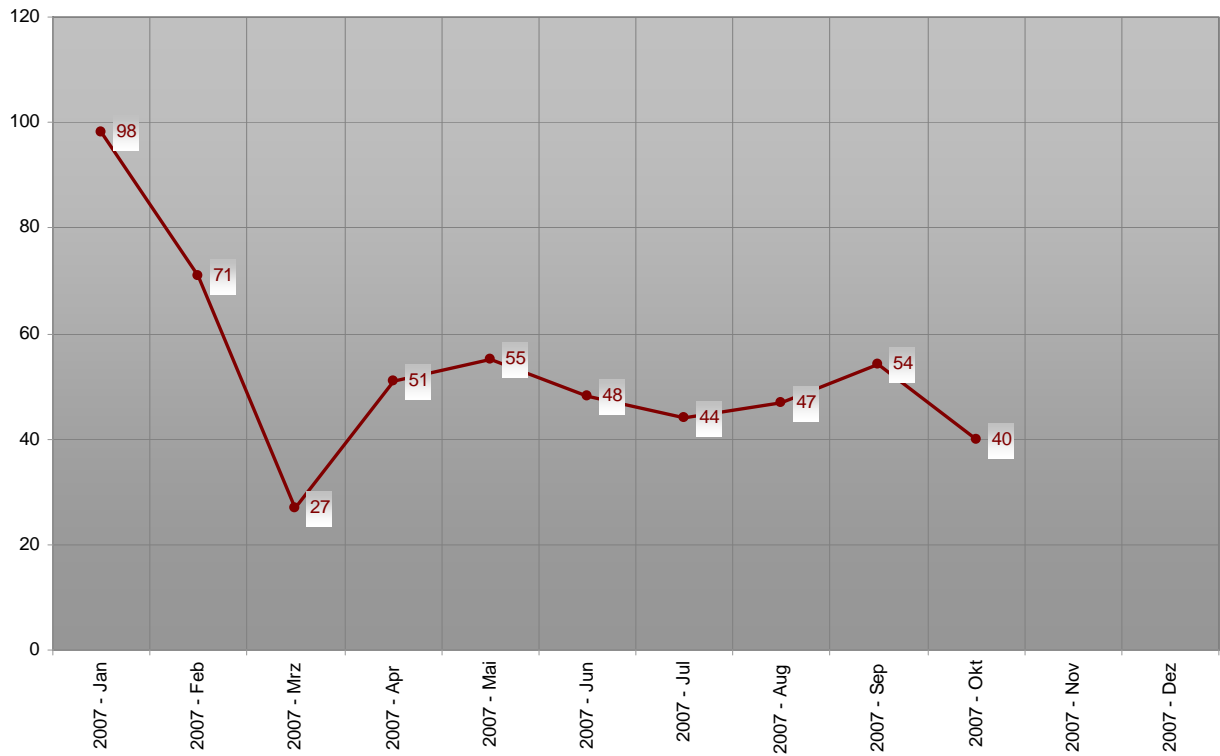
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



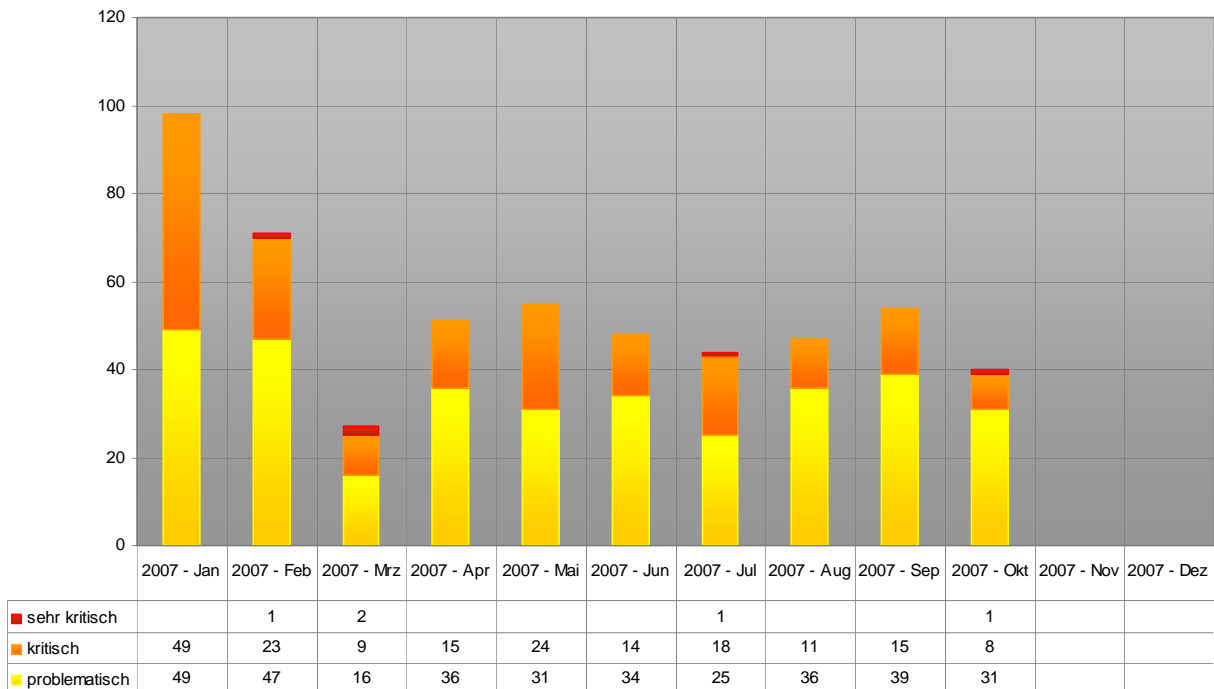
	2007 - Aug	2007 - Sep	2007 - Okt
Cross Site Scripting (XSS)	7	11	5
Denial of Service (DoS)	5	8	8
Designfehler	1	7	5
Directory Traversal	0	0	0
Eingabeungültigkeit	0	6	1
Fehlende Authentifizierung	0	0	0
Fehlende Verschlüsselung	0	0	0
Fehlerhafte Leserechte	0	0	0
Fehlerhafte Schreibrechte	2	0	1
Format String	0	0	0
Konfigurationsfehler	1	0	1
Pufferüberlauf	24	16	15
Race-Condition	0	1	0
Schwache Authentifizierung	0	0	1
Schwache Verschlüsselung	0	0	1
SQL-Injection	0	2	0
SymLink-Schwachstelle	0	0	0
Umgehungs-Angriff	4	2	1
Unbekannt	3	1	1

