Secorvo Security News
Januar 2005

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

Nr. 1, 4. Jhrg. 2005
Stand 28. Januar 2005

ISSN 1613-4311

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

Inhalt

Editorial: Von Hasen und Igeln

Sie erinnern sich? Es war einmal an einem Sonntagmorgen im Herbst... ein Märchen der Gebrüder Grimm, erzählt an Ihrem Kinderbett, oder dem Ihrer Kinder.

Haben Sie nicht auch geschmunzelt über die List des Igels, der den Wettlauf gegen den körperlich weit überlegenen Hasen gewinnt, indem er sich in die Ackerfurche duckt und abwechselnd mit seiner Frau „Ich bin schon da!“ ruft, sobald der Hase das Ziel vermeintlich als Erster erreicht?

Zu denken hat mir damals gegeben, dass mein Großvater zu sagen pflegte: "Wahr muss die Geschichte sein, mein Sohn, sonst könnte man sie ja nicht erzählen.“

Und tatsächlich, da stellt sich, Jahrzehnte später, mit Blick auf das wirkliche Leben ein Déjà-vu ein. Der IT-Nutzer ruft: „Ich brauche einen sicheren Internetzugang“ – und Sie starten, installieren Firewall, Virenscanner und Spamfilter. Sie sind noch nicht fertig, da ruft er schon: „Ich brauche einen sicheren Laptop“ – und Sie sorgen für einen VPN-Tunnel, Personal Firewall und Festplattenverschlüsselung. Es ist noch nicht alles lauffähig, da ruft er bereits: „Meine E-Mails will ich auf meinem BlackBerry lesen“ – verschlüsselt natürlich. Und Sie rennen los und...

Eigentümlich nur, dass mir dabei meine kindliche Sympathie für den ob seiner krummen Beine verhöhnten und sich listig rächenden Igel ein wenig abhanden gekommen ist. Spielt nicht der Hase fair, indem er sich an die Regeln hält und alles gibt? Und ist nicht in Wahrheit der Igel grausam, nicht der erst hochnäsige Hase?

Auch aus diesem Märchen lässt sich also etwas fürs Leben lernen:

Erstens: Wenn die Igel nicht gestorben sind, leben sie noch heute. Zweitens: Eine höhere Geschwindigkeit löst nicht das Problem, sondern verkürzt die Lebenserwartung des Hasen.

Und drittens: Wer nicht auf dem Feld verenden möchte, sollte sich gelegentlich auch einmal in die Ackerfurche ducken.

1 Security News

1.1 Aktualisiertes IT-Grundschutzhandbuch des BSI

Am 10.01.2005 wurde eine aktualisierte Version des Grundschutzhandbuchs auf den Webseiten des BSI im PDF-Format zum Download bereit gestellt. Die HTML-Version soll in Kürze folgen. Neu hinzu gekommen sind die Bausteine „Router und Switches“, „S/390 und zSeries“ sowie „PDA“; der Baustein Sicherheitsgateway (Firewall) wurde überarbeitet. Das Grundschutzhandbuch deckt damit weitere wichtige Systeme ab – wird damit aber zugleich immer umfangreicher und komplexer. Daher wird über eine Ersetzung der inzwischen eher untertriebenen Bezeichnung „Grund“-Schutz diskutiert.

Fakt ist: Wer nach IT-Grundschutz zertifiziert ist, hat in der Regel ein hohes IT-Sicherheitsniveau erreicht. Kombiniert mit adäquatem Sicherheitsmanagement und ergänzenden Maßnahmen für besonders gefährdete Systeme sorgt Grundschutz für einen umfassenden Schutz der Unternehmens-IT.

1.2 Anti-Spyware Tool

Unter den am 11.01.2005 von Microsoft veröffentlichten Sicherheitspatches für XP findet sich die Beta-Version eines Anti-Spyware-Tools (MAS). Es erlaubt sowohl eine kontinuierliche als auch eine Anlass bezogene Untersuchung des PC auf verdächtige Programme.

Durch den Kauf der Firma Giant Ende 2004 verfügt Microsoft nun nicht nur über spezielles Spyware-Know-How, sondern auch über ein Programm, das grundsätzlich als umfassende Schädlingserkennungs-Engine ausgelegt ist: Es untersucht Registry und Systembibliotheken auf bekannte Spyware, prüft ausgewählte Konfigurationseinstellungen und arbeitet mit einer aktualisierbaren Signaturdatenbank – das Grundgerüst eines jeden Virenschutzprogramms.

