secorvo
security consulting

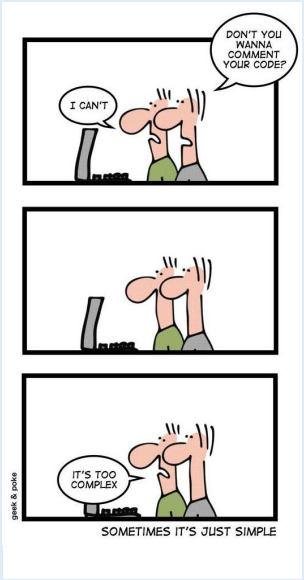
Secorvo Security News

Mai 2012

Die Geister, die ich rief...

Der Umgang mit unkontrollierter Komplexität wurde schon Goethes Zauberlehrling zum Verhängnis. Zunächst verlief alles nach Wunsch des Protagonisten: Er verschaffte sich durch Nutzung eines Reinigungstools eine Arbeitserleichterung. Leider wies dieses einige Schwachstellen auf und ließ sich durch den Lehrling nicht mehr kontrollieren – da wuchs dem Armen die Unbeherrschbarkeit seines Setups über den Kopf: "*Die ich rief, die Geister, werd ich nun nicht los.*"

Moderne Software-Entwicklung weist erschreckend viele Parallelen zu Goethes Lehrling auf. So verlässt sich heute die Mehrheit der Anwendungen auf externe Bibliotheken und Frameworks. Der eigene Code dient häufig nur noch der abstrakten Orchestrierung von wie durch Zauberhand bereit gestellter Funktionalität. Das tiefere Verständnis der genutzten Werkzeuge geht dabei verloren. Gerade die Sicherheit des Endprodukts aber hängt wesentlich von der Sicherheit der verwendeten Bibliotheken ab – und um die ist es nicht besonders gut bestellt: Aspect Security fand im März 2012 in jeder vierten Bibliothek bekannte Sicherheitsbugs. Der geregelte Umgang mit der Komplexität externer Komponenten muss zumindest die Kontrolle der genutzten Werkzeuge und den Überblick über Schwachstellen gewährleisten.



Der Weg zur Meisterschaft ist steinig. Aber nur die erlaubt den erlösenden Ruf: "*In die Ecke, Besen! Besen! Seids gewesen!*"

Inhalt

secorvo
security consulting

Security News

Puls des Internet

Das SSL Observatory der Electronic Frontier Foundation (vgl. SSN 12/2010 und 02/2012) widmet sich den SSL-Zertifikaten in „freier Wildbahn" samt den ausstellenden Trust Centern. Eine gute Ergänzung bietet SSL Pulse, eine am 25.04.2012 publizierte Statistik über die Sicherheit von SSL-Websites, bei der unter anderem die Konfiguration der angebotenen SSL/TLS-Protokollversionen und Cipher Suites geprüft wurde. In diese Übersicht flossen die Ergebnisse von ca. 200.000 SSL Server Tests der Qualys SSL Labs ein.

Beunruhigendes Ergebnis: ca. drei Viertel aller Sites sind anfällig gegen die im September 2011 publizierte BEAST Attacke, die es einem Angreifer unter bestimmten Umständen ermöglicht, SSL/TLS-geschützte Passwörter oder Cookies zu ermitteln. Die technische Analyse verrät naturgemäß nicht, ob die betroffenen Serverbetreiber diese Bedrohung als zu gering bewerten, um die mit einem Update oder Einschränkungen verbundenen Gegenmaßnahmen zu ergreifen, oder ob sie die Attacke schlicht nicht kennen. Betreibern öffentlicher SSL/TLS-Server ist jedenfalls sehr zu empfehlen, den eigenen Server dem (kostenfreien) SSL Server Test zu unterziehen – und sei es nur als Rückversicherung, dass die beabsichtigte Konfiguration korrekt umgesetzt ist – bevor andere feststellen, dass der Server doch nicht zum letzten Viertel zählt.

Warnung vor Hotspots

Am 08.05.2012 warnte das Internet Crime Complaint Center (IC3) des FBI, dass Laptops, die sich in öffentliche (Hotel-) WLANs einbuchen, eine Verseuchung durch Malware befürchten müssen. Diese Warnung reiht sich ein in ähnliche Hinweise auf versteckte Manipulationen von Betreibern öffentlicher Hotspots – und kann Techniker erstmal nicht überraschen.

Mit zunehmender Moblilität steigt jedoch die Gefahr, dass Nutzer öffentlichen Hotspots blind vertrauen. Verlässlichen Schutz bietet die Nutzung des VPN-Zugangs der eigenen Firma oder ein vertrauenswürdiges „Personal VPN". Mindestens aber sollte eine „Personal Firewall" Zugriffe von außen abblocken und jeder mobile Nutzer sicher stellen, dass er nicht über ungesicherte Verbindungen auf kritische Dienste zugreift oder vertrauliche Informationen übermittelt.