Verlauf der letzten drei Monate Schwachstelle/Kategorie

Registrierte Schwachstellen by scip AG

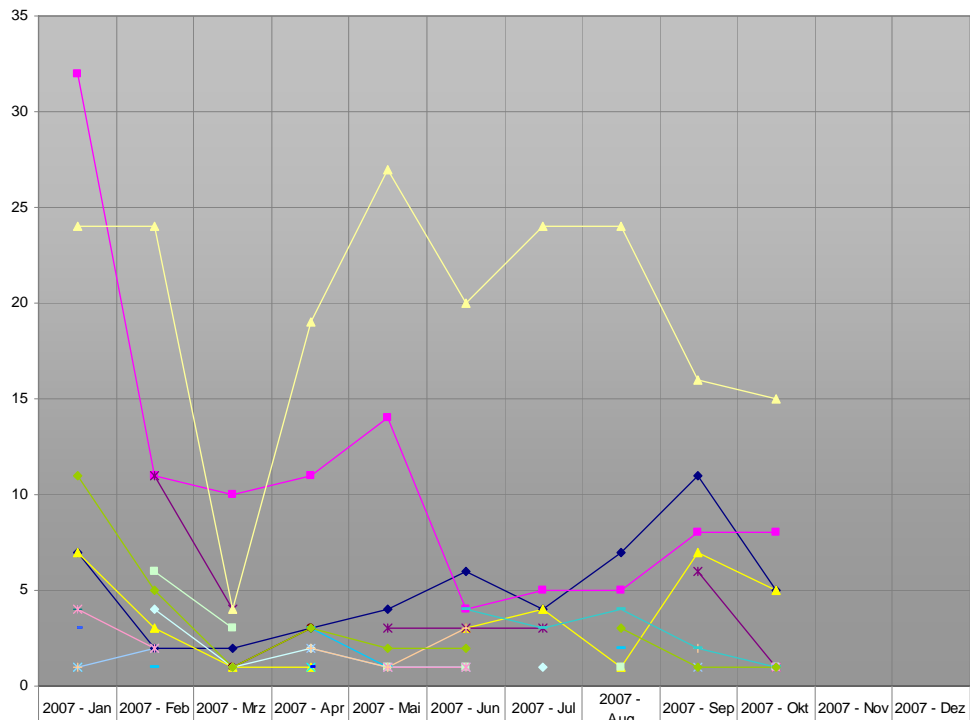


Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2007



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2007

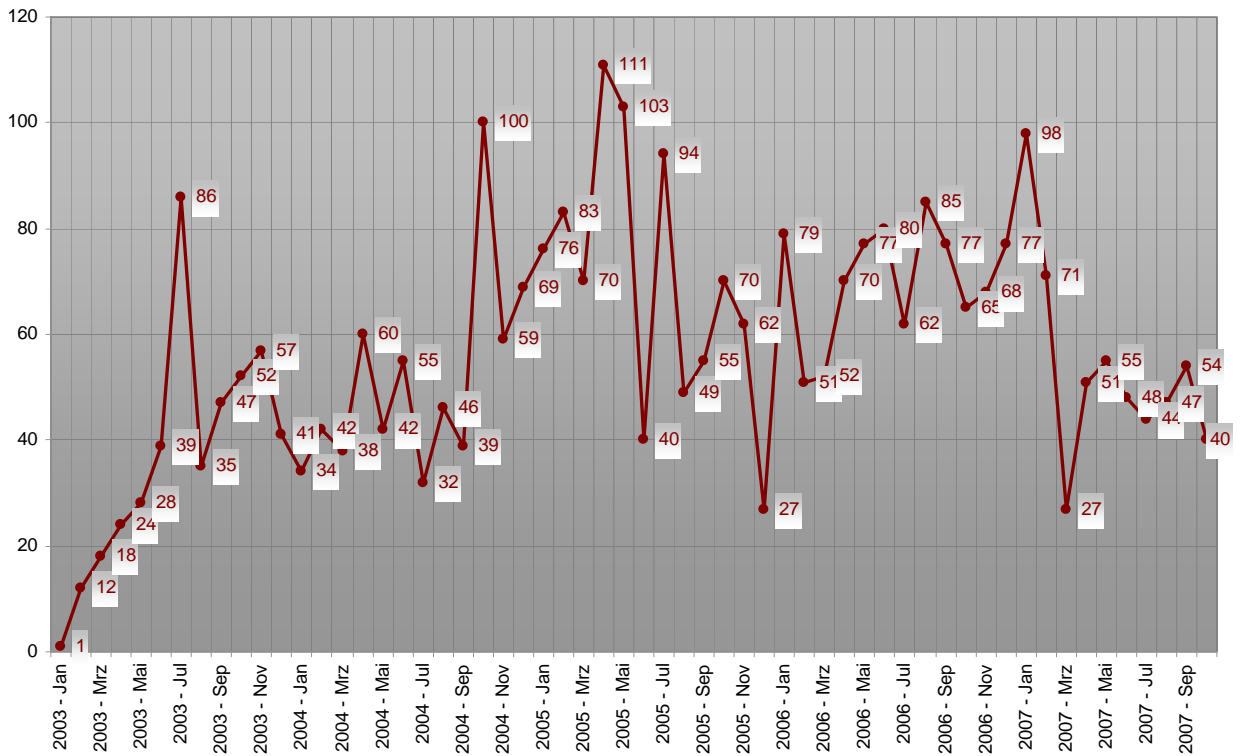




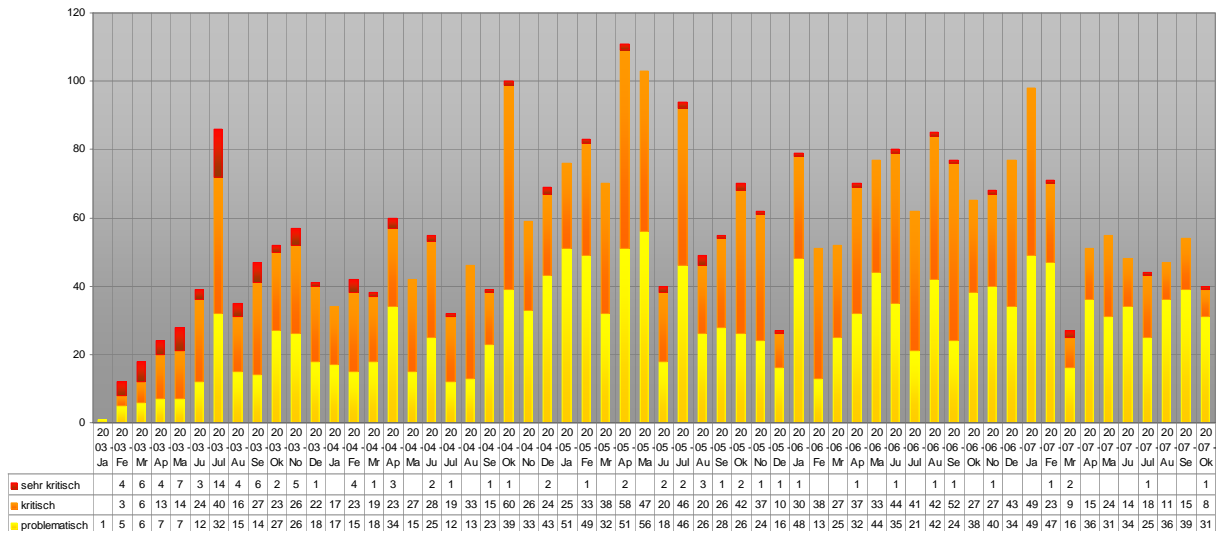
	2007 - Jan	2007 - Feb	2007 - Mrz	2007 - Apr	2007 - Mai	2007 - Jun	2007 - Jul	2007 - Aug	2007 - Sep	2007 - Okt	2007 - Nov	2007 - Dez
◆ Cross Site Scripting (XSS)	7	2	2	3	4	6	4	7	11	5		
■ Denial of Service (DoS)	32	11	10	11	14	4	5	5	8	8		
▲ Designfehler	7	3	1	1		3	4	1	7	5		
✕ Directory Traversal	1			1								
✱ Eingabeungültigkeit		11	4		3	3	3		6	1		
● Fehlende Authentifizierung			1	3								
⊕ Fehlende Verschlüsselung	4											
⚡ Fehlerhafte Leserechte	3											
⚡ Fehlerhafte Schreibrechte		1		3	1			2		1		
⊕ Format String		4	1	2			1					
■ Konfigurationsfehler		6	3		1	1		1		1		
▲ Pufferüberlauf	24	24	4	19	27	20	24	24	16	15		
✕ Race-Condition	1	2		2	1	1			1			
✱ Schwache Authentifizierung	4	2			1	1				1		
● Schwache Verschlüsselung											1	
⊕ SQL-Injection	1			2	1	3			2			
⚡ Symlink-Schwachstelle	3											
