

Contents

1. Editorial
2. Neue Sicherheitslücken
3. Kreuzworträtsel
4. Impressum

1. Editorial

Webblogs ein Sicherheitsrisiko?

Der Siegeszug der Webblogs begann bereits vor einiger Zeit. In Übersee und Asien sehr verbreitet, sind sie nun auch in europäischen Gefilden auf dem Vormarsch. Wie so viele Errungenschaften im World Wide Web wurde diese zu Beginn vornehmlich von Studenten und Technikern verwendet. Angefangen als Webtagebuch oder Netztagebuch - in welchem der Autor (aka. Blogger) seine tägliche Surftouren durchs Internet historisierte und mit persönlichen Informationen erweiterte - wurden die Webblogs immer mehr zu Kolumnen oder Newslettern. Die jeweiligen Verfasser wollten Ihre Erfahrungen, zum Beispiel dem Eindringen in ein Netzwerk, mit der ganzen Welt teilen und dadurch ein Mehr an Informationen durch die Leser und damit auch ein Mehr an Wissen erlangen. Unter IT-Fachkreisen sind einschlägige Blogs (Kurzform von Webblog) sehr beliebt und werden seit längerem regelmässig aufgesucht.

Bei der Präsentation der Ergebnisse eines durch uns durchgeführten Security Audit bei einer internationalen Bank mit schweizer Domizil kamen wir im anschliessenden Gespräch auf das Thema Webblog zu sprechen. Der Kunde teilte uns mit, dass das Mutterhaus aus dem asiatischen Raum Webblogs als Sicherheitsrisiko

einstuft. Die Frage stelle sich nun, wie und welche geeignete Massnahmen man unternehmen könne, um die Nutzung und Einsicht dieser zu verhindern.

Die Einstufung von Webblogs als Sicherheitsrisiko kann grundsätzlich nachvollzogen werden. Jeder effektive Angreifer oder beauftragte Sicherheitsfirma, wird bei einem Penetration Test in einem ersten Schritt ein Footprinting umsetzen. Dabei werden, vereinfacht ausgedrückt, sovielen Informationen über die Angriffsobjekte wie möglich zusammengetragen. Dadurch können beispielsweise Schwachstellen lokalisiert, ein Bild der Infrastruktur eruiert oder aber gezielte Social Engineering Attacks (in diese Kategorie gehört auch Phishing) vorbereitet werden. Lesen Sie dazu auch die ausgesuchten [Fachartikel](#) über [Phishing](#), [Google als Hacker-Tool](#) oder [Security Auditing](#).

Eine interessante Ausgangslage. Wie kann man verhindern, das jemand Informationen, zu welchen er Zugriffsberechtigt ist, ins weltweite Netz stellt? Wenn die Fragestellung so lautet ist meine Antwort schlicht: Es kann nicht verhindert werden! - Webblogs sind ein gutes Beispiel für das Versagen rein technischer Massnahmen. Grundsätzlich arbeiten Webblogs mit Standard Webzugriffen (z.B. HTTP POST-Anfragen auf ein PHP-Frontend). Dies bedeutet, dass wenn Sie Web zulassen, Sie auch Webblogs erlauben.

Klar könnten Sie Blacklist dedizierter Webblogs führen oder den Stream nach definierten Strings untersuchen lassen. Doch damit haben Sie sich ein neues Hobby zugelegt. Keine wirklich sinnvolle Lösung für Ihr Problem und vorallem nur ein halbes Pflaster auf eine Problemstellung, denn welche weiteren kommen wohl in Zukunft noch auf Sie zu? Wir können den Missbrauch von Informationen lediglich erschweren in dem wir ein Framework aus unterschiedlichen und



aufeinander abgestimmten Massnahmen definieren. Diese beginnen bei Zusätzen/Anhängen zu den Arbeitsverträgen, gehen über Verweise beim Aufrufen des Browser bezüglich Logging der Daten, dem Einbinden der Linienverantwortung als auch der technischen Sperrung des Hochladens von Dateien. IT-Security ist ein Prozess.