Vertrauenswürdiges Internet

Am 10.05.2012 kündigte die NCC Group an, das verlorene Vertrauen in das Internet durch die Schaffung einer neuen Top-Level-Domäne (TLD) *.secure* wieder zurück zu gewinnen. Zuteilungen für Domänen unterhalb der neuen TLD sollen nur Betreiber erhalten, die Mindestsicherheitsstandards für ihre Systeme vorweisen können.

Details hierzu werden zur Zeit abgestimmt. Es ist aber bereits bekannt, dass die durchgängige Verwendung von SSL/TLS für Webseiten, die Absicherung von DNS mit DNSSEC und die Verwendung von DKIM für E-Mails gefordert werden. Auf der FAQ-Seite wird angekündigt, dass die Dokumente von Antragstellern durch den Betreiber Artemis überprüft werden.

Aufschlussreich ist der Abschnitt über die Kosten einer *.secure*-Domäne: "*.SECURE domains provide premium value to registrants and their customers an will be priced accordingly.*" Die Erfindung einer Gelddruckmaschine? Auch wenn bereits begründete Zweifel am tatsächlichen Sicherheitsgewinn laut werden, ist eines definitiv sicher: Die indische Regierung wird mit ihrer Domäne kaum glücklich werden: https://in.secure

Neues TK-Recht

Am 04.05.2012 ist das Gesetz zur Änderung telekommunikationsrechtlicher Regelungen in Kraft getreten. Ziel des Gesetzes ist die Stärkung der Verbraucherrechte. Für die Nutzung von Standortdaten der Nutzer wurde in § 98 Abs. 1 TKG eine neue Informationspflicht eingeführt: Der Gerätenutzer – nicht der Anschlussinhaber – muss bei jeder Standortermittlung hierüber per Textmitteilung in Kenntnis gesetzt werden.

Wird der Schutz personenbezogener Daten verletzt, sind neben der BNetzA der Bundesdatenschutzbeauftragte, in schwer wiegenden Fällen die Betroffenen zu informieren. § 109a Abs. 3 TKG verpflichtet die Anbieter ein Verzeichnis über Datenschutzverletzungen zu führen. Die hierdurch entstehende Pflicht zur Selbstanzeige soll durch Verweis auf das Verwertungsverbot in § 42a Satz 6 BDSG rechtsstaatlich entschärft werden.

Die Verpflichtung zur Erstellung und Vorlage eines Sicherheitskonzepts (§ 109 TKG) wurde ausgedehnt auf die Anbieter von Telekommunikationsdiensten. Außerdem wurde entsprechend § 42a BDSG eine Meldepflicht bei Sicherheitsverletzungen in § 109 Abs. 5 und § 109a TKG eingeführt. Die Bundesnetzagentur kann daraufhin den Betreiber oder Dienstanbieter zu einem ausführlichen Bericht verpflichten. Außerdem kann sie nach Abs. 7 dem Betreiber oder Dienstanbieter eine Auditierung auferlegen.

Mit dem Änderungsgesetz zielt der Gesetzgeber darauf, den Datenschutz durch Transparenzpflichten zu stärken. Zwar ist dies zu begrüßen, allerdings muss befürchtet werden, dass gehäufte Transparenz irgendwann zu Abstumpfung der Adressaten führt und damit ihre Wirkung verlieren wird.

Nmap 6

Pünktlich zum nahenden World IPv6 Day hat Gordon „Fyodor" Lion am 21.05.2012 ein neues Release des Portscanners Nmap herausgebracht – passenderweise mit Versionsnummer 6. Eines der Hauptfeatures besteht denn auch in voller IPv6-Unterstützung. Neben den „üblichen" Verbesserungen (schnellere Scan-Engine, mehr und ausgefeiltere Skripte) zeichnet sich ab, dass die Grenzen zwischen Portscanner und Schwachstellenscanner immer mehr verwischen: auch das neue Release von Nmap setzt seinen Vormarsch in Richtung Webanwendungsscanner fort.

Mit dem Einsatz von IPv6 müssen sich Administratoren und Pentester von der beliebten Praxis verabschieden, ein Subnetz nach laufenden Diensten zu durchscannen – das verbietet die schiere Größe des Adressraums von IPv6-Subnetzen. Alternative Ansätze zum Auffinden von Hosts sind beispielsweise in RFC 5157 beschrieben.

Ein Tool, das dabei nützlich werden könnte, ist das neue Nping, das zur Familie der Nmap-Tools hinzugekommen ist; dessen IPv6-Unterstützung ist aber derzeit noch als „experimental" eingestuft.

Einer der Zukunftspläne für Nmap sieht vor, neue NSE-Scripte und OS-Fingerprints über einen Update-Service bereit zu stellen. Aber auch so bleibt Nmap in absehbarer Zukunft eines der wichtigeren Test-Tools für Admins und Pentester.

