Secorvo Security News
Oktober 2003

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch
Secorvo Security Consulting GmbH

Nr. 10, 2. Jhrg. 2003
Stand 20. Oktober 2003

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

Inhalt

Editorial: WYSIWY – B?

In festem Vertrauen auf unsere Erfahrung und Aufmerksamkeit sind wir überzeugt, dass bei kompetenter Nutzung des Internet nichts passieren könne – jedenfalls nicht uns. Schließlich vertrauen wir nicht naiv auf die Gutartigkeit der E-Mail-Anhänge unbekannter Absender, selbst bei bekannten Adressen sind wir skeptisch und öffnen sie nicht. HTML-formatierte E-Mails betrachten wir grundsätzlich nur in reinem Textformat, da sie über Web Bugs heimlich Rückmeldungen an den Sender auslösen können. Spam isolieren und löschen wir nach kurzer Prüfung – die „keep me off that list"-Option geflissentlich ignorierend. Und Updates sowie Sicherheits-Patches beziehen wir nur aus verlässlicher Quelle via CD.

Auch außerhalb des Firmennetzes nutzen wir das Internet ausschließlich mit (Personal) Firewall. ActiveX- und VisualBasic-Script-Komponenten filtern wir heraus, Flash-Intros werden übersprungen, PlugIns nicht automatisch installiert. Und wenn's ums Geld geht, sind wir noch vorsichtiger: Kreditkartennummern vertrauen wir keiner Webseite an, Passwort-Login und Online-Banking gibt es nur bei SSL-Verbindungen. Dabei prüfen wir: Ist das Zertifikat gültig? Wurde es für die gewählte Webseite ausgestellt? Ist der Schlüssel lang genug?

Zwar ist das Internet so nur noch mit Einschränkung nutzbar. Die Perfidie der Angreifer haben wir dennoch unterschätzt. So gehen wir meist davon aus, dass die Konfigurationsoberfläche kein Potemkinsches Dorf ist – haben wir doch das Credo „What You See is What You Get" tief verinnerlicht.

Wer aber garantiert uns, dass der Mechanismus vieler Werbe-Banner, eine Interaktionsbox zu simulieren, uns nicht beim Homebanking die SSL-Verbindung nur vortäuscht? Dass die URL-Anzeige im Browser auch den verbundenen Server anzeigt? Dass eine E-Mail vom angegebenen Sender stammt? Sollte das World Wide Web so zum „What You See is What You Believe", werden, wäre das der Anfang vom Ende dieses effizienten Mediums.

1 Security News

1.1 „U-Bahn-Spoofing" in Hamburg

Das News-Forums Symlink dokumentierte am 06.10.2003 eine Manipulation der Infobildschirme der Hamburger U-Bahn (siehe Fotos). Hacker hatten die Texte der eingeblendeten Nachrichten abgefangen und modifiziert. Dabei machten sie sich zu Nutze, dass die in vielen U-Bahn-Waggons installierten Windows95-Systeme ihre Meldungen an bestimmten U-Bahnhöfen über ungesicherte WLAN-Verbindungen beziehen. Auch wenn diese Aktion sicherlich mehr Unterhaltungswert als Gefährdungspotenzial besitzt, dokumentiert sie die inhärenten Sicherheitsprobleme heutiger WLAN-Lösungen.

1.2 Neue EU-Studien

Die im Juli 2003 von der EU-Kommission vorgelegte Studie "Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview" kommt zu dem Ergebnis, dass sich das Gleichgewicht zwischen Privatsphäre einerseits und Sicherheit andererseits durch moderne Kommunikationstechniken und staatliche Reaktionen auf Kriminalität und Terrorismus zu Ungunsten des individuellen Datenschutzes verschoben hat. Zugleich wurden die Vorbehalte hinsichtlich des Schutzes der Privatsphäre und der Sicherheit als Haupthindernis für die Akzeptanz von e-Commerce-Angeboten identifiziert. Die Studie untersuchte insbesondere die Auswirkungen der neuen Kommunikationstechnologien, z. B. die „elektronischen Spuren", die man im Internet oder beim Telefonieren mit dem Handy hinterlässt und die für andere Zwecke als die Strafverfolgung missbraucht werden könnten.

In einer zweiten, gerade fertig gestellten Studie trägt die europäische Kommission der in Art. 12 der EG-Richtlinie zu elektronischen Signaturen geforderten Prüfung der „Durchführung dieser Richtlinie" Rechnung.