Daher sprießen bereits die Gerüchte, Microsoft wolle doch noch in den Virenschutz-Markt einsteigen. Genährt wird dieser Verdacht dadurch, dass die genannten Sicherheitspatches – etwas versteckt – ein zweites Tool enthalten: ein „Malicious Software Removal Tool“, das nicht allein die in der Vergangenheit für ausgewählte Viren bereit gestellten Deinstallationstools zusammenfasst, sondern zusätzlich im Hintergrund versucht, ein erneutes Auftauchen dieser Viren zu erkennen.

1.3 Anfänger für Office...

...statt Office für Anfänger: In einem am 10.01.2005 bei der International Association for Cryptologic Research eingereichten Papier enthüllt ein Forscher aus Singapur, dass Microsoft bei der Verschlüsselung von Dokumenten in Office dieselbe Schlüsselfolge mehrfach verwendet. Dies gilt unter Kryptologen als typischer Anfängerfehler und sorgt dafür, dass Dokumente trotz starker 128-Bit RC4-Verschlüsselung unter Umständen leicht entschlüsselt werden können.

Bei Motoren gilt die alte Weisheit „Hubraum ist durch nichts zu ersetzen, außer durch mehr Hubraum!“. Bei Entwurf und Review eines Sicherheitskonzepts gilt dies analog – für langjährige Erfahrung.

1.4 DoS gegen VoIP bei IOS

Wie nicht anders zu erwarten, weisen auch moderne Voice-over-IP Systeme Schwachstellen auf. Da es sich dabei „nur“ um IT-Systeme handelt, trifft man auch hier auf bekannte Lücken durch fehlerhafte Implementierungen und Protokollschwächen. Jüngstes Beispiel ist ein von Cisco am 19.01.2005 veröffentlichtes Security Advisory: Bei Telephony Service (ITS), Call-Manager Express (CME) und Survivable Remote Site Telephony (SRST) bestimmter IOS-Versionen kann mit präparierten Nachrichten ein Reboot des Systems ausgelöst werden. Per „Dauerbeschuss“ lässt sich so ein ausgewachsener Denial-of-Service-Angriff durchführen. Es wird empfohlen, die aktuellen Updates baldigst einzuspielen.

1.5 Microsoft lässt Patches intensiver testen

Wie die Zeitschrift eWeek am 12.01.2005 berichtete, startet Microsoft ein „Security Update Validation Program“: Zukünftig sollen Sicherheitspatches nicht nur von Microsoft selbst und wenigen Großkunden getestet, sondern an weitere externe Beta-Tester verteilt werden. Hierdurch sollen in der Vergangenheit aufgetretene Problemfälle vermieden und die Qualität der Patches – und damit auch die Sicherheit – gesteigert werden. Das Programm verdient weitere Beobachtung; der Erfolg wird sich an den bei künftigen Patches auftretenden Problemen erweisen müssen.

1.6 Apple Security Update

Nicht nur Windows braucht Patch Management: Am 25.01.2005 veröffentlichte Apple das erste Security Update des Jahres für das hauseigene Betriebssystem Mac OS X.

Dabei wurde zugleich die vorher Datumsbasierte Bezeichnung der Security Updates auf eine laufende Nummer (2005-001) umgestellt – eine ebenso einfache wie wirkungsvolle Maßnahme, um Anwendern die Prüfung zu erleichtern, ob alle Updates bereits eingespielt wurden.

1.7 Einheitliche Sperrung

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) hat am 21.12.2004 dem Sperr e. V. – Verein zur Förderung der Sicherheit in der Informationsgesellschaft – die bundeseinheitliche Telefonnummer 116 116 für die Sperrung von EC-, Kredit- Handy-, Krankenkassen- und Kundenkarten zugeteilt. Die Rufnummer muss 180 Tage ab Zuteilung, also ab Anfang Juli 2005 (im Inland entgeltfrei) erreichbar sein.

1.8 Anti-Phishing

Am 20.01.2005 veröffentlichte die Anti-Phishing Workung Group einen Report über die erkannten Phishing-Aktivitäten im Dezember 2004. Demnach werden die meisten der gefälschten Server zum ab„phish“en von Passwörtern nicht, wie man vielleicht erwarten könnte, in Osteuropa, Fernost oder Offshore-Steuerparadiesen installiert, sondern in den USA.