Wohlgemerkt der Einflussbereich begrenzt sich, in der Grosszahl der Fälle, auf die unter Ihrer Hoheit stehenden Infrastruktur. Nicht zu vergessen sind Fax, Telefon, Photokameras, Aufnahmegeräte usw. und natürlich das auswendig lernen von dedizierten Informationen... Schlussendlich ist ein Mass an Vertrauen, ohne Blindheit, in den Mitarbeiter angebracht, denn im Endeffekt arbeitet er ja für die Firma!

Es zeigt sich einmal mehr, dass Informationen das grösste Gut darstellen. Auch zeigt es sich wiederkehrend, dass mit der IT-Security Brille betrachtet, ein authentisierter Benutzer ein grosses Risiko darstellt. Technisch kann nicht verhindert werden, dass Photos von Bildschirmanzeigen durchgeführt oder Daten andersweitig gebraucht werden. Stellt sich einmal mehr die Frage wie man den Mitarbeiter in den Security Prozess integrieren kann. Sensibilisierungsschulungen (Awareness) sind ein Ansatz. Doch weiss ich aus eigener Erfahrung, dass auch „sensibilisierte“ Personen sich nicht immer daran halten. Vergessen wir nie, dass zur Einhaltung von Regeln immer an etwas gedacht werden muss und dieser Vorgang kostet Energie (denken Sie an die Physik und potenziellen Energie...), welche man nicht immer aufwenden möchte. Es gilt ein Framework aus unterschiedlichen Massnahmen aus differenten Einflussbereichen aufeinander abzustimmen und Sicherheit als Prozess zu verstehen.

Simon Zumstein <sizu-at-scip.ch>
Geschäftsleiter
Zürich, 17. Mai 2005

2. Neue Sicherheitslücken

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

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

Contents:

- 3.1 Netscape bis 7.2 Netscape Extension 2 GIF-Dateien Pufferüberlauf
- 3.2 Macromedia ColdFusion MX 7 HTTP 404 Fehlermeldung Dateiname Cross Site Scripting
- 3.3 F5 Networks 3-DNS Controller bis 4.6.2 login_radius schwache Authentisierung
- 3.4 F5 Networks BIG-IP bis 4.6.2 login_radius schwache Authentisierung
- 3.5 IBM WebSphere Application Server bis 6.0 HTTP 404 Fehlermeldung Dateiname Cross Site Scripting
- 3.6 Microsoft Windows XP bis SP2 grosse Bilder Denial of Service
- 3.7 F5 Networks BIG-IP bis 9.0.4 Cache fehlerhafte Authentisierung
- 3.8 Sun Java System Web Proxy Server bis 3.6 SP6 unbekannter Pufferüberlauf
- 3.9 Microsoft Windows 2000 Web View webvw.dll Web erweiterte Rechte

2.1 Netscape bis 7.2 Netscape Extension 2 GIF-Dateien Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 26.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1416>

Netscape Communicator ist ein relativ beliebter Webbrowser für die Windows- und UNIX-Betriebssysteme. Während des Aufkommens des Internets lieferten sich der Netscape Navigator und der Microsoft Internet Explorer ein Kopf an Kopf Rennen um die Herrschaft im World Wide Web. Mark Drowd der ISS X-Force hat einen schwerwiegenden Pufferüberlauf in der Netscape Extension 2 bei der Verarbeitung von GIF-Dateien entdeckt. Über diese kann ein Angreifer durch ein korruptes GIF-Bild beliebigen Programmcode auf dem Zielsystem ausführen lassen. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Als Workaround wird der Einsatz eines anderen Webbrowsers - zum Beispiel des aktuellen Mozilla Firefox - empfohlen.

Expertenmeinung:

In der Tat, das Mozilla-Projekt steht absolut in der Schusslinie, wenn es um neue Schwachstellen geht. Praktisch keine Woche vergeht, an der nicht irgendeine Sicherheitslücke in Firefox und co. Bekannt werden. Das Spiel wiederholt sich: Umso populärer eine Lösung wird, umso grösser ist das Interesse der Angreifer, sich mit den Schwachstellen dieser auseinanderzusetzen. Tragisch an dieser Geschichte ist jedoch, dass Mozilla angeblich explizit auf Sicherheit ausgelegt wurde und nicht die Fehler von Microsofts Webbrowser wiederholen will. Die Realität zeigt da jedoch etwas anderes. Mozilla ist halt nur ein weiteres Projekt, bei dem die Sicherheit zweitrangig ist - Ein Problem, das stets auf dem Rücken der Benutzer ausgetragen wird.