⊕ Umgehungs-Angriff						4	3	4	2	1		

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2007

Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat

4. Interview

4.1 Interview mit Steven Christey – Common Vulnerabilities and Exposures List of The MITRE Corporation

Steven Christey, <http://cve.mitre.org/>
 Marc Ruef, maru@scip.ch

Steve Christey ist Technical Lead der Common Vulnerabilities and Exposures List der The MITRE Corporation. Das Ziel der CVE ist die einheitliche Identifizierung von Schwachstellen – ein Name für eine Schwachstelle. Weltweit verweisen Firmen auf diese definierten Nummern.

scip AG: Hallo Steve. Vielen Dank, dass Du Dir die Zeit für dieses Interview nimmst. Du hast bei CVE die Position des Technical Lead inne. Wie liest sich Deine Job Description?

Steve: Ich bin für die Qualitätssicherung, die Konsistenz der Beiträge sowie das Einhalten von Terminen zuständig. Dabei leite ich das Team der Analysten, begutachte vor der Veröffentlichung ihre Arbeiten und lenke die zukünftigen Entwicklungen des CVE-Projekts. Hierbei arbeite ich sehr eng mit meinen Kollegen Dave Mann, der Leiter des Projekts, sowie Bob Martin, Leiter des Compatibility Programms, zusammen.

