secorvo
security consulting

Secorvo Security News

September 2008

Editorial: Verhältnisunmäßig

Große Erregung: Millionen Kontendaten, für kleines Geld zu erwerben, bieten fette Beute für Betrüger, die Banken glaubhaft versichern, im Besitz von Einzugsermächtigungen zu sein. Verbraucherschützer trommeln, die Republik ist empört, und der Bundesinnenminister gipfelt.

Die richtige Aufregung, aber zum falschen Anlass. Seit 1998 wertet Google täglich Milliarden Suchanfragen zur Erstellung und Verfeinerung von Abfrageprofilen aus. Zähneknirschend hat Google am 08.09.2008 auf Druck der Artikel-29-Gruppe den europäischen Datenschutzbeauftragten angekündigt, „damit zu beginnen", die IP-Adressen in den Such-Logs schon (sic!) nach neun Monaten zu anonymisieren. Sechs Tage zuvor hatte Google seinen neuen Browser Chrome publiziert. Welch Koinzidenz. Millionenfach heruntergeladen, erlaubt Chrome die Verknüpfung von Suchanfragen mit Webseitenaufrufen – und einer eindeutigen Browser-ID. Abgleiche der Suchprofile mit den Webseiten von Social Networks, Personensuchmaschinen wie 123people oder yasni, den Adressangaben in Telefonbüchern oder Nachbarbeschimpfungen liefern Google (und z.T. auch dessen Nutzern) von immer mehr Menschen ein Persönlichkeitsprofil. Von da zum Großen Bruder ist es nur noch einen klitzekleiner Klick. Wer braucht da noch die sechsmonatige Vorratsdatenspeicherung?

Immerhin regt sich inzwischen etwas im Innenministerium. Sogar in die seit sieben Jahren überfällige Verabschiedung eines Datenschutz-Audit-Gesetzes, an die kein Datenschützer mehr zu Glauben wagte, kommt Bewegung. Allerdings lassen einige der Gipfelergebnisse eher operative Hektik befürchten: Durch die Abschaffung des Listenprivilegs würde keine einzige Kontonummer gerettet, und ein Kopplungsverbot wiese Google nicht in die Schranken.

„Wer weiß, wie Gesetze und Würste zu Stande kommen, kann nachts nicht mehr gut schlafen", soll Otto von Bismarck gesagt haben. Den meisten Metzgern würde er heute damit Unrecht tun.

Inhalt

Security News

WASC Studie

Am 08.09.2008 hat das Web Appliction Security Consortium (WASC) die Ergebnisse des Projekts „Web Application Security Statistics 2007" veröffentlicht. Im Rahmen dieser Studie wurden zum besseren Verständnis der Sicherheitslage bei Web-Anwendungen über 32.000 Sites automatisiert und manuell untersucht. Die im Detail vorgestellten Ergebnisse sind aufschlussreich und erschreckend zugleich: Wenn auch nur knapp über 7% der untersuchten Anwendungen automatisiert kompromittiert werden konnten, wurden in über 96% der Anwendungen bei manueller Suche schwerwiegende Schwachstellen gefunden. Insbesondere handelte es sich um Anfälligkeiten für Cross-Site-Scripting, Information Leakage, SQL-Injection und Predictable Resource Location.

Als Basis diente die WASC Threat Classification 1.0 aus dem Jahr 2005. Trotz der etwas betagteren Grundlage bietet die Studie eine umfassende Analyse der benutzten Methoden und erzielten Ergebnisse. In diesem Zusammenhang triff es sich gut, dass am 15.09.2008 der Aufruf zur Mitarbeit an der Weiterentwicklung zur WASC Threat Classification 2.0 erfolgte. Allen an Web-Sicherheit Interessierten legen wir die Beobachtung dieser Entwicklung sehr ans Herz.

Nmap auswerten

Am 07.09.2008 ist der Netzwerkscanner Nmap in Version 4.75 erschienen. Darin wurde das GUI Zenmap um die Visualisierungskomponente Radialnet erweitert. Zwei sehr sinnvolle Funktionen – Datenaggregation mehrerer Scans und eine Netztopologiedarstellung – stehen nun zur Verfügung, sofern die Scan-Ergebnisse im XML-Format vorliegen.

Dies vereinfacht die Analyse der Scanergebnisse erheblich, da zeitlich auseinanderliegende Scans in einer Auswertung darstellbar sind – der Praktiker weiß: Nicht immer sind alle Hosts online oder dürfen im selben Arbeitsablauf gescannt werden. Erfreulicherweise funktioniert die Aggregation auch mit älteren XML-Dateien des 4.60-Releases. Die Topologie des Netzwerks ist konzentrisch und mit relativer Hopdistanz darstellbar, inklusive Ergebnisdetails für gescannte IPs. Ein übersichtlicher Netzplan als Nebenprodukt eines Audits ist ein erheblicher Mehrwert. Ein Wermutstropfen bleibt: Für umfangreiche IP-Ranges braucht man viel CPU-Zeit – und scharfe Augen.