Der Prüfbereicht "The legal and market aspects of electronic signatures" kommt zu dem Ergebnis, dass die Richtlinie in fast allen Mitgliedsstaaten (sowie den Beitrittskandidaten) umgesetzt wurde, variierende Interpretationen einzelner Artikel jedoch zu teils großen Unterschieden in der Anwendung sowie der nationalen Gesetzgebung geführt haben. Er identifiziert eine Reihe von Problemfeldern, die auf EU-Ebene Beachtung finden sollten, um die gewünschte Harmonisierung elektronischer Signaturen zu erreichen. Stefan Kelm, Security Consultant bei Secorvo, war als Autor an der Erstellung dieser Studie beteiligt.

1.3 IT-Grundschutz kompakt

Am 18.09.2003 wurde vom Bundesamt für Sicherheit in der Informationstechnik (BSI) der „Leitfaden IT-Sicherheit" (IT-Grundschutz kompakt) publiziert (415 kB). In der 48-seitigen Broschüre werden die häufigsten Versäumnisse und die wichtigsten Sicherheitsmaßnahmen überschaubar und verständlich dargestellt. Ergänzt wird der Leitfaden durch eine Einführung zum IT-Grundschutzhandbuch sowie kurze Checklisten für die wichtigsten Bereiche.

1.4 Security Tools (Update)

Seit dem 01.10.2003 ist v2.5 beta 38 von Cain & Abel verfügbar. Das Multifunktionstool, welches viele Angriffsmöglichkeiten wie ARP-Spoofing und eine Reihe von Passwortcrackern enthält, bietet nun wie L0phtCrack die Möglichkeit, gesniffte SMB-Hashes direkt an den Passwortcracker zu übergeben. Dadurch können schwache Benutzerpasswörter bei NT 4.0 oder Windows 2000 im NTLM-Standard-Modus innerhalb von Stunden geknackt werden.

Der verbreitete Portscanner Nmap, der ständig weiterentwickelt wird, liegt seit dem 06.10.2003 in Version 3.48 vor und enthält nun über 650 Signaturen zur Erkennung von Diensten und Betriebssystemen.

1.5 Top 20 Security Bugs

Die von SANS in Zusammenarbeit mit internationalen Unternehmen erstellte und jährlich aktualisierte Liste der 20 häufigsten Sicherheitsschwächen unter Windows (10) und Unix/Linux (10) wurde am 08.10.2003 publiziert. An dieser Fassung haben das US-Department of Homeland Security sowie Sicherheitsbehörden aus Großbritannien und Kanada mitgewirkt.

1.6 Spam-Bounces – die Kehrseite der Medaille

Nicht nur Würmer à la Sobig verwenden gefälschte, aber real existierende E-Mail-Absender (vgl. Security News 8/2003), sondern auch immer mehr Spam-E-Mail-Versender segeln unter falscher Flagge. Da sich unter abertausenden Spam-Adressaten viele finden, die gar nicht existieren, gerade in Urlaub sind oder sich über die Spam-Mail beschwerden wollen, landen Abwesenheitsnotizen, Fehlermeldungen („Bounces“) und Beschwerden in der Mailbox des vermeintlichen Absenders – zumindest so lange, bis diese überquillt.

Am 09.10.2003 brachen die Mail-Server des zu QSC gehörenden Providers Ginko unter der Last solcher Spam-Bounces ein.

1.7 Fehler in OpenSSL

Am 30.09.2003 wurde eine mit hohem Risiko bewertete Schwachstelle im ASN.1-Parser publiziert, der sich in allen auf OpenSSL basierenden Implementierungen findet: Beim Einlesen manipulierter Zertifikate im Rahmen der SSL/TLS-Client-Authentifikation treten Pufferüberläufe auf, die einen Denial-of-Service Angriff auf SSL-Server ermöglichen. Ob auch die Ausführung von beliebigem Code möglich ist, ist noch unklar.

Besonders schwer wiegt der Fehler dadurch, dass die Überläufe auch dann auftreten, wenn ein bösartiger Client sein Zertifikat unverlangt sendet. Wer OpenSSL im Einsatz hat, sollte daher umgehend auf die entsprechend gesicherten Versionen 0.9.6k bzw. 0.9.7.c aktualisieren.

Die zu dieser Sicherheitslücke publizierten Advisories fördern nebenbei zu Tage, in wie vielen kommerziellen Produkten dieser Code enthalten ist. Die illustere Liste reicht von Cisco Routern und PIX Firewalls über den Apple Macintosh bis zu Novell.

OpenSSL ist nicht die einzige Open Source Crypto-Software, die aktuelle Sicherheitslücken vermeldet: Auch zu den beiden Secure-Shell Implementierungen LSH und OpenSSH wurden seit Mitte September mehrere Advisories publiziert.

