secorvo
security consulting

Secorvo Security News

September 2009

Profilvertrieb

Die hohe Kunst des Vertriebs beginnt lange vor der Kontaktaufnahme mit potentiellen Kunden. Ein gutes Produkt, gute Argumente und ein überzeugungsstarker Vertrieb allein garantieren keinen Verkaufserfolg: Entscheidend sind die „Streuverluste" bei der Auswahl der Kontakte. Daher ist das Bemühen verständlich, die Selektion durch das Sammeln von Informationen zu schärfen. Besonders viel versprechend sind echte Interessenten – Menschen mit Bedarf, die sich bereits über das Angebot informiert haben.

Da bietet der eigene Internetauftritt gänzlich neue Möglichkeiten. Webseiten-Optimierungstools wie Google Analytics haben den Appetit geweckt: Welche Seiten hat ein Nutzer besucht? Hat er eine Demo-Software, ein Datenblatt oder eine Leistungsbeschreibung heruntergeladen? Wie viel Zeit hat er auf der Seite verbracht?

Wie schön wäre es, aus der IP-Adresse auf die Identität des Besuchers schließen und ihn unmittelbar kontaktieren zu können! Oft ist das nicht schwierig: Hat er einmal ein Kontaktformular ausgefüllt, können Name und Anschrift im CRM mit der IP-Adresse verknüpft werden – und jeder weitere Besuch lässt sich zuordnen. Kostenlose Angebote wie utrace oder infosniper liefern auf Knopfdruck Provider und Domaininhaber, kommerzielle Anbieter ordnen IP-Adressen recherchierte Namen zu. Und wäre es vor einem Anruf nicht gut zu wissen, bei welchem Wettbewerber der Besucher sich vorher informiert hat und welches Bildungsniveau und Interessenprofil aus dem Surfverhalten abgeleitet werden können?

Tatsächlich ist die Erstellung von Surf-Profilen ohne Einwilligung des Betroffenen verboten (§ 12 Telemediengesetz). Ein Passus in der Datenschutzerklärung, der eine implizite Einwilligung bei Nutzung annimmt, genügt § 13 (2) TMG nicht. Verstöße sind jedoch verbreitet, wie das Xamit-Datenschutzbarometer vom 30.06.2009 belegt. Wer sicher gehen will, prüft eine Webseite vorher – vielleicht auch einmal die des eigenen Arbeitgebers...

Inhalt

secorvo
security consulting

Security News

Playstation-Cracker

Am 08.07.2009 gelang es der Forschungsgruppe um Arjen Lenstra an der École Polytechnique Fédérale de Lausanne, nach knapp sechs Monaten einen diskreten Logarithmus auf einer elliptischen Kurve über einem endlichen Primkörper von 112 bit zu lösen – mit anderen Worten: den privaten Schlüssel eines asymmetrischen Kryptosystems auf einer elliptischen Kurve der Moduluslänge 112 bit zu bestimmen. Ein neuer Rekord. Zuletzt war im Oktober 2002 die Berechnung eines diskreten Logarithmus auf einer elliptischen Kurve über einem 109 bit großen endlichen Körper gelungen (SSN 1/2003).

Nicht nur die verwendeten „Rechenknechte" sind ungewöhnlich – Lenstra parallelisierte die Berechnung in einem Cluster von über 200 Playstations. Auch die Implikationen sind erheblich, wie Lenstra gemeinsam mit Peter Montgomery, einem weiteren Schwergewicht der Faktorisierungsforschung, in einer IACR-Online-Veröffentlichung vom 01.09.2009 darlegt: Anders als in der berühmten Schlüssellängen-Prognose, die Lenstra 1999 mit Verheul publizierte, kommen die Autoren zu dem Schluss, dass mit der Faktorisierung einer 1024 bit langen Zahl kaum vor 2020 zu rechnen sei; die erste Faktorisierung eines 768 bit langen RSA-Modulus erwarten sie für das kommende Jahr. Diese Einschätzung deckt sich mit einer Prognose von Secorvo aus dem Jahr 2001 (SSN 5/2004).

Durchbruch: 15 = 3*5

Bereits im Jahr 1994 entdeckte Peter Shor einen Algorithmus, der es erlaubt, das RSA-Kryptoverfahren in polynomialer Zeit zu brechen, also ebenso schnell, wie man damit verschlüsseln oder signieren kann. Ein Krypto-GAU. Zum Glück läuft sein Algorithmus nur auf einem hypothetischen Quantencomputer.

Am 03.09.2009 wurde bekannt, dass es Physikern der Universität Bristol gelungen ist, einen rudimentären Quantencomputer zu bauen. Damit gelang es, mit Shors Algorithmus die Zahl 15 in die Primfaktoren 3 und 5 zu zerlegen. Das gleiche Kunststück gelang Forschern von IBM schon im Jahr 2001; die Gruppe aus Bristol verkleinerte jedoch den Experimentalaufbau deutlich. Die Kontrolle von mehr Quanten-Bits zur Faktorisierung größerer Zahlen ist allerdings auch ihnen nicht gelungen.