Regelmässig fungiere ich dabei als Schnittstelle zu Software-Entwicklern, Security-Anbietern, Researchern, Koordinatoren von Drittherstellern, Regierungsbehörden und anderen Gruppierungen. Die meiste Zeit investiere ich dabei in das Reservieren von CVE-Nummern, so dass diese in einer initialen Veröffentlichung neuer Schwachstellen verwendet werden können. Oftmals kommen Leute mit weiteren technischen Details auf uns zu, so dass wir die bestehenden CVE-Beschreibungen anpassen und erweitern können.

scip: Nun, eine zugleich einfache und schwierige Frage für den Anfang: Wann wird etwas als Verwundbarkeit (engl. vulnerability) verstanden und durch das CVE Editorial Board diskutiert? Wie der Abschnitt zu den Terminologien auf der Webseite demonstriert (<http://cve.mitre.org/about/terminology.html#Problem>), kann es hierbei komplett unterschiedliche Ansichten geben.

Die besagte Definition ist politisch motiviert und wahrt selbst auf technischer Ebene ihre Gültigkeit! Im Sommer 1999, kurz bevor wir mit einer ersten Version der "Common Vulnerability Enu-

meration" an die Öffentlichkeit traten, entbrannte im Rahmen des Editorial Board eine hitzige Diskussion zu diesem Thema. So wurden einige CVE-Titel durch diverse Leute nicht als "Verwundbarkeiten" verstanden. Viele der CVE-Einträge entstanden von den Berichten entsprechender Securityscanner. Diese sind darum bemüht, nicht nur sicherheitsrelevante Probleme zu melden, sondern ebenfalls solche, die sich auf Richtlinien - zum Beispiel das Anbieten des finger-Dienstes zur Ermittlung von bestehenden Benutzernamen - zurückführen lassen. Abgesehen von "Privacy Issues" kann eine solche Unschönheit nicht für die Kompromittierung des Systems genutzt werden. Wir wollten derlei Angriffsflächen dennoch innerhalb von CVE abhandeln, um die Diskussion dieser toolübergreifend gestalten zu können. So führten wir den Begriff "exposure" ein und änderten den Namen des Projekts zu "Common Vulnerabilities and Exposures". Die Grundlage dafür sollte eine einfache und klare Definition der Begrifflichkeiten bilden.

Ein grundlegendes Problem, wie Du richtig bemerkt hast, sind die verschiedenen Sichtweisen. Es gibt Leute, die von CVE-Einträgen Hinweise darauf erwarten, wie in ein System eingebrochen werden kann, welche Patches für das Beheben eines Fehlers erforderlich sind, usw. Wir versuchen uns hingegen auf die Verwundbarkeit als solche zu fokussieren.

„So wurden einige CVE-Titel durch diverse Leute nicht als "Verwundbarkeiten" verstanden.“

Selbst wenn man sich auf solche Verwundbarkeiten konzentriert, können die Prioritäten innerhalb von Unternehmungen bezüglich Risikotoleranz, Bedrohungslage, externen Faktoren wie Regulierungen sowie die Möglichkeit der Prävention und Reaktion gänzlich unterschiedlich ausfallen. Diese Abweichungen spiegeln sich selbst in der Definition des Common Vulnerability Scoring System (CVSS), einer standardisierten Metrik zur individuellen Bewertung von umgebungsbezogenen Angriffsmöglichkeiten, wieder.

Diese Diversität sowie die fortwährende Evolution in diesem Bereich berücksichtigend, versuchen wir die Bedürfnisse der CVE-Nutzer zu verstehen und weiterzuarbeiten. Aus diesem Grund beinhaltet CVE praktisch jede Schwäche, die sich sicherheitsrelevant auf den Bereich der Informationstechnologie auswirken kann. Dennoch müssen wir Grenzen setzen. Zum Beispiel führen wir keine Einträge zu Gegebenheiten, die

ausschliesslich ein dediziertes Paket einer einzelnen Webseite betrifft. Wir fokussieren uns also auf verbreitete Software, die durch Firmen gekauft und in ihren Netzen betrieben werden kann.

Wir haben ebenfalls ein separates Projekt ins Leben gerufen, welches ähnliche Fälle adressieren soll. So beschäftigt sich CCE (Common Configuration Enumeration) zum Beispiel mit IT-Richtlinien und Konfigurationen, während sich Common Event Expressions (CEE) um Security Events und Logging kümmert.

Nach diesem Exkurs erscheint es vielleicht fast ein bisschen ironisch, dass ich selbst nicht genau sagen kann, was eine Vulnerability überhaupt ist. Die meisten Definitionen greifen auf andere vage Begriffe zurück, so dass ein weitläufiger Spielraum für Interpretationen zurückbleibt. Erst wenn wir verständliche Modelle haben, um die Funktionsweise von Software zu definieren, werden wir mit akkuraten Begriffsdefinitionen aufwarten können. Selbstverständlich ist CVE nach wie vor von Nutzen, auch wenn es bisher keine perfekte Antwort für diese schwierige Frage gibt.

Scip: Im Juli 2007 wurde der 25'000 Eintrag in der CVE-Datenbank vorgenommen (<http://cve.mitre.org/news/index.html#20070705a>). Herzliche Gratulation hierzu! Was war denn die verrückteste Schwachstelle, die jemals im Board diskutiert wurde? Und welches scheint die wichtigste oder schwerwiegendste Sicherheitslücke, die Du jemals gesehen hast, gewesen zu sein?