2.2 Macromedia ColdFusion MX 7 HTTP 404 Fehlermeldung Dateiname Cross Site Scripting

Einstufung: **kritisch**
Remote: Ja
Datum: 26.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1415>

ColdFusion MX ist ein kommerzieller, von der

Firma Macromedia entwickelter Applikations-Server für Unix, Linux und Windows. Dr_insane publizierte einen zuvor schon durch ihn in IBM WebSphere Application Server bis 6.0 entdeckten Fehler. Dort wird ebenfalls bei einer HTTP 404 Not Found Fehlermeldung standardmässig der Dateiname der nicht existierenden Ressource angezeigt. Ein Angreifer kann diese Übernahme der Daten für einen entsprechenden Angriff nutzen. Als Beispiel wird die simple URL `http://www.scip.ch/[script>alert('XSS');[/script].cfm` ausgewiesen. Als Workaround wird empfohlen, eine modifizierte 404 Fehlermeldung zu nutzen.

Expertenmeinung:

Cross Site Scripting Angriffe wie dieser werden gerne unterschätzt. Richtig angewendet können sie jedoch beachtlichen Schaden für die Betroffenen darstellen.

2.3 F5 Networks 3-DNS Controller bis 4.6.2 login_radius schwache Authentisierung

Einstufung: **kritisch**
Remote: Ja
Datum: 25.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1414>

F5 Networks ist Hersteller verschiedener Lösungen für high-end Load Balancing und Switching (vorwiegend auf Layer 7). Wie der Hersteller in seinem nur für Kunden zugänglichen Advisory meldet, existiert ein Designfehler in login_radius, das zur Umgehung gewisser Authentisierungen genutzt werden könne. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Fehler, der ebenfalls BIG-IP aus dem gleichen Haus betrifft, wurde in der Software-Version 4.6.3 behoben.

Expertenmeinung:

Schon der zweite Fehler diese Woche in einem F5 Networks Produkt. Spekulationen wird damit guter Nährboden gegeben: Wird das Produkt erst jetzt wirklich eingesetzt und dadurch auf Herz und Nieren geprüft? Oder ist das nur ein dummer Zufall, dass zwei Sicherheitsprobleme praktisch zur gleichen Zeit publik werden? Wie dem auch sei täte auch F5 Networks gut daran, sich auf ein solides Quality Management zu verlassen, denn in der Sicherheitsbranche werden Fehler nur selten verziehen.

2.4 F5 Networks BIG-IP bis 4.6.2 login_radius schwache

Authentisierung

Einstufung: **kritisch**
Remote: Ja
Datum: 25.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1413>

F5 Networks ist Hersteller verschiedener Lösungen für high-end Load Balancing und Switching (vorwiegend auf Layer 7). Das mitunter bekannteste Produkt ist BIG-IP, das eben diese Funktionalität für grössere Netzwerke zur Verfügung stellt. Wie der Hersteller in seinem nur für Kunden zugänglichen Advisory meldet, existiert ein Designfehler in login_radius, das zur Umgehung gewisser Authentisierungen genutzt werden könne. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Der Fehler, der ebenfalls den 3-DNS Controller aus dem gleichen Haus betrifft, wurde in der Software-Version 4.6.3 behoben.

Expertenmeinung:

Schon der zweite Fehler diese Woche in einem F5 Networks Produkt. Spekulationen wird damit guter Nährboden gegeben: Wird das Produkt erst jetzt wirklich eingesetzt und dadurch auf Herz und Nieren geprüft? Oder ist das nur ein dummer Zufall, dass zwei Sicherheitsprobleme praktisch zur gleichen Zeit publik werden? Wie dem auch sei täte auch F5 Networks gut daran, sich auf ein solides Quality Management zu verlassen, denn in der Sicherheitsbranche werden Fehler nur selten verziehen.

