secorvo
security consulting

Secorvo Security News

Januar 2009

Editorial: Sammler

Die Begehrlichkeit kennt keine Schranken, nur Steigerung.
Lucius Annaeus Seneca (ca. 1-65 n. Chr.)

Wer die Datenschutzpraxis nicht nur aus den Gazetten kennt, den wundert eher Seltenheit als Ausmaß der aktuellen Datenschutzvorfälle. Technikentwicklung und explodierende Speicherkapazitäten lassen den Umfang personenbezogener Datensammlungen ständig anschwellen – deutlich schneller als die Sensibilität der für die Datenverarbeitung Verantwortlichen, und wohl auch die der Betroffenen.

Natürlich erfolgt die Verarbeitung immer zu deren eigenem Wohle: Schließlich geht es um zielgenauere Angebote, bedienungsfreundlichere Webseiten und Fehlerbeseitigung. Sobald ein „Mehrwert" winkt, sind die Betroffenen selbst nur zu gerne bereit, die Sammlungen um sensibelste Daten zu ergänzen.

Nirgendwo wird das deutlicher als am Beispiel von Google. Erst am 27.01.2009 hat das Unternehmen lautlos seine Datenschutzerklärung geändert: Neben den üblichen Web-Log-Daten (deren Zulässigkeit in Deutschland umstritten ist) und Cookies, die den Surfer eindeutig identifizieren, speichert Google nun auch Daten über die Nutzung der Google-Dienste. Chrome transferiert außerdem alle URLs, die der Nutzer besucht, direkt an Google. Und wer auf Seiten surft, die Google Analytics verwenden (99 % der Webseitenbetreiber ignorieren Googles Kennzeichnungspflicht), liefert Google sein komplettes Bewegungsprofil im Cyberspace. Schließlich sind da noch Google Mail und das Handybetriebssystem Android, bei denen Mail-Verzeichnisse, Adressbücher und Terminkalender nicht direkt mit dem lokalen PC, sondern über Googles Server abgeglichen werden.

Eine mächtige Datensammlung in den Händen eines einzelnen Unternehmens. Selbstverständlich werden diese Daten zu keinen anderen Zwecken genutzt als zu den in der Datenschutzerklärung angegebenen. Zumindest bisher. Wenigstens angeblich. Und gelöscht wird nach neun Monaten. Frühestens. Sagt Google.

Inhalt

Editorial: Sammler

Security News

PKI-Praxisprobleme

No Risk – No Web

Passwörter in Browsern

Gelöscht ist gelöscht

Common PKI 2.0 erschienen

Secorvo News

Secorvo College aktuell

Trau keiner Wahl ...

Veranstaltungshinweise

Fundsache

Security News

PKI-Praxisprobleme

Eine möglichst weitgehende Kompatibilität mit unterschiedlichen, besonders auch älteren Datenformaten ist in den meisten Fällen ein erwünschtes Merkmal von IT-Systemen – für die Sicherheit ist sie es häufig jedoch nicht. Ein Beispiel aus der PKI-Welt: Während Kryptologen wegen der Schwachstellen im Hashalgorithmus SHA-1 bereits einen SHA-3 suchen (SSN 10/2008), akzeptieren gängige Systeme immer noch klaglos dessen mittlerweile gebrochenen Urgroßvater MD5 (SSN 3/2005).

Am 30.12.2008 präsentierte Alexander Sotirov beim 25C3 Kongress, wie er zusammen mit Kollegen amerikanischer und europäischer Forschungseinrichtungen ein Sub-CA Zertifikat erzeugen konnte, das denselben MD5-Hashwert hat wie ein SSL-Zertifikat, das die Forscher von einem öffentlichen Trustcenter signieren ließen. Über den heimlichen Zwilling des regulär bezogenen Serverzertifikats wurden die Forscher quasi zum ebenso unautorisierten wie unkontrollierten Unterverkäufer des betroffenen Anbieters – da es um eine Demonstration ging, rückwirkend nur bis Ende 2004. Während der Nutzen von SSL ohnehin umstritten ist, löste der Beitrag bei Trustcentern natürlich umgehend Aktivitäten und Klarstellungen aus.