Rootkit für Jedermann

Am 03.09.2008 wurde das voll funktionsfähige Open Source Rootkit „Debug Register" (DR) in der Version 0.1 für Linux-Kernels 2.6.x (Intel-IA32-Architekturen) vom Penetrationstest-Werkzeughersteller Immunity Inc. zum Download veröffentlicht. Seine Funktionen umfassen die Unterstützung für versteckte Prozesse, Netzwerksockets, Daten sowie eine Backdoor.

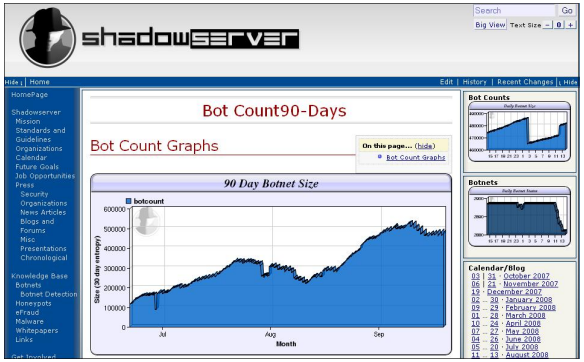
Das Rootkit arbeitet wie ein Kernel-Debugger und nutzt vorhandene System-Interrupts der Intel-CPUs – eine Technik, die bisher von Malware kaum eingesetzt wurde, da dafür ein tiefes Systemverständnis erforderlich ist. Mit einem Entwicklungsaufwand von ca. zwei Wochen lässt sich der Code um eine Tarnung auf Kernel-Ebene erweitern.

Damit wurde die Entwicklung leistungsfähiger Malware im Linux-Umfeld erheblich beschleunigt. Ohne einen wirksamen Integritätsschutz der Systemumgebung ist gegen derartige Low-Level-Angriffe kein Kraut gewachsen.

Botnetz-Wachstum

Die 2004 gegründete Shadowserver Foundation hat sich zur Aufgabe gemacht, die „dunklen Seiten des Internet" zu beleuchten. Von Sicherheitsspezialisten werden die Entwicklungen bei Viren und Malware sowie von Botnetzen beobachtet; Ergebnisse und weitere Informationen werden auf den Webseiten der Initiative veröffentlicht.

Dabei wurde in den vergangenen drei Monaten ein sprunghaftes Wachstum von Botnetzen beobachtet: Die geschätzte Anzahl der übernommenen Systeme hat sich fast vervierfacht. Ursache hierfür dürften unter anderem Malware-Mailings anlässlich der Olympiade sein. Auch wurden PCs verstärkt über kompromittierte Webserver infiziert.



Die Entwicklung zeigt, dass es weiterer technischer und organisatorischer Maßnahmen bedarf, um Client-Systeme adäquat zu schützen. Nutzern empfehlen wir die Beachtung entsprechender Warnungen, beispielsweise unter www.bsi-fuer-buerger.de.

Endlich DNSSEC?

Die Schwächen des Internet Domain Name Systems (DNS), die bei den unlängst veröffentlichten Cache Poisoning Attacken (siehe SSN 07/08) zu Tage traten, kommen nicht überraschend. Bereits im Januar 1997 wurde in RFC 2065 die erste Version der DNS Security Extensions (DNSSEC) veröffentlicht. Nach zwei Überarbeitungen ist DNSSEC seit März 2005 in den RFCs 4033 ff. spezifiziert und in verbreiteter DNS-Software, z. B. BIND, integriert – kann also nach Internet-Zeitmaßstäben als ausgereift gelten.

DNSSEC nutzt elektronische Signaturen zur Sicherung der erteilten Auskünfte. Die dabei benötigte PKI wird jedoch nicht wie üblich über X.509-Zertifikate realisiert; statt dessen erteilen Nameserver direkt Auskunft über die Public Keys der Nameserver darunter liegender Ebenen. Hierin liegt auch einer der Gründe, dass DNSSEC trotz langer Vorlaufzeit noch nicht global eingesetzt wird: Genau so umstritten wie die Kontrolle über die Root-Nameserver ist auch die politische Frage, wer deren Schlüsselpaar als „Trust Anchor" des Internet kontrollieren soll.

Mit Erlass vom 22.08.2008 ordnete die US-Regierung – kaum zufällig zeitgleich mit den jüngsten DNS-Attacken – für die von ihr kontrollierte Government Top-Level Domain („gov") die flächendeckende Einführung von DNSSEC bis Ende 2009 an. Die einschlägigen Umsetzungsempfehlungen der NIST Special Publication 800-81 sind für jeden DNS-Verantwortlichen einen Blick wert.

Ein Multiplikator-Effekt könnte sich einstellen, wenn Service-Provider, die für einzelne Behörden deren .gov-Domains hosten, ihre Insfrastruktur fit für DNSSEC machen müssen und diesen Zusatz-Dienst dann auch anderen Kunden anbieten.

