secorvo
security consulting

Secorvo Security News

November 2009

Social Engineering 2.0

Für viele Jugendliche ist der eigene Auftritt in SchülerVZ, Wer-kennt-wen oder Facebook inzwischen ein soziales Muss, wie die Nutzerzahlen von Sozialen Netzwerken belegen. Und immer mehr Berufstätige pflegen ihre Kontakte über Business-Netzwerke wie Xing oder publizieren ihre Ein- und Ansichten in Twitter. Diese Entwicklung ist schon allein aus Datenschutzperspektive bedenklich: Neben den gespeicherten Personendaten kennt der Netzwerk-Betreiber alle Kontaktbeziehungen, das Nutzungsverhalten und die Suchanfragen.

Für einen Social Engineer ist ein mächtigeres Auskunftssystem hingegen kaum vorstellbar. Jeder registrierte Nutzer kann die öffentlichen Teile aller Personenprofile einsehen und nach Unternehmen und Personen, in deren persönlichen Daten, Interessen und Kontakten recherchieren – ideales Informationsfutter für einen gezielten Social Engineering Angriff. Da die Identität bei der Registrierung nicht überprüft wird, fällt es leicht, sich mit falschem Namen und CV anzumelden, um sich anschließend in das Kontaktnetz anderer Nutzer hineinzumogeln. Dann sind deren Kontakte, Telefondurchwahl und Mobilfunknummer, Interessen, E-Mail-Adresse und jede Änderung im Kontakt-Netzwerk sichtbar. Und Auswertungstools wie Twitnest liefern die wichtigsten Kontaktknoten frei Haus.

Zum Schutz vor raffinierten Social Engineers hilft da nur ein striktes Nutzungsverbot – oder die Aufklärung über „Dos and Don'ts".

Abb. 1: Twitnest-Grafik

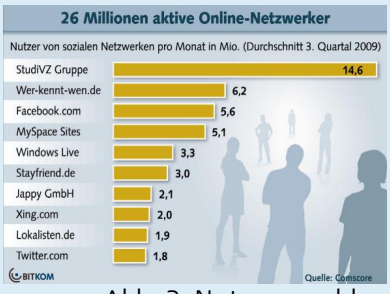

Abb. 2: Nutzungszahlen

Inhalt

secorvo
security consulting

Security News

Angriff auf SSL/TLS

Marsh Ray und Steve Dispensa deckten am 04.11.2009 eine bislang unbekannte, gravierende Schwäche des SSL- und TLS-Protokolls – seit Januar 1999 IETF-Standard – auf. Sie erlaubt einem Angreifer, beliebigen Text in die Kommunikation zwischen Client und Server einzuschleusen. Im Fall von HTTPS kann das z. B. dazu führen, dass ein Client ein vom Angreifer bestimmtes Formular im Kontext einer neuen Sitzung angezeigt bekommt.

Die Schwäche betrifft das Protokoll zur Neuaushandlung von Sitzungsschlüsseln. Zwar bleibt die Vertraulichkeit gewahrt, aber bei der Aushandlung entsteht eine „Authentizitäts-Lücke", durch die nicht nur der Client oder Server, sondern auch ein Angreifer die (üblicherweise gar nicht benötigte) Neuaushandlung veranlassen kann. Der Angriff wurde zunächst für Client-Zertifikate demonstriert, funktioniert jedoch auch allein mit Server-Zertifikat. Betroffen sind alle Anwendungsprotokolle vom Online-Banking bis POP3S, die SSL/TLS nutzen.

Als schnelle Abhilfe gibt es zumindest für OpenSSL einen Patch, der die Neuaushandlung von Schlüsseln einfach abschaltet.

Ein so wirksamer Angriff auf ein so gut untersuchtes und etabliertes Protokoll wie SSL/TLS kommt sehr überraschend. Er zeigt aber einmal mehr, dass Schwachstellen oft an den „Nähten" auftreten (hier der Kontextwechsel zwischen zwei Sitzungen), und dass daher selten genutzte Features in einem Sicherheitsprotokoll entweder weggelassen oder mindestens ebenso genau analysiert werden sollten wie das Kernprotokoll.

(Alp)Traum iPhone

Dem seit dem 19.06.2009 in Deutschland verfügbaren iPhone 3GS hat Apple neben einer neuen Betriebssystemversion auch eine hardware-basierende Verschlüsselung gegönnt. Dank dieser und weiterer Sicherheitsfunktionen wie IPSec VPN, WPA2 Enterprise Wi-Fi und SSL/TLS erfreut sich das iPhone 3GS auch in Unternehmen wachsender Beliebtheit. Um letzte Zweifler von der Sicherheit des iPhone zu überzeugen, bietet Apple mit dem Dienst „Mobile Me" für 79 €/Jahr die Services „Mein iPhone suchen" und „Remote Wipe" an. Damit sollen sich ein vermisstes iPhone lokalisieren und alle Benutzerdaten aus der Ferne löschen lassen.