Aber das Problem ist nicht auf SSL beschränkt: Am 17.01.2009 veröffentlichte Didier Stevens ein per Authenticode signiertes „Hello, World!"-Programm, dessen böser MD5-Zwilling, der damit ebenso gültig signiert ist, glücklicherweise nur so tut, als ob er die Festplatte löscht. Obwohl für den offiziellen Zeitstempel SHA-1 verwendet wird, gilt dieser ebenso für beide Programme, da in Authenticode-Zeitstempel nur die angebrachte Code-Signatur, nicht aber der eigentliche Programmcode eingeht. Die Software von Peter Selinger zum Erstellen von Programm-Zwillingen ist ebenfalls im Netz verfügbar.

Nicht den MD5, sondern die in der Praxis eher ungebräuchlichen Signaturalgorithmen DSA und ECDSA betrifft ein Security Advisory des OpenSSL Projekts vom 07.01.2009. Die OpenSSL-Implementierung derartiger Signaturen liefert bei der Prüfung u. U. andere Fehlercodes als beim verbreiteten RSA-Verfahren. OpenSSL selbst und weitere betroffene Systeme lassen auch „rechnerisch falsche" Signaturen als gültig durchgehen, weil sie diese speziellen Fehlercodes nicht richtig auswerten.

Allen drei Fällen ist gemeinsam, dass ihnen am einfachsten beizukommen wäre, wenn es die PKI-Software erlaubte, die für Zertifikats- bzw. Signaturprüfung akzeptablen Algorithmen auf diejenigen zu beschränken, die als sicher gelten und auch tatsächlich gebraucht werden. Die Herausforderung für die Hersteller wäre dabei nicht, diese Funktionalität einzubauen, sondern sie so umzusetzen, dass Anwender sie einfach und effektiv nutzen können.

No Risk – No Web

Die detaillierte Analyse „Bootkits – die Herausforderung des Jahres 2008" von Kaspersky Lab, publiziert am 18.12.2008, führt erneut eindrucksvoll vor Augen, welchen Bedrohungen alle Nutzer beim Surfen im Web ausgesetzt sind. Die Erkenntnisse sind keine bahnbrechenden Neuigkeiten. Ein Google-Whitepaper vom 04.04.2007 mit dem Titel „The Ghost In The Browser" enthält umfangreiche Analysen ähnlicher Bedrohungen beim Surfen im Web. Allerdings wird in der Bootkits-Analyse verdeutlicht, wie verschiedene Eigenschaften und architekturbedingte Schwachstellen oder Mängel des Internets clever ausgenutzt werden, um zufällige Opfer mit Schadsoftware zu infiltrieren.

Zur Zeit gibt es keine umfassenden Schutzmechanismen gegen entsprechende Attacken durch Drive-by-Downloads. Die meisten Ansätze erfordern entweder hohe Anpassungs- und Wartungsaufwände oder werden als Einschränkung des „Surfgenusses" empfunden; beides ist mit geringer Akzeptanz verbunden. Trotzdem sind aktuelle Virenscannersuites, spezielle Surftools (z. B. NoScript, RequestPolicy und zukünftig auch Application Boundaries Enforcer) sowie eine gehörige Portion Vorsicht angeraten, um wenigstens gegen die häufigsten Angriffe gewappnet zu sein. Unter Umständen kann ein Werkzeug wie Bothunter helfen, Fälle aufzuspüren, bei denen das Kind schon in den Brunnen gefallen ist. Leider ist das in der Regel nicht leicht zu erkennen.

Passwörter in Browsern

Am 12.12.2008 veröffentlichte Robert Chapin die Ergebnisse eines umfangreichen Tests der Passwortmanager aktueller Versionen der Windows-Browser Firefox, Chrome, Opera, Safari und Internet Explorer. Die Ergebnisse sind ernüchternd: Von 21 Tests bestanden Firefox und Opera ganze sieben – und schnitten damit am besten ab. Chrome und Safari erfüllten nur zwei Sicherheitsanforderungen.