Beruhigend für RSA-Anwender: In der Welt herkömmlicher Computer stockt die Entwicklung besserer Faktorisierungsalgorithmen, in der Welt der Quanten die von größeren Computern.

Soziale Sicherheitsbugs

Nachdem im von Aviv Raff zum „Month of Twitter Bugs" erklärten Juli 2009 insgesamt 31 Schwachstellen in Third-Party-Diensten rund um Twitter veröffentlicht wurden, stand im September das nächste Soziale Netzwerk im Brennpunkt. Pünktlich zum Bergfest des „Month of Facebook Bugs" am 15.09.2009 wurde im „Halfway Report" ein Zwischenstand veröffentlicht. Danach wurde auch diesmal jeden Tag ein „FAXX Hack" (= Facebook Application XSS/XSRF) veröffentlicht.

Wie einige Social Networks haben Facebook und Twitter einen rasanten Aufstieg hinter sich. Der Erfolg bringt aber offensichtlich zahlreiche Sicherheitslücken mit sich. Beide „MoB"s haben zu einer Erhöhung der Sicherheit der Plattformen beigetragen – wohl auch, weil sich die Betreiber und Entwickler bei der Behebung der Schwachstellen sehr kooperativ zeigten. Hoffentlich nehmen sich weitere Social Networks daran ein Beispiel.

WLAN-Sicherheit

Würden Sie mit einem Flugzeug fliegen, das, sagen wir mal, von Straßenbauingenieuren konstruiert wurde? Wohl kaum. In der digitalen Welt passieren Dinge dieser Art jedoch andauernd. Das WEP-Protokoll zur kryptografischen Sicherung von WLAN-Datenübertragungen gehört zu der Sorte von ad-hoc-Kryptografie, die von Laien entworfen wurde. Es überraschte daher nicht, als WEP im Jahr 2001 gebrochen wurde (SSN 3/2002).

Ein zentraler Punkt der Angriffsstrategie war dabei eine Methode mit dem Namen chopchop. Beim Entwurf des WEP-Nachfolgers WPA verfiel man daher auf die Idee, dieser Strategie mit einer anti-chopchop-Funktion zu begegnen - dazu wurde TKIP erfunden. Anstatt einen fundierten Protokollentwurf vorzulegen, wurde mehr oder weniger lediglich der spezielle Angriff abgewehrt, dem WEP zum Opfer gefallen war.

Im November 2008 wurde eine Schwäche von TKIP bekannt, durch die ein chopchop-Angriff auf WPA möglich wurde (SSN 11/2008). Der Angriff dauert strategiebedingt etwa eine Viertelstunde und ermöglicht lediglich das Erreichen von Teilzielen; ein Angreifer kann das WLAN also (noch) nicht übernehmen. Am 15.07.2009 veröffentlichten japanische Forscher einen praktikablen physischen Man-in-the-Middle-Angriff, der den Angriff verbessert und auf unter eine Minute beschleunigt. Auch wenn dieser nur relativ „kleine" Angriffsziele erreicht, zeigt sich einmal mehr: Hat man erst einmal einen guten Ansatzpunkt für das Brecheisen gefunden, ist die Kiste bald offen.

Was sollte man daraus lernen? Erstens, dass der Umstieg auf WPA2 mit AES-CCMP spätestens jetzt fällig ist, und zweitens, dass beweisbare Sicherheit gelegentlich ein sehr praktisches Fundament für langfristige Sicherheit bildet.

Top Cyber Security Risks

Die von SANS im September 2009 veröffentlichten „Top Cyber Security Risks" bestätigen Trends, die uns schon länger am Herzen liegen. Danach sind die beiden Top Sicherheitsthemen ungepatchte Client-Software, über die Schadcode eingeschleust werden kann, sowie Schwachstellen in Web-Applikationen.

Diese Beobachtung deckt sich mit unseren eigenen Erfahrungen, dass einerseits Netzwerk- und Perimetersicherheit in Firmen immer besser werden, es andererseits aber immer schwieriger wird, die eingelassenen Daten zu kontrollieren. Die Stadtmauern sind errichtet – an den Torkontrollen muss jedoch noch gearbeitet werden.

Open Source Security

Am 21.09.2009 hat der Toolhersteller Coverity den „Scan Open Source Report 2009" veröffentlicht. Für den zum ersten Mal 2006 auf Initiative des Department of Homeland Security (DHS) veröffentlichten Bericht wurden 280 auf C/C++ basierende Open Source Projekte mit statischer Code-Analyse auf Schwachstellen untersucht und vergleichend bewertet. Die Ergebnisse, Metriken und Benchmarks präsentiert der Bericht ausführlich auf 35 Seiten.