2.5 IBM WebSphere Application Server bis 6.0 HTTP 404 Fehlermeldung Dateiname Cross Site Scripting

Einstufung: **kritisch**
Remote: Ja
Datum: 25.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1412>

Die kommerzielle WebSphere Software von IBM ist eine universell einsatzfähige und schnelle Plattform für e-business on demand. Dr_insane entdeckte eine klassische Cross Site Scripting-Schwachstelle in IBM WebSphere Application Server bis 6.0. Dort wird bei einer HTTP 404 Not Found Fehlermeldung standardmässig der Dateiname der nicht existierenden Ressource angezeigt. Ein Angreifer kann diese Übernahme der Daten für einen entsprechenden Angriff nutzen. Als Workaround wird empfohlen, eine modifizierte 404 Fehlermeldung zu nutzen.

Expertenmeinung:

Cross Site Scripting Angriffe wie dieser werden gerne unterschätzt. Richtig angewendet können sie jedoch beachtlichen Schaden für die Betroffenen darstellen.

2.6 Microsoft Windows XP bis SP2 grosse Bilder Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 22.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1411>

Microsoft Windows XP stellt eine Weiterentwicklung des professionellen Windows 2000 dar. Andrew entdeckte, dass auf Microsoft Windows XP übergrosse Bilder beim Rendering eine Denial of Service hervorrufen können. Dies kann beispielsweise durch ein HTML-Dokument mit eingebettetem Bild umgesetzt werden. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler existiert auch auf Systemen mit installiertem Service Pack 2. Als Workaround wird empfohlen, keine Bilder unbekannter oder zweifelhafter Herkunft anzuzeigen, wenn zeitgleich kritische Applikationen ausgeführt werden. Es ist damit zu rechnen, dass Microsoft einen Patch für das Problem herausgeben wird.

Expertenmeinung:

Besonders kritisch ist dieses Problem, weil zur aktuellen Stunde nicht bekannt ist, ob es sich hierbei um einen produktiven ausnutzbaren Pufferüberlauf handelt. Ist dies der Fall, könnte gar beliebiger Programmcode ausgeführt werden - Eventuell gar mit System-Rechten. Es bleibt also abzuwarten, wie sich die Sache noch entwickelt wird und was Microsoft zu tun gedenkt.

2.7 F5 Networks BIG-IP bis 9.0.4 Cache fehlerhafte Authentisierung

Einstufung: **kritisch**
Remote: Ja
Datum: 21.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1409>

F5 Networks ist Hersteller verschiedener Lösungen für high-end Load Balancing und Switching (vorwiegend auf Layer 7). Das mitunter bekannteste Produkt ist BIG-IP, das eben diese Funktionalität für grössere Netzwerke zur Verfügung stellt. Wie der Hersteller in seinem nur für Kunden zugänglichen Advisory meldet, existiert ein Designfehler in der Konfigurationsmöglichkeit der Geräte bis 9.0.4.

Und zwar werden lange Passwörter in einem Cache abgelegt und bei einer späteren Authentisierung entsprechend nicht noch einmal überprüft. So ist es unter gewissen Umständen möglich, dass eine Authentisierung ohne gültiges Passwort umgesetzt werden kann. Der Fehler wurde in der Software-Version 9.0.5 behoben.

Expertenmeinung:

Ein wirklich unschöner Fehler, der bei keiner Software-Lösung passieren darf. Es bleibt zu hoffen, dass dies der letzte Fauxpas von F5 Networks bleibt, denn mit derlei Unschönheiten kann man sich den Ruf in einer aufmerksamen Branche schnell verderben.

2.8 Sun Java System Web Proxy Server bis 3.6 SP6 unbekannter Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 20.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1408>

Der Sun Java System Web Proxy (ehemals Sun ONE Web Proxy Server) ist eine kommerzielle Proxy-Lösung für Unternehmen. Wie der Hersteller in seinem Alert 57763 berichtet, existiert eine nicht näher beschriebene Pufferüberlauf-Schwachstelle in Sun Java System Web Proxy Server bis 3.6 SP 6. Ein Angreifer könne darüber Programmcode mit den Rechten des Servers ausführen. Technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Sun hat das Problem mit dem Service Pack 7 adressiert.

Expertenmeinung:

Da nahezu keine Details zur Schwachstelle bekannt sind, ist die Einschätzung sehr schwierig und zum jetzigen Zeitpunkt nicht möglich. Gerade deshalb bleibt Administratoren nichts anderes übrig, als schnellstmöglich die empfohlenen Gegenmassnahmen umzusetzen.

