secorvo
security consulting

Secorvo Security News

Februar 2009

Editorial: Double Cross

NSA offering ‚billions' for Skype eavesdrop solution. The register, 12.02.2009

Der Psychologe und Kommunikationswissenschaftler Paul Watzlawick wäre begeistert gewesen. In „Wie wirklich ist die Wirklichkeit" erläuterte er 1976 anschaulich das Phänomen der Interdependenz, illustriert am Beispiel geheimdienstlicher Desinformation („XX"). Hier finden wir nun ein Exempel in Reinkultur. Was lässt sich aus dem angeblichen Angebot der NSA lernen? Dass sie Skype tatsächlich nicht abhören kann? Oder dass sie den Eindruck erwecken möchte, dass sie es kann, damit Nutzer sich auf die Vertraulichkeit verlassen – und hemmungslos offen kommunizieren?

Tatsächlich lässt sich die Aussage systematisch analysieren. Angenommen, das Gerücht ist wahr. Wann würde die NSA davon profitieren? Fall 1: Sie kann Skype bisher nicht entschlüsseln und findet jemanden, der Skype bricht. Dann kann sie es – und gewinnt, selbst wenn es bekannt wird (denn erstens wird das mglw. für eine Desinformation gehalten, und zweitens gibt es bisher keine gute Alternative). Allerdings kostet sie das einen Milliardenbetrag. Fall 2: Findet sie niemanden, bleibt die Situation, wie sie ist – die Nutzer wissen nicht, dass sie niemanden gefunden hat und nicht abhören kann. Fall 3: Sie kann Skype bereits entschlüsseln und findet niemanden, der es schafft. Auch dann gewinnt sie – denn das stärkt das Vertrauen der Nutzer in Skype. Kritisch ist allein Fall 4: Sie kann Skype entschlüsseln, und jemand bricht Skype. Dann kann sie verlieren – nicht nur einen Milliardenbetrag für etwas, das sie nicht braucht, sondern auch die Nutzer, die bisher darauf vertrauten, dass die NSA nicht mithören kann. Daraus lernen wir: Die NSA ist sich sicher, dass das Brechen von Skype schwierig ist – es ist ihr entweder sehr viel Geld wert, oder sie ist überzeugt, dass es niemandem gelingen wird.

Übrigens: Man munkelt, Secorvo habe Skype gebrochen, wolle das Wissen aber nicht an die NSA verkaufen.

Jetzt sind Sie dran.

Inhalt

secorvo
security consulting

Security News

Wurm drin

Nun gibt es sicherlich zahlreiche Gründe, sich für einen Computer des Herstellers Apple zu entscheiden. Ein Grund hat allerdings inzwischen nur noch wenig Überzeugungskraft: Das Betriebssystem OS X sei erheblich sicherer als Windows. Am 13.02.2009 veröffentlichte Apple das Sicherheitsupdate 2009-001 für Mac OS X 10.4 und 10.5. Damit stopft Apple insgesamt 48 Sicherheitslücken in über 20 Betriebssystemkomponenten, darunter ein kritischer Zero-Day-Bug im Safari-Browser. Wer – ungeachtet des schlechten Abschneidens beim Umgang mit Passworten (siehe SSN 01/2009) – die Windows-Version von Safari nutzt, sollte umgehend auf Version 3.2.2 wechseln.

Spätestens jetzt wird es Zeit, auch unter OS X die Software-Update-Funktion zu aktivieren. Denn nun ist auch für Apple-Nutzer das Paradies zu Ende. (Vielleicht hätten sie besser nicht hineingebissen.)

Druckerpatch

Es ist so weit: Die Sicherheitsdisziplin des Patchens hat nicht nur Apple, sondern auch die Peripheriegeräte erreicht. Am 04.02.2009 veröffentlichte HP einen Security Patch für seine Laser- und Farbdrucker, der eine kritische Sicherheitslücke schließt. Geschickt ausgenutzt kann sie Unberechtigten den Zugriff auf Druckdateien ermöglichen.

Angesichts immer leistungsfähigerer „Embedded Systems“ und der zunehmenden Vernetzung von Kleinstgeräten wird es nun nicht mehr lange dauern, bis Security Patches auch beim digitalen Bilderrahmen, dem MP3-Player und dem E-Book-Reader zur Gewohnheit werden – sofern die Hersteller nicht endlich beginnen, ihre Entwickler in sicherer Softwareentwicklung zu trainieren. Dann könnte es bald Zeit werden, vom PC zur Schreibmaschine „upzugraden“.

Schwächelnde Profis

Nachdem der Hashalgorithmus MD5 gebrochen und der Secure Hash Standard (SHA) von 1993 erst 2002 und erneut im Oktober 2008 wegen neuerer Angriffe aktualisiert werden musste, schrieb das US-amerikanische NIST am 02.11.2007 ähnlich wie 10 Jahre zuvor beim AES eine „Cryptographic Hash Algorithm Competition“ aus. Bis zum 31.10.2008 konnten Kandidaten für einen Nachfolger des SHA-2 (Arbeitstitel: SHA-3) gemeldet werden.