Steve: Viele Schwachstellen sind sonderbar, macht man sich die Mühe sie im Detail zu betrachten. Oftmals stolpere ich über Funktionen, in denen der Entwickler einen Haufen Spaghetti-Code zusammengeschustert hat. Dieser scheint nicht selten derart komplex, dass es fast ein Wunder ist, dass das adressierte Problem halbwegs intelligent gelöst werden konnte. Es bleibt sodann fast ein Ding der Unmöglichkeit, den wirren Hintergrund, der hier geschaffen wurde, in seiner Vielschichtigkeit zu begreifen. Derlei Funktionen enthalten oftmals Fehler, die man auf den ersten Blick gar nicht sieht. Und trotzdem handelt es sich dabei meistens um grundlegende Probleme.

Es gibt hier eine konkrete Schwachstelle, an die ich mich erinnern kann. Sie erhält zwar nur 6 von 10 möglichen Punkten auf der Sonderbarkeits-Skala, dennoch gestaltet sie sich sehr obskur: Die Rede ist von CVE-2002-0934. Das besagte

Problem sieht aus wie eine herkömmliche Directory Traversal-Schwachstelle. Da es ein eher unpopuläres Produkt betraf, wurde der Fehler nur durch wenige Spezialisten untersucht. Das Problem war von grosser Besonderheit, weil der Entwickler einen Schutzmechanismus eingebracht hatte, um eben solche Angriffe abzuwehren. Zu diesem Zweck entfernte er als erstes "..", um danach Sonderzeichen zu filtern. Doch die Sonderzeichen hätten gefiltert werden sollen, bevor "." entfernt wurde. Denn aus der korrupten Sequenz ".|" wurde sodann das unliebsame "..", welches sich für entsprechende Attacken einspannen liess.

Dieser Eintrag beeindruckte mich in verschiedener Hinsicht. Als erstes zeigt es sehr deutlich auf, dass auch die defensive Programmierung mit eigenen Problemen zu kämpfen hat. Es ist also nicht ohne weiteres möglich, sämtliche Schwachstellen in umfassender Weise zu adressieren. Zudem handelte es sich um eine komplett neue Angriffstechnik. Doch dies wurde so nicht wahrgenommen, denn das Produkt war unpopulär. Dadurch wurde aber zeitgleich aufgezeigt, dass die Researcher nicht immer so gute Arbeit machen, wie sie machen könnten. Es gibt einfach zu wenige Whitepaper zu diesen und anderen unpopulären Themen. Und aus diesem Grund ist unser Verständnis für viele Arten von Problemen, abgesehen von Pufferüberlauf-Attacken, sehr gering. Schlussendlich hatte noch nicht mal der Finder dieser Schwachstelle realisiert, dass er auf eine neue Angriffstechnik gestossen ist.

Sonderbare Einträge wie CVE-2002-0934 kommen regelmässig vor, weshalb ich intern eine Liste mit den interessantesten Problemen betreue. Eine ältere Version dieser Liste findet sich in Absatz 10.5 des PLOVER Dokuments unter <http://cwe.mitre.org/documents/sources/plover-text.txt> - Nun, ein Problem, das ursprünglich als sonderbar galt, kann plötzlich zur Normalität werden. Jenachdem, wie oft der Sachverhalt wiederentdeckt wird.

„Nicht mal der Finder der Schwachstelle hat realisiert, dass er auf eine neue Angriffstechnik gestossen ist.“

Welche Einträge die wichtigsten und schwerwiegendsten darstellen, kann ich nicht beantworten. Jenachdem wer gefragt wird, wird hier wohl mit einer komplett anderen Antwort zu rechnen sein.

Scip: Die Anzahl der neu veröffentlichten

Sicherheitslücken steigt Woche für Woche an. Aus diesem Grund wird es besonders wichtig, eine Priorisierung und Vorselektion vornehmen zu können. Wie sieht Euer Prozess der Entscheidungsfindung aus, welche Schwachstellen als erstes besprochen und dokumentiert werden sollen?

Die Anzahl ist in der Tat stetig am wachsen, obwohl dieses Jahr ein bisschen gedrosselt hat. Seiten wie SourceForge bieten eine Vielzahl an verbreiteten Produkten an und es gibt eine Vielzahl technisch begabter Researcher, welche typische Probleme finden können. Die Zunahme der Software-Verteilung, gerade in Bezug auf Webapplikationen, ist wohl der Hauptgrund für die Zunahme der bekanntgewordenen Sicherheitsprobleme.

Alle Vulnerability Information Provider, so auch CVE, müssen sich mit der Frage herummühen, welche Probleme beachtet werden sollen, wie viel Aufwand für Verifikationen investiert werden sollen, welche Details man anbieten möchte und wie schnell dies zu geschehen hat. Wir haben unseren Analyseprozess in den letzten Jahren stark optimiert, doch die Anzahl der Einträge bleibt nach wie vor eine Herausforderung.

Zur Zeit legen wir unseren Fokus auf Software von grossen Herstellern, weit verbreiteten Produkten und neuartige Schwachstellen. Doch dies macht nur 20-30 % aller CVE-Einträge aus. Wir stufen die Priorisierung herunter, haben wir Reports von hochgradig unzuverlässigen Researchern zu verarbeiten oder handelt es sich um eine sehr unbekannte Applikation. Wir beraten mit dem Editorial Board ebenfalls CVE-Nutzer, so dass wir hautnah miterleben können, welche Anforderungen und Prioritäten an unseren Dienst gestellt werden.

Scip: Wie sieht es aus mit den "ewigen Kandidaten"? Kann es sein, dass eine unbekannte Anwendung für ewig unverifizierte Candidates aufweist? Wie will man solchen Karteileichen entgegen?