In erster Linie ist der Bericht eine Hilfestellung für Entscheider, die Sicherheitsaspekte bei der Auswahl von Open-Source-Lösungen berücksichtigen wollen. Aber auch die teilnehmenden Projekte selbst profitierten von der Untersuchung. Die Verbesserung der Qualität und Sicherheit einzelner Projekte wird von Coverity in der „Scan Ladder" gewürdigt. 127 Projekte erklommen die Stufe 1, 36 inzwischen sogar die Stufe 2 – darunter honorige Vertreter wie OpenVPN, OpenLDAP, Perl und Postfix.

Mobilfunk-Knacken für alle

Die Rechenleistung moderner Grafikprozessoren zieht immer mehr Codebreaker an: Bei der Konferenz Hacking at Random präsentierte Karsten Nohl (bekannt durch seine Analyse der Mifare-Chips) am 15.08.2009 ein Projekt zur weltweit verteilten Vorberechnung der Schlüsselsuche für die GSM-Mobilfunk-Chiffre A5.1, die schon lange „angezählt" ist (SSN 9/2003 und SSN 11/2007).

Nach Abschluss dieser Vorberechnung könnten abgehörte GSM-Gespräche unter Rückgriff auf die dabei erzeugte riesige Tabelle in kurzer Zeit entschlüsselt werden. Falls sie überhaupt verschlüsselt waren: Denn ob die Verschlüsselung ein- oder ausgeschaltet wird, entscheidet das GSM-Mobilfunknetz, und macht damit das Abhören via IMSI-Catcher erst möglich – unsichtbar für den Benutzer, denn fast kein Handy zeigt seinem Besitzer an, in welchem Modus es gerade arbeitet.

Secorvo News

Secorvo College aktuell

Zwei Gelegenheiten zur Aktualisierung, Erweiterung und Zertifizierung Ihres Fachwissens bietet Ihnen Secorvo-College noch in diesem Jahr:

Das viertägige Seminar „PKI – Grundlagen, Vertiefung, Realisierung" am **03.–06.11.2009** lässt keine Ihrer Fragen zu Konzeption, Implementierung und Nutzung von PKIs unbeantwortet.

Und vom **23.–27.11.2009** (mit direkt anschließender Prüfung am 28.11.2009) haben Sie Gelegenheit, Ihre Fachkenntnisse mit dem TISP-Zertifikat zu krönen – das inzwischen schon die Visitenkarten von mehr als 300 Absolventen ziert.

Neben detaillierten Seminarprogrammen mit Online-Anmeldung finden Sie auf unseren Webseiten den druckfrischen Seminarkalender 2010 zur Planung Ihrer Seminarbesuche im kommenden Jahr.

Lesefutter

Immer wieder beschäftigt uns die Frage nach der Angemessenheit diverser Anforderungen an eine Passwort-Policy. Das Ergebnis unserer Überlegungen und vieler Diskussionen haben wir nun publiziert – und räumen darin mit einigen liebgewonnenen, aber irreführenden Überzeugungen auf. Wer noch nicht vollständig auf Token-basierte Zwei-Faktor-Authentisierung umgestellt hat, findet in dem Aufsatz „Passwörter – fünf Mythen und fünf Versäumnisse" (Dirk Fox, Frank Schaefer; DuD 7/2009, S. 425-429) möglicherweise den einen oder anderen wertvollen Hinweis.

Auch zum Löschen von Daten kursieren zahlreiche nicht mehr zeitgemäße Vorstellungen (SSN 1/2009), die zu aufwändigen Verfahren führen. Unser schon im Februar erschienene Aufsatz „Sicheres Löschen von Daten auf Festplatten" (DuD 2/2009, S. 110-113) gibt aktuelle Empfehlungen und stellt geeignete Tools vor.

Security News Symposium 2010

Schon jetzt steht er fest – der Termin unseres „Security News Symposiums 2010". Wer das Event am **20.–21.04.2010** nicht verpassen will, kann sich bereits heute online anmelden.

Veranstaltungshinweise

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

Oktober 2009	
03.-04.10.	Datenspuren 2009 (CCC, Dresden)
06.-08.10.	ISSE 2009 (eema & enisa, The Hague/NL)
28.-30.10.	Hack.LU (CSRRT-LU, Luxembourg)
November 2009	
03.-06.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
17.-20.11.	In-Depth Security Conference 2009 (DeepSec, Wien/AU)
19.-20.11.	33. Dafta (GDD, Köln)
23.-27.11.	TISP-Schulung (Secorvo College)
Dezember 2009	
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)

Fundsache

Derzeit erfreuen sich pointierte Historiendarstellungen großer Beliebtheit. So die Geschichte und Funktionsweise des AES – erzählt von Jeff Moser in knapp 70 Strichmännchen-Bildern. Ebenfalls amüsant ist die knappe History of Hacking. Gleichfalls fokussiert und sehr informativ kommt die mit Unterstützung von Jean-Jacques Quisquater entwickelte interaktive Darstellung der Cryptographic Key Length Recommendations von BlueKrypt daher, zuletzt aktualisiert am 28.09.2009.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch

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