Zwei Tage vor Beginn der ersten Hash Function Candidate Conference an der Universität Leuven veröffentlichte Fortify am 20.02.2009 die Ergebnisse einer Analyse der Referenzimplementierungen von 42 der vom NIST für Runde 1 akzeptierten und noch nicht gebrochenen Kandidateneinreichungen.

Ergebnis: Bei sechs Kandidaten fand Fortify mit seinem Source Code Analyser sicherheitskritische Bugs. Besonders peinlich: Die Implementierung des MD6 von Ron Rivest enthielt allein drei (!) Buffer Overflows – und das, nachdem ein Buffer Overflow in der RSA-Referenzimplementierung erst 1999 fast alle SSL- und SSH-Implementierungen kaltgestellt hatte. Merke: Trau' keiner Referenzimplementierung, die Du nicht selbst geprüft hast. Erst recht, wenn sie von einem Kryptologen stammt.

Web Apps – kritisch betrachtet

Mit der am 18.12.2008 erstmalig auf der OWASP-Webseite erwähnten Neuauflage des „OWASP Testing Guide“ wurde ein bewährtes Standardwerk zur Analyse von Web-Applikationen aktuellen Anforderungen angepasst und noch einmal erweitert. Die aktuelle Version v3 erleichtert durch die Einführung von Referenznummern für Testfälle die Kommunikation über Applikationstests gegenüber der Vorgängerversion v2 erheblich.

Inhaltlich wurden die meisten technischen Tests aktualisiert. Einige Testfälle wurden neu sortiert, so dass der neue Guide sich deutlich flüssiger liest, obwohl er um knapp 80 Seiten gewachsen ist. Bei den Tests stechen folgende Änderungen ins Auge: die ausführliche Erweiterung um den Bereich „Configuration Management Testing“, die Ergänzung um Aspekte von „Authorization Testing“ und weitere Änderungen beim „Data Validation Testing“.

Der Ansatz einer ganzheitlichen Betrachtung der Sicherheit von Applikationen über deren gesamten Lebenszyklus steht auch weiterhin im Vordergrund des Guides.

Ergänzend zu dem OWASP-Guide, der eine analytische Sicht der Sicherheit bietet, beleuchtet ein Positionspapier der ENISA zu „Web 2.0 Security and Privacy“ aus dem Dezember 2008 Sicherheits- und Datenschutzrisiken bei aktuellen Trends im World Wide Web. Die Kombination aus motivierendem Überblick und technischem Handwerkszeug gibt Verantwortlichen ausgiebiges Know-How zur Verbesserung der Sicherheit im WWW an die Hand.

Sametime – Same Password

Am 31.01.2009 veröffentlichte Carl Tyler in seinem Blog ein aus Sicherheitssicht kritisches Feature von Lotus Sametime: Ab Version 7.5 kann durch ein Plugin auf die gespeicherten Kennwörter im Klartext zugegriffen werden. Diese Funktion unter-

stützt die Realisierung von Single-Sing-On, könnte aber in verschiedenen Angriffsszenarien ausgenutzt werden: Meldet sich ein Benutzer in einer anderen Community an, die die Installation von Plugins zulässt, können dort ein Plugin installiert und die Sametime-Kennwörter ausgespäht werden. Auch könnte sich über diese Funktion ein Sametime/ Notes-Administrator Zugang zu den Kennwörtern verschaffen. Beide Szenarien sind besonders kritisch, wenn die Sametime-Kennwörter (benutzerfreundlich per Passwortsynchronisation) auch für weitere Anwendungen verwendet werden und somit ein unbefugter Zugriff auf weitere Daten möglich ist.

Sofern nur die im Notes Client integrierte Version von Sametime verwendet oder Samtetime über IBMs LTPA-Token authentifiziert wird, kann die Funktion nicht genutzt werden. In der Stellungnahme des Herstellers IBM vom 06.02.2009 wird darauf hingewiesen, dass derartige Funktionen beabsichtigt sind – und auch bei anderen Produkten wie Browsern verwendet werden, um beispielsweise ein Single-Sign-On zu ermöglichen. Um den eigenen Sicherheitsansprüchen gerecht zu werden, ist vorgesehen, in einer Technote auf die potentiellen Sicherheitsprobleme hinzuweisen und zu definieren, wie ein Schutz – beispielsweise durch eine digitale Signatur und Autorisierung für Plugins – erreicht werden kann. Betroffene Unternehmen sollten diese Diskussion verfolgen.