Steve: Wie sich die Zeiten geändert haben! In den frühen Tagen von CVE haben wir gar keine Candidates veröffentlicht. Damals bestand das Bedürfnis noch nicht, Informationen möglichst zeitnah zu erhalten, weshalb das Editorial Board sich die Zeit nehmen konnte, einen Vorschlag umfassend zu prüfen. Doch schnell wuchs das Verlangen nach möglichst schnell bereitgestellten Daten, weshalb wir die Candidates einführt. Einige Jahre spä-

ter überstieg die Anzahl der Vorschläge die Möglichkeiten der Mitglieder des Editorial Boards. Sie konnten nicht mehr für jeden Beitrag abstimmen, weshalb die Anzahl der Candidates zwangsweise wieder zurückging. Als das Interesse am Projekt plötzlich anstieg, konzentrierten wir uns wieder vermehrt auf das Einführen neuer Candidates. Dabei rückten wir die alten Candidates in den Hintergrund. Zwischenzeitlich wird nicht mehr in Monaten oder Wochen, sondern in Tagen und Stunden gerechnet. Aus diesem Grund unterscheiden wird gar nicht mehr gross zwischen Candidates und Entries. Vor einiger Zeit haben wir gar alle CAN-Prefixes durch CVE ersetzt, was scheinbar niemanden gestört hat. MITRE führt mittlerweile fortwährend Modifikationen bestehender Einträge ein, ohne dass das Editorial Board sämtliche Änderungen bestätigen muss. Zwischenzeitlich stützen wir uns mehr auf den Kontakten zu Herstellern, zuverlässigen Researchern und anderen Vulnerability Information Provider ab.

Es den eben genannten Gründen bietet es sich deshalb an, dass in den kommenden Jahren eine Zusammenführung der Candidates und Entries stattfinden wird. Ein offizieller Entry gewährleistet, dass der Fehler wirklich existiert und die Beschreibung zuverlässig ist. Es wäre schön, wenn diese Abstufung auch in Zukunft irgendwie beibehalten werden könnte. Doch wir haben noch nicht herausgefunden, wie wir diesen Aspekt richtig angehen wollen.

Scip: Ein zentralisiertes und standardisiertes System wie CVE konnte sich im Antiviren-Bereich noch immer nicht etablieren. Was denkst Du, ist der Grund dafür?

Denkt man genauer darüber nach, so bemerkt man, dass Verwundbarkeiten in sich geschlossene Entitäten darstellen. Eine Verwundbarkeit mag zwar eine Reihe komplexer Fehler voraussetzen, um zum Sicherheitsproblem zu werden, welches innerhalb eines Angriffs ausgenutzt werden könnte. Jedoch handelt es sich dabei meistens um ein paar Zeilen Programmcode, die mit einem einfachen Bugfix korrigiert werden

„Ein offizieller Entry gewährleistet, dass der Fehler wirklich existiert und die Beschreibung zuverlässig ist.“

können.

Computerviren und anderer korrupter Programmcode sind jedoch eigenständige Software mit einer breitgestützten Codebasis. Zudem gibt

es wohl weit mehr Viren "in the wild", weder bekanntgewordene Sicherheitslücken, wodurch das Klassifizierungsproblem ein weiteres Mass an Komplexität gewinnt. Varianten bekannter Malware kommen weitaus öfter in Umlauf, weder dies bei Sicherheitslücken der Fall ist.

In der Vergangenheit gab es verschiedene Anläufe in der Antivirus-Community, dieses Problem anzugehen. Common Malware Enumeration (CME), welches ebenfalls von MITRE geführt wird, versucht genau hier anzusetzen. Die Virenproblematik hat sich in den letzten Jahren jedoch signifikant verändert: Neue Malware erscheint immer häufiger und breitflächiger, während Hacking-Attacken immer zielgerichteter ausfallen. Kurzgefasst ist das Problem weitaus komplizierter, weder es auf den ersten Blick den Anschein macht. Das ist unbestritten der Grund, warum es hier noch keine umfassende Lösung gibt.

Scip: MITRE ist dem US-Militär und diversen Regierungsorganisationen angegliedert. Welchen Einfluss haben diese auf Eure Arbeiten? Gibt es Informationen, die aus "Sicherheitsgründen" zurückgehalten werden?

Steve: CVE katalogisiert ausschliesslich an die Öffentlichkeit herangetragene Verwundbarkeiten, weshalb hier kein Interessenskonflikt geschaffen wird. Wir haben schlichtweg nicht mit Problemen zu tun, die noch nicht an die Öffentlichkeit gelangt sind. Sind uns Informationen bekannt, die noch nicht herausgegeben wurden, werden wir uns ebenfalls nicht um eine Veröffentlichung dieser bemühen.

Wir werden seit langer Zeit durch die Regierung unterstützt. Unser gegenwärtiger Sponsor ist das Department of Homeland Security (<http://www.dhs.gov/>). Über die Jahre haben unsere Sponsoren begriffen, welche Rolle und welchen Einfluss CVE hat, sowohl bezüglich ihrer finanziellen als auch ihrer moralischen Unterstützung. Wie zum Beispiel die Anforderungen von NIST an Sicherheitsprodukte, die CVE unterstützen.

In den letzten Jahren hat der Regierungsapparat die Vorteile von CVE für sich entdeckt, was gewissen Einfluss auf die Priorisierung unserer Tätigkeiten hat. Zum Beispiel wird die National Vulnerability Database (NVD) komplett auf der Basis von CVE erstellt. Die neuen Anforderungen von NVD haben uns zeitgleich weitere Möglichkeiten für CVE eröffnet. Das Security Content Automation Protocol (SCAP) Programm stützt

sich ebenfalls auf CVE und anderen MITRE-Projekten ab.