2.9 Microsoft Windows 2000 Web View webvw.dll Web erweiterte Rechte

Einstufung: **kritisch**
Remote: Ja
Datum: 19.04.2005
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1407>

Microsoft Windows 2000 - kurz auch W2k genannt - ist eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Es existieren Versionen für den Einsatz als

Server und solche für den Workstation-Betrieb. GreyMagic entdeckte einen Designfehler in der Bibliothek webvw.dll, die für das Anzeigen von Detailinformationen zu Dateien im Explorer gebraucht wird. Dabei wird beispielsweise der Name des Autors untersucht, ob dieser als Mailadresse identifiziert werden kann. Falls ja, wird die Information in einen anklickbaren mailto-Link umgewandelt. Diese Umwandlung überprüft die Eingaben nicht korrekt, so dass eine Script Injection umgesetzt werden kann. Alleine mit dem Anzeigen einer Datei in dieser Vorschau kann beliebiger Programmcode ausgeführt und erweiterte Rechte erlangt werden. Im Advisory ist ein Beispiel zur Umsetzung eines solchen Zugriffs sowie ein Link zu einem Beispiel-Exploit enthalten. Betroffen von der Schwachstelle ist nur die Windows 2000-Reihe. Als Lösung wird entsprechend der Wechsel zu einer anderen Betriebssystem-Version oder das Deaktivieren der Vorschau-Funktion empfohlen. Letzteres kann mit der Umstellung auf "Use Windows classic folders" in den Ordner-Optionen umgesetzt werden. Microsoft hat rund zwei Wochen später einen Patch zum Download bereitgestellt.

Expertenmeinung:

Grundsätzlich ein Designfehler, der bei den älteren Windows-Betriebssystemen nicht zum Tragen gekommen ist. Trotzdem ist es verwunderlich, dass diese Schwachstelle erst jetzt, viele Jahre nach der Einführung von Microsoft Windows 2000 und XP, bekannt geworden ist.

3. Kreuzworträtsel

Datendefinitionssprache (in SQL)	Linux: Löscht den Bildschirm	Wonach sucht Wellenreiter		Kopf von Microsoft	Grafische Bedienoberfläche	Wagennüklaut		Analog-Digital-Wandler	Virtual Private Network
		Freeware Security scanner	1					Linux: Kopiert Dateien	
Backup Domain Controller		DOS: Kommando für Attributänderung					optische Platte		
Port-scanner	Wer entwickelte die Flash	Verschlüsselungssoftware		Hinzufügen funktionaler Anforderungen	DOS: Zeigt die Uhrzeit an	Vorgänger von Windows 2000		Top-Level-Domain von Schweden	
		3	Projekt Suche ausserirdischem Leben				Javascript		
DOS: Vergleicht den Inhalt von Dateien			Prozedur aufruf auf entferntem Rechner	Programmiersprache (Handel, Banken)		Data Encryption Standard		scip monthly Security Summary	
		UNIX: Kommando equivalent zu dir unter DOS				Autor von "Applied Cryptography"		Systemüberprüfung ob Software erworben	
		UNIX: Speicherplatz jedes Verzeichnis	2					DOS: Kopiert Dateien	
Abgelaufene oder zurückgegebene Zertifikate					Briefqualität	Denial of Service		Seitenbeschreibungssprache des WWW	4
		Zeilenvorschub	Computer Online Adventure		6				
Bedienoberfläche für OS/2		Linux: Sucht Zeichenfolge in einer Datei							
Klassischer UNIX-Texteditor			Dateisystem von Windows 9x	Wo sind Konfigurationsdateien unter UNIX	5				
		UNIX: Verschieben einer Datei							
Private Person TLD									

Wettbewerb

Mailen Sie uns das erarbeitete Schlüsselwort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten. Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.06.2005**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

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

SECURITYTRACKER



4. Impressum

Herausgeber:

scip AG

Technoparkstrasse 1

CH-8005 Zürich

T +41 1 445 1818

<mailto:info@scip.ch>

<http://www.scip.ch>

Zuständige Person:

Marc Ruef

Security Consultant

T +41 1 445 1812

<mailto:maru@scip.ch>

PGP:

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

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

Nutzen Sie unsere Dienstleistungen!

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

Das [Errata](#) (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online.

Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)