Helix ist tot, es lebe Helix

Nessus hat es vorgemacht (vgl. SSN 06/2008) – nun hat auch e-fense als Entwickler des äußerst populären Forensik-Werkzeugkastens Helix sein Lizenzmodell geändert. Seit dem 23.01.2009 ist Helix weder Open Source noch frei verfügbar. Wer künftig „Helix Pro“ einsetzen möchte, muss sich für ca. 15 Dollar pro Monat beim Hersteller registrieren lassen – was freilich noch immer deutlich preisgünstiger ist als die meisten anderen kommerziellen Forensik-Tools. Glücklich schätzen können sich diejenigen, die vor wenigen Monaten die letzte freie Version heruntergeladen haben (vgl. SSN 10/2008).

Fast zeitgleich mit der Kommerzialisierung von Helix ist übrigens am 11.02.2009 eine Beta-Version von Backtrack erschienen – eine Live-Distribution, die zumindest rudimentäre Forensik-Funktionen enthält.

Online Games – Serious Business

Am 28.01.2009 wurde im Presseportal der Polizei Nordrhein-Westfalen über eine kuriose Diebstahlanzeige berichtet: Ein Spieler eines Online-Rollenspiels war seiner virtuellen, mit viel zeitlichem und finanziellem Aufwand erworbenen Ausrüstungsgegenstände beraubt worden.

Die Anzeige wirft zahlreiche technische und rechtliche Fragen auf. Interessant ist allerdings, dass die Fragestellung deutlich präsenter ist, als vielleicht angenommen. Schon im November 2008 beleuchteten 18 Autoren in einem ENISA-Bericht „Virtual Worlds, Real Money“ auf 80 Seiten Sicherheitsrisiken und Empfehlungen für „Massively-Multiplayer Online Games and Social and Corporate Virtual World“. Ereignisse in zahlreichen „virtuellen Welten“ – nicht nur in Second Life – dürften in den kommenden Jahren in wachsendem Maße Auswirkungen in der „realen Welt“ haben. Der kurzweilig geschriebene Bericht gibt davon einen ersten Eindruck.

TCG-versiegelt

Die Trusted Computing Group (TCG), der u. a. Hersteller wie HP, IBM, Lenovo und Sun Microsystems angehören, hat am 27.01.2009 zwei richtungsweisende Standards zur Verschlüsselung von Speichersystemen sowohl für Desktops und Laptops als auch für Enterprise Lösungen veröffentlicht.

Angesichts der schwer verdaulichen 80 bzw. 130seitigen Standards gerät leicht aus dem Blick, dass die TCG damit die Grundlage für eine einheitliche und von den Chips der PC-Hardware-Hersteller unterstützte Verschlüsselung von Speichermedien gelegt hat. Sollte sich der Ansatz durchsetzen, könnten verschlüsselte Festplatten in wenigen Jahren der „Hardware-Standard“ sein – und die heutigen Spezialanbieter einschlägiger Softwarelösungen sich auf die allein schon herausfordernde Aufgabe des Schlüsselmanagements konzentrieren.

Secorvo News

Secorvo College aktuell

Nur noch wenige Seminarplätze sind im März für Sie frei: Vom 09.-14.03.2009 können Sie Ihr Wissen mit dem begehrten T.I.S.P.-Zertifikat besiegeln. Wertvolle Tipps für die erfolgreiche Umsetzung von Sicherheitsmaßnahmen zur Schließung von Sicherheitslücken bekommen Sie im Seminar "IT-Sicherheitsaudits in der Praxis" - nutzen Sie Ihre Chance, bevor auch dieses Seminar vom 17.-19. 03.2009 ausgebucht ist.

Im April halten wir einen Klassiker zu Grundlagenthemen für Sie bereit: "IT-Sicherheit heute" vom 21.-24.04.2009. Buchen Sie Ihren Platz noch bis zum 16.03.2009 mit Frühbucherrabatt. Alle weiteren Termine und Infos finden Sie auch in unserem Seminarkalender 2009.

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

Veranstaltungshinweise

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

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)
April 2009	
21.04.	2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (Usenix, Boston/US)
21.-24.04.	IT-Sicherheit heute (Secorvo College)
26.-30.04.	Eurocrypt 2009 (IACR, Köln)

Fundsache

Bereits am 10.12.2008 hat Google sein "Browser Security Handbook" unter Google Code veröffentlicht, um die Entwicklung sicherer Web 2.0-Anwendungen zu fördern. Seitdem haben die Autoren um Michal Zalewski die Gegenüberstellung der Sicherheitsfeatures aktueller Browser-Versionen aufgrund jüngster Tests mehrfach aktualisiert. Die Übersicht gibt wertvolle Hinweise zur Sicherheit aktueller Browser und geht damit über die Untersuchung von Robert Chapin (SSN 01/2009) hinaus.

Impressum

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

ISSN 1613-4311

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