Der Sicherheitsgewinn ist jedoch begrenzt, denn zur Deaktivierung beider Dienste genügt es, die SIM-Karte zu wechseln. Auch die Datenverschlüsselung lässt sich umgehen, selbst wenn das iPhone durch einen Passcode gesperrt ist, wie Jonathan Zdziarski am 23.07.2009 in einem Interview mit dem Magazin Wired beschrieben und in einem tags darauf auf Youtube veröffentlichten Video demonstriert hat. Denn wie beim iPhone 2G/3G ist eine „Sicherung" der Benutzerdaten auch beim iPhone 3GS ohne Aufspielen einer modifizierten Firmware und ohne Brechen der Verschlüsselung möglich. Dazu wird das iPhone von einer RAM-Disk gebootet und dann die Partition mit den Benutzerdaten als Raw-Disk-Image gesichert – für die Entschlüsselung der Daten sorgt das iPhone dabei automatisch. Anschließend lässt sich das Raw-Image unter Mac OS mounten oder mit gängigen Forensik-Tools analysieren.

Das Glück des Forensikers ist in diesem Fall zugleich der Alptraum des Sicherheitsverantwortlichen, der seinem Management darlegen muss, warum der sichere Einsatz des iPhones im Unternehmen tatsächlich nicht so einfach ist, wie Apple verspricht.

Windows 7 Sicherheitsprofile

Mit dem am 28.10.2009 von Microsoft veröffentlichten Security Compliance Management Toolkit stehen nun neben einer detaillierten Dokumentation der Sicherheitseinstellungen von Windows 7 auch zwei direkt nutzbare Grundtypen von Sicherheitsprofilen zur Verfügung: Die Profile EC (Enterprise Client) und SSLF (Specialized Security – Limited Functionality), beide schon von ihrer Einführung für Windows XP, Server 2003, Vista und Server 2008 im Februar 2009 bekannt.

SSLF folgt dem Prinzip, Sicherheitseinschränkungen vor Funktionalität zu stellen, und legt damit eine gute Grundlage für die Härtung kritischer Systeme. Spezialisten sei als weiterführende Lektüre das Windows 7 and Windows Server 2008 R2 Application Quality Cookbook empfohlen.

Schade nur, dass der Fehler von vergangenen Windows-Härtungen konsequent fortgesetzt wurde: auch diesmal werden die Sicherheitseinstellungen der Zugriffskontrolllisten (DACL) für u. a Dateisystem, Registrierung und Dienste (Services) sowie die dazugehörigen Auditfunktionen (SACL) nicht weiter gewürdigt. Mit Windows NT4 (SP6a) war Microsoft da schon einmal weiter.

OWASP Top 10 runderneuert

Im Rahmen der OWASP Appsec 2009 in Washington stellte Dave Wichers am 13.11.2009 die Überarbeitung der bekannten OWASP Top 10 vor. Zeitgleich wurde der Release Candidate 1 der Top 10 zum Download veröffentlicht.

Bei der neuen Version handelt es sich um die inzwischen dritte Überarbeitung. Die Änderungen liegen etwas im Verborgenen, prägen aber den Charakter der neuen Top 10 grundlegend. Listeten

die Vorgängerversionen die am meisten auftretenden Schwachstellen bei Web-Anwendungen auf, orientieren sich die Top 10 nun an Risiken, die nach vorgegebenen Kriterien bewertet wurden. Dabei wurden Angreifer, Ausnutzbarkeit der Schwachstelle und mögliche Auswirkungen berücksichtigt.

Auch die Darstellung der Top 10 hat sich verändert. Zielte das Dokument bisher hauptsächlich darauf, die Awareness von Entwicklern für Schwachstellen zu verbessern, wurde die Zielgruppe jetzt auf Entscheider, Tester und Sicherheitsexperten erweitert. Jeder Eintrag besteht aus einer Bewertung des Risikos, der Vorstellung von Schutzmaßnahmen, Beispielen und Referenzen. Die meisten der enthaltenen Verweise zeigen auf hilfreiche OWASP-eigene Dokumente.

In den neuen Top 10 haben die beiden Spitzenreiter der Vorversion „Injection" und „XSS" die Plätze getauscht. Auf Platz 6 und 8 finden sich als Neueinsteiger „Security Misconfiguration" und „Unvalidated Redirects and Forwards". Zur Zeit befinden sich die Top 10 noch in der Review-Phase. Kommentare und Verbesserungsvorschläge an den Autor sind herzlich willkommen.

Vorsicht Falle!

Für einen am 04.09.2009 veröffentlichten Technical Report hat sich Frank Stajano von der Universität Cambridge mit Paul Wilson, einem der Autoren der BBC-Serie „The Real Hustle" (einer Art Mischung aus „Vorsicht Falle!" und „Vorsicht Kamera!") zusammen getan – nicht, um Prinzipien der Informationssicherheit anschaulich zu illustrieren, sondern um die „menschlichen Faktoren" zu verstehen, die Trickbetrüger regelmäßig ausnutzen.