Besonders ernüchternd: Allein Firefox und Opera überprüfen, ob das automatisiert eingetragene Passwort auch von derselben Internet-Adresse stammt, für die es gespeichert wurde, und ob das Protokoll (bspw. http vs. https) übereinstimmt. Und lediglich Firefox erwartet – als einziger der getesteten Browser – die Zustimmung des Nutzers, wenn Herkunftsadresse oder das Übermittlungsprotokoll im entsprechenden Eintrag des Passwortmanagers überschrieben werden soll.

Zwar sollte man zumindest auf mobilen Geräten ohnehin von der Nutzung eines Browser-Passwortmanagers absehen, sofern das System nicht vollständig verschlüsselt ist. Denn der verschlüsselte Passwort-Speicher könnte auf einem verlorenen System einer Brute Force-Attacke zum Opfer fallen. Dennoch ist eine Browser-Attacke für einen Angreifer sehr viel attraktiver: Mühe- und spurenlos lassen sich bei entsprechender Verbreitung der Schadsoftware in kürzester Zeit Millionen Passwort-Datensätze einsammeln – und sogar automatisiert missbrauchen. Ein Browser mit fehlerhaftem Passwortmanager ist ein Blankoscheck für „Drive-by"-Angreifer.

Wer sicher gehen will, dass der Passwortmanager seiner Browser-Version zumindest den wichtigsten Anforderungen genügt, sollte sie der von Chapin entwickelten Online-Überprüfung unterziehen.

Gelöscht ist gelöscht

Bekanntlich führt das Löschen einer Datei in modernen Betriebssystemen nicht zur Beseitigung der Daten vom Speichermedium. Zur großen Freude von Forensikern lassen sich daher oft alle Dateien rekonstruieren, die jemals auf einer Festplatte gespeichert wurden. In der Maßnahmenempfehlung M 2.167 der IT-Grundschutz-Kataloge des BSI wird für das sichere Löschen von Dateien folgerichtig ein zwei- bis dreimaliges Überschreiben empfohlen.

Datenschützer gehen noch weiter: Im IT-Grundschutz-Baustein B 1.5 „Datenschutz" vom 04.07. 2007 werden für das datenschutzgerechte Löschen von personenbezogenen Daten mindestens sieben, bei Daten hoher Schutzstufe sogar 33 Überschreibzyklen gefordert. Diese Forderung dürfte auf eine (missverstandene) Veröffentlichung von Peter Gutmann („Secure Deletion of Data from Magnetic and Solid-State Memory") vom 22.07.1996 zurück gehen – die sich auf inzwischen veraltete Festplattentechnologie bezog. Daher sorgte der Beitrag „Overwriting Hard Drive Data: The Great Wiping Controversy" von Craig Wright, Dave Kleiman und Shyaam Sundhar auf der ICISS 2008 (16.-20.12.2008) für Wirbel: Abgesehen von ein paar technischen Fehlern (siehe „Further Epilogue" in Gutmanns Papier) stellen die Autoren überzeugend klar, dass die Rekonstruktion eines einzigen, einmal überschriebenen Bits immer nur mit einer gewissen Wahrscheinlichkeit gelingt. Selbst wenn die Erfolgsaussicht 99,9 % erreicht, liegt die Wahrscheinlichkeit, eine nur 2 kB große Datei zu rekonstruieren, bei 0,000076 % (so viel wie ein 6er im Lotto). Merke: Ein einfaches, einmaliges und vollständiges Überschreiben genügt für ein sicheres Löschen.

Common PKI 2.0 erschienen

Am 20.01.2009 wurde Version 2.0 der Common PKI-Spezifikation (ehemals ISIS-MTT) vom T7 e. V., dem Verband der Trustcenter-Betreiber, und dem TeleTrusT e. V. veröffentlicht. Die neue Version wurde – unter Mitwirkung von Secorvo – dem aktuellen Stand der in der Common PKI zusammengestellten und profilierten internationalen Standards angepasst und trägt so der Entwicklung auf dem Gebiet der PKI-Standardisierung seit der Publikation von ISIS-MTT 1.1 (am 16.03.2004) Rechnung.