Diese Server waren durchschnittlich nur 5,9 Tage am Netz – daher ist bei Phishing-Attacken vor allem die erste Woche nach deren Auftreten kritisch. Daraus erklärt sich auch, dass einschlägige E-Mails oft an überdeutlichen Hinweisen auf ihre vorgeblich besondere Dringlichkeit zu erkennen sind.

Einen anderen Weg der Phishing-Detektion gehen, wie am 21.01.2005 gemeldet wurde, die Entwickler des Mozilla Mail-Clients Thunderbird: Sie wollen den Anwender warnen, wenn er eine in der Mail enthaltene URL anklickt, bei der z. B. anstelle des im Text angezeigten Hostnamens eine IP-Adresse hinterlegt ist. Umstritten ist jedoch, wie diese Warnung einem Endanwender verständlich vermittelt werden kann...

1.9 12. DFN-CERT Workshop

Die wichtigste deutsche Security-Konferenz wirft wieder einmal ihre langen Schatten voraus: Bereits zum zwölften Mal wird am 2. und 3. März im Kongresszentrum (CCH) in Hamburg der zweitägige DFN-CERT/ PCA-Workshop stattfinden. Das auch diesmal sehr viel versprechende Programm dürfte auch 2005 wieder deutlich mehr als 300 interessierte Teilnehmer aus Forschung, Unternehmen und Behörden anlocken und zum Diskutieren anregen.

Als eingeladener Sprecher konnte Lance Spitzner gewonnen werden, der vor allem für das Projekt „Honeynet“ verantwortlich zeichnet. Auch die anderen Vorträge versprechen interessante Themen auf hohem Niveau.

2 Secorvo News

2.1 Secorvo College aktuell

Secorvo College startet in das Jahr 2005 nicht nur mit einem um vier neue Seminare

erweiterten Angebot, sondern auch mit verkürzten Reisezeiten für Sie: Das neue Domizil von Secorvo liegt in Fußweite vom Karlsruher Hauptbahnhof (300 m) und fünf Autominuten von der A5.

Die Seminare im Februar geben einen Überblick über die IT-Sicherheit heute und vertiefen das zunehmend wichtige Thema Information Security Management (Anmeldung).

http://www.secorvo.de/college

2.2 Forensik Symposium

Secorvo veranstaltet im Rahmen der Karlsruher IT-Sicherheitsinitiative und in Kooperation mit Viccon am 01.-02.03.2005 das Computer Forensik Symposium 2005. Die systematische „virtuelle Spurensicherung" hat in den beiden vergangenen Jahren mit der Zunahme erfolgreicher Angriffe auf die IT-Infrastrukturen von Unternehmen spürbar an Bedeutung gewonnen. Das Programm des Symposiums beleuchtet das Thema erstmals von allen Seiten – aus der Perspektive der Strafverfolgung, der Unternehmenspraxis, der Technik und der „best practices".

2.3 DuD 2005

Inzwischen steht das Programm der diesjährigen siebten Konferenz „Datenschutz und Datensicherheit – DuD 2005", konzipiert und geleitet von den Herausgebern der Fachzeitschrift DuD. Sie findet am 18.-19.04.2005 in alter Tradition im Berliner Dorint-Hotel Schweizerhof statt; eine rechtzeitige Anmeldung wird empfohlen (die Teilnehmerzahl ist auf 100 begrenzt).

2.4 Teamverstärkung

Seit Mitte Januar ergänzt Ralph Wiedemann das Secorvo-Team: Er bringt mehrjährige Berufserfahrung als IT-Sicherheitsverantwortlicher, Berater und Projektleiter für IT-Security mit und verstärkt unser Know-How rund um Firewalls, PKI-basierte VPNs, Security-Audits, Intrusion Detection und Security Policies.

3 Veranstaltungshinweise

Februar 2005	
15.-17.02.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
21.-22.02.	IT-Security Management (Secorvo College, Karlsruhe)
21.-25.02.	Information Security Management (Secorvo College, Karlsruhe)
März 2005	
01.-02.03.	Computer Forensik Symposium 2005 (KA-IT-Si, Karlsruhe)
02.03.	Datenschutz kompakt (Secorvo College, Karlsruhe)
02.-03.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
15.-16.03.	D-A-CH Security 2005 (GI/OCG/ BITKOM/SI/TTT, TU Darmstadt)
April 2005	
05.-07.04.	Sichere E-Mail-Kommunikation (Secorvo College, Karlsruhe)
05.-08.04.	Sicherheit 2005 (GI, Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)

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

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 225 171-0
Fax +49 721 225 171-100

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

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