Secorvo Security News
Oktober 2002

Dirk Fox
Secorvo Security Consulting GmbH

Nr. 4, 1. Jhrg. 2002
Stand 13. Oktober 2002

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

Inhalt

Editorial: Was die 40 Räuber dem Präsidenten voraus hatten

Die Diskussion über Mindestanforderungen an Passworte ist mindestens so alt wie die 270ste Geschichte der 1001 märchenhaften Nächte des Kalifen von Bagdad aus dem 9. Jahrhundert. Darin knackt Ali Baba den Zugang zur Räuberhöhle durch Abhören des Passworts „Sesam, öffne dich!“. Immerhin ein Passwort mit 18 Zeichen, darunter zwei Sonderzeichen – zumindest in der deutschen Übersetzung.

Damit waren die Räuber weit fortschrittlicher als 1.100 Jahre später Bill Clinton, der als Präsident der Vereinigten Staaten Ende Juni 2000 das Bundesgesetz zur digitalen Signatur elektronisch unterzeichnete – und dabei den Namen seines Hundes Buddy als Passwort wählte. Offenbar hatte ihn niemand darauf hingewiesen, dass nicht nur ein Passwort mit lediglich fünf Stellen ohne Sonderzeichen viel zu leicht erratbar ist, sondern dass Namen von Familienangehörigen auch keinen Schutz vor Social Engineering bieten und daher grundsätzlich tabu sein sollten. Mit dem Ausplaudern des verwendeten Passworts vor laufenden Kameras outete er sich gänzlich als Negativbeispiel – Ali Baba musste sich immerhin in einem Baum verstecken, um das Passwort belauschen zu können.

Trotz der gestiegenen Sensibilität in Fragen der IT-Sicherheit sind Passworte bis heute nicht nur zentrales, sondern häufig auch wohlfeiles Objekt der Begierde. Dabei gibt es zahlreiche öffentlich verfügbare Empfehlungen zur Wahl guter Passworte, wie z. B. – pars pro toto – die des Datenschutzbeauftragten des Kantons Zürich:

http://www.cnlab.ch/pwcheck/empfehlungen.html

Einen Vorzug zumindest haben moderne Passwortsysteme gegenüber dem Schutzmechanismus der Räuberhöhle: Ein Passwort kann (und sollte regelmäßig) geändert werden – damit lässt sich der mögliche Schaden immerhin begrenzen.

1 Security News

1.1 Cyber Security – strategisch

Die amerikanische Regierung hat am 17.09.2002 den Entwurf eines Strategie-Papiers zur Verbesserung der Sicherheit des Internet („National Strategy To Secure Cyberspace“) veröffentlicht:

http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf (2,4 MB)

Die Veröffentlichung erfolgte nicht ganz freiwillig: Durch eine Indiskretion war eine Vorversion des Konzepts an die Öffentlichkeit geraten – und hatte einen Aufschrei der Internet-Zugangs-Provider ausgelöst: Sie sollten zur kostenlosen Verteilung von Schutzsoftware an private Kunden verpflichtet werden. Aus der nun für zwei Monate zur öffentlichen Kommentierung freigegebenen Fassung wurden alle „Kanten“ herausgefeilt. Sie hat daher eher den Charakter einer Empfehlungssammlung denn den eines wirksamen Maßnahmenpapiers.

1.2 Zeit der Security Surveys

In unübersichtlichen Zeiten schlägt die Stunde der Studien. Zahlreiche Security Surveys bieten derzeit Einschätzungen der Bedrohungslage, des Verbreitungsgrads von Sicherheitslösungen und Abschätzungen der Budgets für IT-Sicherheit.

Die Repräsentativität der einzelnen Erhebungen ist allerdings sehr unterschiedlich. Und auch die Ergebnisse klaffen zum Teil stark auseinander. Die konkreten Zahlen erscheinen daher wenig verlässlich. Aussagekraft haben eher Studien übergreifende Trends. Davon sind einige wenig überraschend, wie z. B. die nach wie vor hohe Bedeutung der Bedrohung durch Viren.

Eine Entwicklung ist jedoch bemerkenswert: Der Anteil externer Attacken hat erheblich zugenommen – und übertrifft in einigen Befragungen erstmals den der Insiderangriffe. Offen bleibt, ob dies tatsächlich auf eine geänderte Bedrohungslage hinweist – oder eher Resultat einer verbesserten Protokollierung ist.