Eine wesentliche Neuerung von Common PKI 2.0 stellt die Signatur-API dar, die das PKCS#11-Profil von ISIS-MTT 1.1 ersetzt. Sie basiert auf der eCard-API-Spezifikation des Bundes, ist aber deutlich kompakter, da sie sich auf die Funktionen beschränkt, die zur Anwendung der in Common PKI definierten Datenformate für Signatur und Verschlüsselung benötigt werden.

Secorvo News

Secorvo College aktuell

Seit 2004 haben mehr als 250 Sicherheitsexperten das T.I.S.P.-Zertifikat erworben. Im März steht das erste T.I.S.P.-Seminar bei Secorvo College auf dem Programm. Frühbucher sollten sich bis zum 09.02.2009 die letzten vergünstigten Plätze sichern.

Damit Softwareentwicklung in Zukunft sicherer wird, hat ISSECO einen international Zertifizierungsstandard für Software-Engineers entwickelt. Eine Schulung mit Prüfung zum CPSSE (Certified Professional for Secure Software Engineering) bietet Secorvo erstmals im Februar und September an.

Neben Klassikern wie IT-Sicherheit heute und PKI hält Secorvo College spannende neue Themen aus allen Bereichen der IT-Sicherheit für Sie bereit. Termine und Seminar-Details finden Sie im Seminarkalender und den ausführlichen Seminarprogrammen.

Trau keiner Wahl ...

... die du nicht selbst gefälscht hast: Auf dem ersten Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) im neuen Jahr wird Dr. Jörn Müller-Quade das mit dem Deutschen IT-Sicherheitspreis 2008 ausgezeichnete "Bingo Voting" vorstellen – ein Verfahren, bei dem der Wähler einen Beleg erhält, der es ihm ermöglicht, die korrekte Zählung der eigenen Stimme zu überprüfen. Dr. Müller-Quade war einer der Gutachter vor dem Bundesverfassungsgericht zu elektronischen Wahlmaschinen und leitet das Europäische Institut für Systemsicherheit (E.I.S.S.). Der Vortrag findet statt am 19.02.2009 im Schlosshotel Karlsruhe, Beginn: 18 Uhr. Im Anschluss gibt es – wie gewohnt – Gelegenheit zum "Buffet-Net(t)working". Um Anmeldung wird gebeten.

Veranstaltungshinweise

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

Februar 2009	
03.-04.02.	19. SmartCard-Workshop (Fraunhofer, Darmstadt)
19.02.	Trau keiner Wahl, die du nicht selbst gefälscht hast (KA-IT-Si, Karlsruhe)
22.-25.02.	16th Int. Workshop on Fast Software Encryption (IACR, Leuven/BE)
März 2009	
09.-13.03.	T.I.S.P.-Schulung (Secorvo College)
15.-17.03.	Sixth IACR Theory of Cryptography Conference (IACR, San Francisco, US)
16.-19.03.	Third International Workshop on Secure Software Engineering (SINTEF, Fukuoka/JP)
17.-18.03.	16. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
17.-19.03.	IT-Sicherheitsaudits (Secorvo College)
24.-25.03.	Security Awareness (Secorvo College)
31.03.-03.04.	Forensik - Verfahren, Tools, Praxiserfahrung (Secorvo College)

Fundsache

Einer der häufigsten Fehler in Datenbank basierten Web-Anwendungen ist die Anfälligkeit für SQL-Injection (Platz zwei der OWASP Top 10). Am 05.12.2008 haben die Oracle-Mitarbeiter Mark Fallon, Bryn Llewellyn und Howard Smith ein 67seitiges White Paper („How to write SQL injection proof PL/SQL“) mit wertvollen Hinweisen veröffentlicht, wie sich sichere SQL-Abfragen entwickeln lassen.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, 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