1.8 Hacker stiehlt Spielequellcode

Üblicherweise erfährt die Öffentlichkeit wenig über erfolgreiche Einbrüche von Hackern und den angerichteten Schaden. In einem nun bekannt gewordenen Fall war dies anders: Ein Hacker, der möglicherweise eine Sicherheitslücke in Outlook nutzte, konnte um den 19.09.2003 Zugriff auf den Quellcode des noch unveröffentlichten zweiten Teils des populären Spiels Half-Life erlangen und verbreitete den Code anschließend im Internet.

Im Verlauf des vom Hersteller Valve Software bestätigten Vorfalls wurden von dem oder den Angreifern u. a. „Keystroke-Logger“, die per Software alle Tastendrücke des Benutzers aufzeichnen, auf Rechnern von Valve-Mitarbeitern installiert. Damit ein Spieler, der den internen Aufbau des Spiels kennt, keinen unfairen Vorteil daraus ziehen kann, müssen nun Teile von Half-Life 2 umgeschrieben werden. Dadurch wird sich das Erscheinen des Spiels über das für die Branche so wichtige Vorweihnachtsgeschäft hinaus verzögern.

Das Beispiel zeigt, dass die veröffentlichten Sicherheitsschwächen wichtiger Anwendungen (wie Outlook oder Internet Explorer) und Betriebssysteme keineswegs ein „theoretisches“ Problem darstellen, sondern zu erheblichen, wenn auch oft unveröffentlichten Schäden führen.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminar „IT-Security Management“ – buchbar als zweitägiges Intensiv- oder einwöchiges Grundlagenseminar (**03.-04.11.** bzw. **03.-07.11.2003**) – führt in Aufbau, Prozesse und Strukturen des Sicherheitsmanagements ein. Am Beispiel eines fiktiven Unternehmens werden Standards und rechtliche Rahmenbedingungen konkret.

Eine aktuelle „Standortbestimmung“ der IT-Sicherheit leistet das Seminar „IT-Sicherheit heute“ (**11.-13.11.2003**), das sich als inhaltliche Auffrischung und Einstieg in das Themengebiet eignet.

Nach den Würmer- und Virenattacken der vergangenen Monate aktueller denn je: Die sichere Konfiguration des Betriebssystems Windows (NT/2000/XP). Insider-Einblicke gewährt das Seminar „Inside Windows Security“ am **18.-19.11.2003**.

Hilfestellung für die Einführung von E-Mail-Verschlüsselung im Unternehmen und viele Tipps aus der Beratungspraxis bietet das Seminar E-Mail-Sicherheit am **25.-26.11.2003**.

2.2 “Anti-Spam-Symposium”

Mit einem „Anti-Spam-Symposium“ am **18.-19.11.2003** greift die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) die Diskussion des angemessenen Umgangs mit unerwünschten E-Mail-Nachrichten („Spam“) in Unternehmen auf. Namhafte Referenten werden diese Frage aus rechtlicher, technischer und organisatorischer Perspektive beleuchten. Das Symposium, für das Microsoft als Sponsor gewonnen werden konnte, richtet sich an alle mit Abwehrmaßnahmen gegen Spam befassten Verantwortlichen in Unternehmen und Behörden – IT-Leiter, Management, Techniker und Datenschutzbeauftragte (Heise-Ticker).

Programm und Anmeldung unter
http://www.anti-spam-symposium.de

3 Veranstaltungshinweise

Oktober 2003	
30.10.	„IT – Aber sicher!“ (KA-IT-Si, Karlsruhe)
November 2003	
03.-04.11.	IT-Security Management (Secorvo College, Karlsruhe)
03.-07.11.	Information Security Management von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
10.-11.11.	ZertiFA 2003 (Computas, Köln)
11.-13.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
18.-19.11.	Anti-Spam-Symposium (KA-IT-Si, Karlsruhe)
18.-19.11.	Inside Windows Security (Secorvo College, Karlsruhe)
24.-25.11.	IT Incident Management & Forensik (GI, Stuttgart)
25.-26.11.	E-Mail-Sicherheit (Secorvo College, Karlsruhe)
Dezember 2003	
03.-04.12.	PGP & Co. im Betrieb (Secorvo College, Karlsruhe)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

Herausgeber (V.i.S.d.P.): Dirk Fox

Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News“) an security-news@secorvo.de anfordern.

Wir freuen uns über Ihr konstruktiv-kritisches Feedback an
redaktion-security-news@secorvo.de