Hier eine Auswahl aktueller Studien:

Global Information Security Survey (März 2002), Ernst & Young, 459 Teilnehmer (weltweit):
http://www.ey.com.pl/gcrdownload/GISS_2002.pdf (2 MB)

KES/KPMG-Studie (Frühjahr 2002), 260 Teilnehmer (D):
http://www.kes.info/studie2002/ (mehrteilig)

CSI/FBI Computer Crime and Security Survey (April 2002); 503 Teilnehmer (US):
http://www.gocsi.com/pdfs/fbi/FBI2002.pdf (2,2 MB)

Information Security Breaches Survey 2002 (April 2002) von PWC und dem britischen dti; 1000 Teilnehmer (UK):
https://www.security-survey.gov.uk/isbs2002_detailedreport.pdf (1 MB)

Australian Computer Crime and Security Survey (Mai 2002) von AusCert und Deloitte Touche Tohmatsu; 95 Teilnehmer:
http://www.auscert.org.au/Information/Auscert_info/2002cs.pdf (347 kB)

Umfrage „IT-Sicherheit 2002“ (Juni 2002) von silicon.de; 483 Teilnehmer (D):
http://www.sicherheit-im-internet.de/download/IT-Sicherheit.pdf (428 kB)

BSA Cyber Security Survey (Juli 2002), BSA, 395 Teilnehmer (US):
http://www.bsa.org/security/resources/2002-07-22.131.pdf (315 kB)

Information Security Magazine Survey (September 2002), 215 Teilnehmer (US):
http://www.infosecuritymag.com/2002/sep/2002survey.pdf (267 kB)

IT-Security Studie (September 2002) von InformationWeek, 8.188 Teilnehmer weltweit (828 aus D):
http://www.informationweek.de/studien/stud_it_security2002.ppt (8,5 MB)

1.3 CERT-Verbund

Mit der Gründung eines CERT Verbunds durch sechs deutsche Computer Emergency Response Teams – CERT-Bund (BSI), DFN-CERT, S-CERT (Sparkassenorganisation), Siemens-CERT, BCRS (IBM) und Telekom-CERT – gibt es seit dem 01.09.2002 ein Koordinationsgremium für übergreifende CERT-Aktivitäten in Deutschland. Durch eine Intensivierung der Zusammenarbeit sollen u. a. die Reaktionszeiten bei sicherheitsrelevanten Ereignissen verkürzt werden:

http://www.bmi.bund.de/dokumente/Pressemitteilung/ix_90395.htm

1.4 RC5-64 Contest gelöst

Am 28.01.1997 startete RSA Security Inc. einen groß angelegten „Crypto Contest“: 13 „Krypto-Rätsel“, mit unterschiedlich langen (40 bis 128 bit) Schlüsseln verschlüsselte Texte (einmal DES, zwölf mal RC5), wurden zur Kryptoanalyse freigegeben:

http://www.rsasecurity.com/rsalabs/challenges/secretkey/secret-key.html

Die ersten vier Rätsel (RC5-40/-48/-56 und DES-56) wurden noch im Jahr 1997 gelöst. Seitdem war es ruhig um den Contest geworden – bis nun die mit einem Preis von 10.000 US$ dotierte RC5-64-Verschlüsselung gebrochen wurde: von 331.252 über das Internet verbundenen Rechnern, die in vier Jahren 15.769.938.165.961.326.592 verschiedene Schlüssel – 47% des Schlüsselraums – systematisch ausprobiert hatten („Brute Force“):

http://www.distributed.net/rc5

Zuletzt erreichten die vernetzten Rechner einen Durchsatz von über 127 Milliarden Schlüsseln pro Sekunde. Die richtige Lösung wurde schon am 14.07.2002 entdeckt; durch einen Softwarefehler wurde die Entschlüsselung – und damit der Beleg für die faktische Unsicherheit von 64 bit langen symmetrischen Schlüsseln – aber erst am 27.09. 2002 bekannt.

1.5 Würmerplage

Zwei Würmer mit dramatischen Auswirkungen halten derzeit Administratoren in Atem:

Der Wurm „Slapper“ bzw. „bugtraq.c“ nutzt einen bekannten Fehler im SSLv2-Handshake des OpenSSL-Moduls (siehe Secorvo Security News 2/2002), um auf einem Linux-Server einen Buffer Overflow zu erzeugen. Dann kopiert er das Programm „bugtraq.c“ auf den kompromittierten Server und übersetzt es mit gcc. Dieses schaltet einen Port zur Nutzung des Servers für verteilte DoS-Angriffe frei und sucht dann nach weiteren Linux-Servern. Betroffen sind Linux-Systeme mit Apache und mod_ssl. Schutz bietet die Installation der OpenSSL-Versionen ab 0.9.6e:

http://www.openssl.org

Derweil leidet die Windows-Welt unter dem Wurm „Bugbear“, der sich über E-Mail-Anhänge mit zufälligem Dateinamen und wechselndem Betreff sowie Netzlaufwerke verteilt. Er nutzt eine Schwachstelle im IE 5.01 und 5.5, durch die Attachments von HTML-E-Mails beim Öffnen ausgeführt werden. Anschließend versucht er, installierte Virenscanner und Sicherheitsprogramme zu deaktivieren. Er öffnet eine Hintertür auf Port 36794, über die ein entferntes System beliebige Kommandos und Programme ausführen kann, protokolliert alle Tastatureingaben und versendet sie per E-Mail an ein externes System:

http://cert.uni-stuttgart.de/ticker/article.php?mid=974

2 Secorvo News

2.1 Secorvo College aktuell

„Security Awareness“ wird zunehmend zum zentralen Thema in Unternehmen und Behörden. Mit dem Seminar „Defense Lab“ bietet Secorvo College am 03.-04.12.2002 in Zusammenarbeit mit der Schweizer Firma Compass Security Network Computing erstmals ein „Online-Hacking“-Seminar, in

dem die Vorgehensweise von Angreifern erläutert und zahlreiche typische Angriffe life vorgeführt werden:

http://www.secorvo.de/college

2.2 Browser-Konfiguration

Dass von aktiven Komponenten auf Webseiten erhebliche Bedrohungen ausgehen können, ist keine Neuigkeit. Viele Unternehmen haben inzwischen zentrale Filtersysteme eingerichtet, die das Eindringen bösartigen Codes über Webseiten verhindern. Aber nicht jeder PC nimmt hinter einer gut konfigurierten Firewall Deckung: Mobile Systeme mit Internet-Zugang, die sich nicht nur bei Außendienstmitarbeitern großer Beliebtheit erfreuen, sind oft unzureichend geschützt. Denn hier hängt alles an der Konfiguration des Browsers (oder der „Personal Firewall“).

Eine anschauliche Darstellung von Bedrohungen durch aktive Komponenten und Konfigurationshinweise für Microsofts Internet Explorer bietet das von Secorvo in Zusammenarbeit mit Microsoft Deutschland entwickelte Video „Safer Surfen“, das Mitte Oktober fertiggestellt wird. Vorbestellung:

http://www.secorvo.de/video

Für Surfer, die sich ihrer Sache nicht sicher sind, hat der Datenschutzbeauftragte des Kantons Zürich zusammen mit der Hochschule für Technik in Rapperswil (CH) einen Online-Sicherheitscheck für Browser entwickelt, den seit Ende März 2001 schon mehr als 400.000 Besucher genutzt haben:

http://152.96.120.35/

Nach Abschluss des vierstufigen Tests gelangen Sie zur statistischen Auswertung, die Erschreckendes offenbart: 69-85% aller getesteten Systeme haben Scriptsprachen (VBScript, JScript, JavaScript) freigeschaltet, und 25,5% erlauben die Ausführung von signierten ActiveX-Komponenten. Obwohl die Test-Teilnehmer sicher für Datensicherheit sensibilisiert waren: ca. 3.600 Systeme (1,5%) waren für ActiveX ein offenes Scheunentor, und auf etwa 4.800 Rechnern (1,6%) waren freigegebene Laufwerke sichtbar.

3 Veranstaltungshinweise

Oktober 2002	
24.10.	„Wie gut schwimmt Ihr Server?“ (KA-IT-Si, Karlsruhe)
28.-29.10.	IT-Sicherheit für KMU (VDI/IHK Köln)
November 2002	
05.-07.11.	IT-Sicherheit heute (Secorvo College)
07.-08.11.	Praxis des betrieblichen DSB (Euroforum, Berlin)
12.-13.11.	Inside Windows Security (Secorvo College)
19.-20.11.	Lotus Notes Security (Secorvo College)
20.-22.11.	IT-Security- und Riskmanagement (ZfU, Zürich)
26.-27.11.	Sichere E-Mail-Kommunikation (Secorvo College)
Dezember 2002	
02.-03.12.	IsSec 2002 (Computas, Berlin)
03.-04.12.	Defense Lab (Live Hacking) (Secorvo College)

Aktuelle Veranstaltungsübersicht:
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 automatische Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail an security-news@secorvo.de (Subject: „Subscribe Security News“) anfordern.