Neuer Ripper

Seit dem 06.05.2012 steht Version 2.5 des forensischen Werkzeugs RegRipper für Windows zur Verfügung. Bisherige Plugins funktionieren nicht nur weiterhin; mit ihnen können nun die Metadaten einzelner Dateien wie z. B. Benutzerprofilen (NTUSER.DATs) oder Dateigruppen wie Verknüpfungen (*.LNKs) direkt aus den schreibgeschützten Volume Shadow Copies (VSC) abgefragt werden. Dadurch kann auf das fehleranfällige Kopieren von Dateien aus VSCs verzichtet werden. Mit Unterstützung des neuen Dateisystems ReFS ist RegRipper bereits für Windows 8 gerüstet.

Secorvo News

Seminare für alle

Sie haben Verstärkung im Team bekommen? Herzlichen Glückwunsch! Als Steilkurs für die neue Kollegin oder den neuen Kollegen empfehlen wir unser Seminarpaket aus "Sicherheitsmanagement heute" und "IT-Sicherheit heute". Und falls an Ihrer Bürowand noch kein T.I.S.P.-Zertifikat prangen sollte: Das nächste Zertifizierungsseminar bieten wir vom **17.–21.09.2012**. Das T.I.S.P.-Buch erhalten Sie mit der Anmeldung vorab – als erbauliche Urlaubslektüre. Weitere Seminarangebote und die Möglichkeit zur Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

4. Tag der IT-Sicherheit

Gemeinsam mit der IHK Karlsruhe, dem Cyber-Forum e.V. und KASTEL veranstaltet die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **12.07.2012** bereits zum vierten Mal den "Tag der IT-Sicherheit". Die Veranstaltung beginnt um 14.00 Uhr im Saal Baden der IHK Karlsruhe. Auch in diesem Jahr erwartet Sie wieder ein spannendes Vortragsprogramm. Ausgewiesene Experten stellen den Stand der Entwicklung bei Hackerangriffen („Live Hacking") und Schutzstrategien in Theorie und Unternehmenspraxis vor. Gelegenheit zum fachlichen und persönlichen Austausch mit Referenten, Teilnehmern und Ausstellern bietet die „Networking-Pause".

Nach der positiven Ressonanz der vergangenen Jahre rechnen wir mit zahlreichen Teilnehmern und empfehlen daher eine frühzeitige Anmeldung. Wir freuen uns auf Ihre Teilnahme!

Sicher – sicherer – Android?

Besitzern von Smartphones bietet sich eine reiche, ständig größer werdende Auswahl von Apps. Aber wie sicher ist eine Mobile-Banking-App, wenn das neueste Tablet-Spiel "unerwünschte Nebenwirkungen" hat? Wie gut können sensitive Daten in Unternehmens-Apps geschützt werden, wenn die Smartphone-Besitzer daneben so viele Apps eigener Wahl installieren, wie der Speicher hergibt?

Mit diesen und anderen Fragen setzt sich Hans-Joachim Knobloch (Secorvo) beim nächsten KA-IT-Si Event am **21.06.2012** auseinander. Sein Vortrag "Apps - tickende Bomben im Bauch des Androiden?" gibt einen Überblick über die Sicherheitsarchitektur von Android, beleuchtet verschiedene Bedrohungsszenarien und stellt Mechanismen sowie Konzepte zur sicheren Gestaltung von Android-Apps vor.

Beginn der Veranstaltung ist um 18.00 Uhr im Panoramasaal der IHK Karlsruhe. Um Anmeldung wird gebeten.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juni 2012	
18.-19.06.	DuD 2012 (Computas, Berlin)
19.-21.06.	Forensik (Secorvo College, Karlsruhe)
21.06.	Sicher – sicherer – Android? (KA-IT-Si, Karlsruhe)
Juli 2012	
12.07.	4. Tag der IT-Sicherheit (IHK, CyberForum, KASTEL, KA-IT-Si, Karlsruhe)
21.-26.07.	Blackhat USA 2012 (Las Vegas/US)
26.-29.07.	DEFCON 20 (Las Vegas/US)
August 2012	
06.-08.08.	DFRWS 2012 (DFRWS, Washington/US)
08.-10.08.	21th USENIX Security Symposium (Usenix, Bellevue/US)
19.-23.08.	Crypto 2012 (IACR, Santa Barbara/US)
20.-24.08.	SecSE 2012 (SINTEF, Prag/CZ)
27.08.	Sommerakademie 2012 (ULD Schleswig-Holstein, Kiel)

Fundsache

Kaum zu glauben: Die schier unausrottbare SQL-Injection – der „Buffer-Overflow der Web-Applikationen" – wird 2012 bereits 14 Jahre alt. Die Erstveröffentlichung erschien 1998 in Heft 54 des Phrack Magazine (Volume 8).

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox, Safuat Hamdy, Kai Jendrian (Editorial), Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting. Abdruck des Cartoons mit freundlicher Genehmigung von geek & poke.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news"). Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Alle Texte sind urheberrechtlich geschützt. Jede unentgeltliche Verbreitung des unveränderten und vollständigen Dokuments ist zulässig. Eine Verwendung von Textauszügen ist nur bei vollständiger Quellenangabe zulässig.