Datenschutz-Bußen

Weder die öffentliche Zerknirschung noch der Rückgriff auf den ehemaligen Bundesdatenschutzbeauftragten Jakob haben Lidl geholfen: Am 11.09.2008 verkündeten die Datenschutzaufsichtsbehörden die Verhängung von Bußgeldern in einer Gesamthöhe von knapp 1,5 Mio. Euro, nachdem Lidl seine Mitarbeiter in persönlichkeitsverletzender Weise hatte ausspionieren lassen. Eigenwillige Interpretationen von Arbeitnehmerrechten hatten bereits 2004 zur Verleihung des BigBrotherAward geführt.

Dass es sich beim persönlichkeitsverletzenden Einsatz von Videoüberwachung nicht um ein Kavaliersdelikt handelt, wird auch durch das am 15.09.2008 von der nordrhein-westfälischen Aufsichtsbehörde gegen den Fleischverarbeiter Tönnies verhängte Bußgeld in Höhe von 80.000 Euro bekräftigt. Zur Diebstahlsvorbeugung wurden die Beschäftigten mit über 200 Kameras unter anderem auch in Umkleidekabinen und Sozialräumen überwacht.

Eine gesetzeskonforme Gestaltung der Verarbeitung personenbezogener Daten gebietet inzwischen auch die ökonomische Vernunft. Die Zeiten, in denen sich Datenschutzverstöße aussitzen ließen, sind vorbei.

Secorvo News

Secorvo College aktuell

Pünktlich zu den in Karlsruhe gelegentlich auch im Spätsommer noch südländischen Temperaturen lockt Secorvo College nun mit klimatisierten Räumen. Das scheint sich schnell herumgesprochen zu haben, denn mehrere Seminare waren schon kurz nach dem Ende der Urlaubszeit ausgebucht.

Noch freie Plätze gibt es für die Seminare IT-Sicherheit heute (**07.–10.10.**), IT-Sicherheitsaudits (**28.–30.10.**), Security Awareness (**04.–05.11.**) und das T.I.S.P.-Seminar (**24.–28.11.**).

Programm und Online-Anmeldung unter http://www.secorvo.de/college

Für das Seminar Forensik, das sich ganz besonderer Nachfrage erfreut, haben wir eine Warteliste eingerichtet. Voraussichtlich im Januar 2009 wird es einen zusätzlichen Termin geben. Bitte wenden Sie sich bei Interesse an college@secorvo.de.

Gut gemeint

„Das Gegenteil von gut ist nicht böse, sondern gut gemeint." Das gilt leider auch für verbreitete Passwort-Policies, wie Thomas Maus in seinem Vortrag im Rahmen der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am 25.09.2008 (18 Uhr im Schlosshotel Karlsruhe) zeigen wird. Dabei räumt er mit vielen lieb gewonnenen und, wie das obige Zitat von Gottfried Benn, gerne kopierten „Wahrheiten" auf. Im Anschluss an den Vortrag gibt es, wie gewohnt, Gelegenheit zum Buffet-Networking. Um Anmeldung wird gebeten.

Jubiläums-Nachlese

Für die zahlreichen Glückwünsche, die uns zu unserem 10jährigen Firmenjubiläum erreicht haben, bedanken wir uns auch an dieser Stelle sehr herzlich. Auch die vielen „Geburtstagslob"-E-Mails zu unseren News haben uns sehr gefreut – wir bleiben am Ball, versprochen. Mit den Vorbereitungen für den 20sten Jahrestag haben wir auch schon begonnen.

Veranstaltungshinweise

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

September 2008	
25.09.	Das Gegenteil von gut ist - gut gemeint (KA-IT-Si)
Oktober 2008	
07.-10.10.	IT-Sicherheit heute (Secorvo College)
07.-09.10.	ISSE (TeleTrust), Madrid/ES
27.-30.10.	Hack-in-the-Box 2008, Kuala Lumpur/MY
28.-30.10.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
November 2008	
04.-05.11.	Security Awareness - Methoden, Konzepte, Best Practice (Secorvo College)
11.-13.11.	Forensik – Verfahren, Tools, Praxis (Secorvo College)
18.-21.11.	Information Security Management (Secorvo College)
24.-28.11.	T.I.S.P.-Schulung (Secorvo College)
Dezember 2008	
02.-04.12.	Sichere Softwareentwicklung (Secorvo College)

Fundsache

Bei der Betätigung des „Home Buttons“ eines iPhones schrumpft die aktuell offene Anwendung und blendet sich aus. Dieser optische Effekt wird im iPhone durch das Erstellen von Bildschirmfotos realisiert – SubSeven lässt grüßen. Das iPhone löscht ältere Fotos zwar, aber bei einer forensischen Untersuchung des iPhones treten diese Spuren offenbar wieder hervor. Ein Feature für die Strafverfolgung – oder ein Westentaschenspion?

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Karin Schuler, Hans-Joachim Knobloch, Jochen Schlichting

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