Doch es gibt auch andere, nicht regierungsbezogene Einflüsse. Zum Beispiel setzt PCI der Kreditkartenindustrie auf CVSS und die Einstufung von CVSS basiert auf dem CVE-System. Wir konnten viele internationale Hersteller in das Kompatibilitätsprogramm von CVE holen und damit weltweit tätige Representative für das Editorial Board gewinnen. Ebenso treten wir regelmässig auf einschlägigen Konferenzen auf.

Es bleibt eine Herausforderung, allen Erwarten gerecht zu werden und dabei das ursprüngliche Ziel von CVE nicht aus den Augen zu verlieren. Aber ich denke, wir machen hier einen guten Job.

Scip: Mit CVE wurde endlich ein akademischer und empirischer Ansatz in den manchmal ein bisschen esoterisch wirkenden Bereich der Computersicherheit eingebracht. Was sind wohl die nächsten Schritte, um in diesem Bereich ein Mehr an Genauigkeit und Zuverlässigkeit gewährleisten zu können.

Steve: Dem Vulnerability Research Bereich täte es nicht schlecht, wenn die Researcher sich besser organisieren und den Informationsfluss einfacher gestalten könnten. Dies bleibt verhältnismässig schwierig, weil die jeweiligen Researcher sehr unabhängig arbeiten. Es wäre schön, könnten die theoretischen und praktischen Researcher ihre Erkenntnisse unkompliziert teilen. Es wäre nämlich im Interesse beider Lager, doch niemand scheint sich dieser Aufgabe annehmen zu wollen.

Kurzgefasst kann gesagt werden, dass die Verbesserung der Qualitätssicherung im Softwarebereich eine entscheidende Rolle zu spielen hat. Wir müssen Schwachstellen dort begegnen, wo sie entstehen: Im Entwicklungszyklus selbst. Es gibt verschiedene Bestrebungen, die den Entwicklern versuchen dabei zu helfen, dieses Ziel zu erreichen. Seien dies nun die OWASP Top Ten, diverse Bücher oder unterschiedliche Zertifizierungen. Mittlerweile gibt es schliesslich verschiedenste Researcher, die eine Schwachstelle beruflich und professionell untersuchen. Softwaregestützte Audits haben sich in den letzten Jahren drastisch verbessert, so dass auch dieses noch relativ junge Gebiet massgeblichen Einfluss auf die Verbesserung der Codequalität haben wird.

„Unser gegenwärtiger Sponsor ist das Department of Homeland Security (<http://www.dhs.gov/>).“

In Mitten all dieser Prozesse bleiben Metriken die wohl grösste Schwierigkeit der Qualitätssicherung im Software-Bereich. Die bisher üblicherweise angewendeten Systeme zählen lediglich die veröffentlichten Schwachstellen in einem Produkt. Doch diese metrischen Systeme haben viele Limitierungen, die auf ihre Primitivität zurückzuführen sind. Es gibt zwar Bestrebungen im akademischen Umfeld, doch auch da gibt es noch nichts Umfassendes vorzuweisen. Ich hoffe, dass in den nächsten beiden Jahren ein Durchbruch zu verzeichnen ist, wie mitunter an Vorträgen der Metricon 2.0 angetönt wurde.

Für diese spezifischen Bereiche der Softwareentwicklung glaube ich, dass unser Projekt mit dem Namen Common Weakness Enumeration (CWE) eine wichtige Rolle spielen wird. Es ist wiederum an CVE angelehnt, versucht jedoch typische Fehler in der Entwicklung und Programmierung, welche zu Sicherheitsproblemen führen können, zu katalogisieren. Dabei betreiben wir Grundlagenforschung - wir entwickeln einer "Vulnerability Theory" -, welche uns dabei helfen soll, das Problem in seinen Grundzügen erfassen zu können. Und auch hier integrieren wir wie bei CVE die Community, um mit vereinten Kräfte etwas Nützliches zu schaffen. Wir hoffen, dass CWE dabei helfen wird, den Informationsaustausch und die Analysetätigkeiten sowie Metriken zu verbessern.

Scip: Seit Jahren ist die Debatte im Gang, ob Full-Disclosure in Mailinglisten gerechtfertigt ist und vorangetrieben werden soll. Die CVE-Datenbank konsolidiert ausschliesslich Informationen und Links zu externen Ressourcen, ohne selbst Daten bereitzustellen. Aus diesem Grund seit Ihr nicht direkt von technischen Möglichkeiten, wie spezifischen Exploits abhängig? Stand es jemals zur Diskussion, dass CVE ebenfalls technische Hintergrundinformationen bereitstellt? Oder wolltet Ihr lieber eine standardisierte Bewertung von Vulnerabilities (z.B. ein Zusammenschluss mit CVSS) angehen?

Steve: Manchmal veröffentlichen Researcher Exploits ohne weitere Details oder technische Hintergrundinformationen. In diesem Fall müssen wir den Exploits zuerst analysieren, um zu verstehen, was er überhaupt macht und welche Schwachstelle er ausnutzt. Dabei verweisen wir nach

wie vor auf die Original-Information (den Exploit), damit auch unsere Nutzer direkt verstehen, auf welcher Informationsbasis da aufgebaut wird.

Wir fokussieren uns darauf, den Lesern nach Möglichkeiten alle Informationen bereitzustellen, damit zwei CVE-Einträge eindeutig voneinander unterschieden werden können. Über die Jahre hinweg haben wir gelernt, dass Details zu Exploits enorm wichtig sein können, um diese Ziel erreichen zu können. Genauso wie der Schwachstellentyp, die betroffenen Parameter oder miteinander bezogenen Software-Komponenten. Aus diesem Grund haben ältere CVE-Einträge manchmal keine Hintergrundinformationen zu Exploits. Damals wussten wir halt einfach noch nicht, wie wichtig diese Daten sein würden.