Der Report stellt zunächst zahlreiche typische, in der Sendung gezeigte Betrugsfälle vor. Daraus leiten die Autoren dann sieben Verhaltensprinzipien von Ablenkung über Herdentrieb bis zum gefühlten Zeitdruck ab, die Betrüger ausnutzen – und die es im Umkehrschluss beim Design von sicher nutzbaren Systemen zu vermeiden gilt.

Das Dokument liefert viele lebendige Beispiele zur Illustration von Security-Themen – und könnte als Lehrmaterial für Entwickler von Security-relevanten Benutzerschnittstellen effektiver sein als manches Theorie lastige „Securitiy & Usability"-Papier. Unterhaltsamer ist es allemal.

Secorvo News

Secorvo College aktuell

Der TISP ist etabliert: Seit der Einführung im Jahr 2004 haben 350 Teilnehmer das Zertifikat erworben – Tendenz steigend. Gehören auch Sie zu den ersten 500 und buchen Sie Ihren Platz in einer der TISP Schulungen 2010 bei Secorvo College – zum Beispiel vom 22. bis 26.02.2010. Auch in der Softwareentwicklung beginnt sich erfreulicherweise Sicherheit als Qualifikation durchzusetzen. Das zeigt unter anderem das Interesse am CPSSE, dem ersten Qualifikationszertifikat für sichere Softwareentwicklung. Nächster Termin: 16. bis 19.03.2010.

Details zu allen Seminaren finden Sie auf unseren Webseiten; die Jahresübersicht 2010 erleichtert die Planung. Wir freuen uns auf Ihre Anmeldung.

Wunsch und Wirklichkeit

Gelegentlich werden auch in der IT-Sicherheit Wünsche wahr. Das zeigt die Awareness-Kampagne „SecurityCup 2009", in der es die FIDUCIA zusammen mit der Agentur DauthKaun geschafft hat, ihre Mitarbeiter wirksam zum Schutz von Informationen, Daten und Know-How zu sensibilisieren. Am 18.02.2010 stellen Sven Kaun (DauthKaun) und Lutz Bleyer (FIDUCIA) die Kampagne auf der ersten Veranstaltung der KA-IT-Si im neuen Jahr vor – wir freuen uns auf Ihre Teilnahme (Beginn wie immer um 18 Uhr im Schlosshotel Karlsruhe, mit anschließendem Buffet-Networking).

Übrigens: Die Unterlagen des letzten diesjährigen KA-IT-Si-Events vom 26.11.2009 zum Thema Datenrettung finden Sie zum Download auf den KA-IT-Si-Seiten.

Feiertagslektüre

Seit Online-Banking in den Fokus von Internet-Angriffen gerückt ist und sowohl Phishing-E-Mails als auch spezialisierte Banking-Trojaner die Vermögen deutscher Bankkunden bedrohen, haben Banken neue Protokollvarianten eingeführt – von iTAN über mTAN bis zum TAN-Generator. Nun hat Hans-Joachim Knobloch zwei grundlegende Verfahren einer Sicherheitsanalyse mittels BAN-Logik unterzogen und die Ergebnisse in Ausgabe 12/2009 der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)" veröffentlicht.

Ebenfalls in der DuD erscheint im Januar 2010 in der Rubrik „Best Practice" eine Empfehlung von Kai Jendrian zur Erweiterung des Web-Browsers Firefox um Add-ons, die die Sicherheit und den Schutz der persönlichen Daten beim Surfen signifikant erhöhen. Da ist möglicherweise der eine oder andere wertvolle Tipp dabei, um an den Feiertagen den Schutz des neuen PCs wirksam zu verbessern.

Weitere Publikationen von Secorvo finden Sie in der Übersicht auf unserer Webseite.

Veranstaltungshinweise

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

Dezember 2009	
06.-10.12.	15th ASIACRYPT 2009 (IACR, Tokio/JP)
27.-30.12.	26th Chaos Communication Congress (CCC, Berlin)
Januar 2010	
19.-21.01.	Omnicard 2010 (inTIME, Berlin)
Februar 2010	
02.-03.02.	20. SIT-SmartCard-Workshop (Fraunhofer-Institut SIT, Darmstadt)
03.-04.02.	ESSoS (DistriNet Research Group, Pisa/I)
05.-07.02.	ShmooCon 2010 (Shmoo Group, Washington/USA)
09.-10.02.	17. DFN Workshop – Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
22.-26.02.	TISP-Schulung (Secorvo College)
März 2010	
16.-19.03.	ISSECO Certified Professional for Secure Software Engineering - CPSSE (Secorvo College)
23.-25.03.	Sicherheitsmanagement heute (Secorvo College)

Fundsache

In einem 123seitigen Report vom 20.11.2009 hat die European Network and Information Security Agency (ENISA) die Nutzung von Cloud-Computing einer Risiko-Analyse unterzogen. Acht von 35 betrachteten Risiken ordnet sie dabei der Risikoklasse „High“ zu. Daraus leitet sie zahlreiche Empfehlungen für die Nutzung von Cloud-Computing ab.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Safuat Hamdy, Kai Jendrian, Hans-Joachim Knobloch, Jochen Schlichting, Jörg Völker

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