Dabei hat CVSS keinen weiteren Einfluss darauf, wie wir unsere Beiträge aufbereiten. Das NVD-Team weist die CVSS Scores zu und versucht, sollte es erforderlich sein, weitere Forschungen zu betreiben.

Scip: Die subkulturelle Dimension von Hackern und Computerwissenschaftlern hat sich in den letzten Jahren stark verschoben. Der Verkauf von Verwundbarkeiten an Firmen wie iDefense (<http://www.iddefense.com/>) oder das Feilbieten von Exploits auf Auktionsplattformen wie WasiSabiLabi (<http://www.wslabi.com/>) wurden salonfähig. Welchen Einfluss hat diese Entwicklung auf Eure Arbeit?

Steve: Drittfirmen wie iDefense und ZDI greifen in ihren Advisories auf CVE-IDs zurück. Und auch die jeweiligen Hersteller beziehen sich auf unsere Einträge. Entsprechend können alle davon profitieren, die CVE nutzen. Die besagten Drittfirmen arbeiten ebenfalls mit den Herstellern zusammen, was dazu führt, dass die technischen Informationen normalerweise korrekt ausfallen. Dies verringert den Aufwand, den wir für die Prüfung entsprechender Meldungen aufwenden müssen. Die Öffentlichkeit erhält damit bessere und zuverlässigere Informationen, weder wenn die Advisories ohne Koordination aufgesetzt werden würden.

Auktionen wie WasiSabiLabi sowie Researcher, die undetaillierte Pre-Advisories herausgeben, stellen eine besondere Herausforderung für CVE und Verwundbarkeitsdatenbanken dar. Wie zuvor erwähnt, stützt sich CVE gerne auf technische Exploits ab, um eindeutig zwischen unter-

„Doch Programmierer bleiben Menschen und Menschen pflegen Fehler zu machen.“



schiedlichen Fehlern unterscheiden zu können. Mit Pre-Advisories und Auktionen fallen diese Details weg, so dass wir nicht wirklich entscheiden können, ob es sich bei einem veröffentlichten Problem um eine altbekannte oder eine neue Sache handelt.

Es gibt weitere Faktoren, die diese Situation verkomplizieren. Wird zum Beispiel in einer Auktion ein Fehler in einem bestimmten Produkt skizziert und jemand anderes schaut sich dies nun genauer an, kann er unter Umständen eben diesen Fehler für sich entdecken. Wie kann nun herausgefunden werden, ob es sich um exakt das gleiche Problem handelt? Andererseits sind solche Gegebenheiten durchaus diskussionswürdig, weshalb CVE gerne Identifiers vergibt und die Gegebenheiten auch über einen längeren Zeitraum hin beobachtet.

Solche Herausforderungen spezieller Natur gibt es immerwieder für das CVE-Projekt. Normalerweise brauchen wir ein bisschen Zeit, bis wir den besten Weg gefunden haben, mit den neuen Anforderungen richtig umgehen zu können. (lacht)

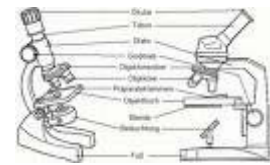
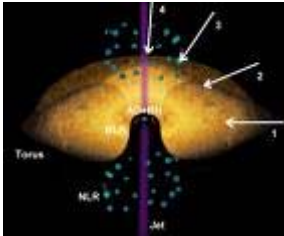
Scip: Die Schweizer Armee hat vor einigen Monaten in den Medien angekündigt, sogenannte Cyber-Soldaten für einen Cyberkrieg ausbilden zu wollen. Für meinen Geschmack kommt diese Forderung ein bisschen spät ... Denkst Du, dass die elektronische Kriegsführung bei internationalen Konflikten in Zukunft fortwährend an Bedeutung gewinnen wird?

Steve: Vor einigen Jahren hätte diese Forderung sehr unrealistisch geklungen. Doch die Tagesmedien machen es einem immerwieder klar, dass sich die Zeiten geändert haben und sehr viel auf dem Spiel steht. Sei dies nun die organisierte Kriminalität oder nationale Bedrohungen (z.B. Terrorismus). Aus diesem Grund ist und bleibt es enorm wichtig, Software-Sicherheit als solche wahrzunehmen und weiterzupflegen. Idealerweise wäre es natürlich wünschenswert, dass die Softwarequalität derartig gut werden würde, dass Projekte wie CVE überflüssig wären. Doch Programmierer bleiben Menschen und Menschen pflegen Fehler zu machen. Es wird also noch viel Zeit verstreichen, bis wir uns über das Erreichen dieser wohl doch utopischen Ziele freuen können.

Scip: Steve, vielen Dank für das Interview. Ich wünsche Dir und Deinem Team weiterhin viel Glück mit CVE!

Steve: Vielen Dank an Dich für die tiefgründigen Fragen. Ich hoffe, dass meine Antworten nicht zu ausschweifend ausfielen (lacht). Wir freuen uns darüber, dass CVE für eine Vielzahl von Leuten genutzt und geschätzt wird. Auch weiterhin werden wir uns den Anforderungen stellen wollen.

5. Bilderrätsel



GESUCHTE BEGRIFFE		
7 Buchstaben (engl.)	8 Buchstaben (engl.)	6 Buchstaben

LÖSUNGSWORT

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 **15.12.2007**. 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> unter Publikationen > scip monthly Security Summary > Errata.

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

SECURITYTRACKER



6. 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 IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams 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, TrendMicro, 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 Summaries finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)