secorvo
security consulting

Secorvo Security News

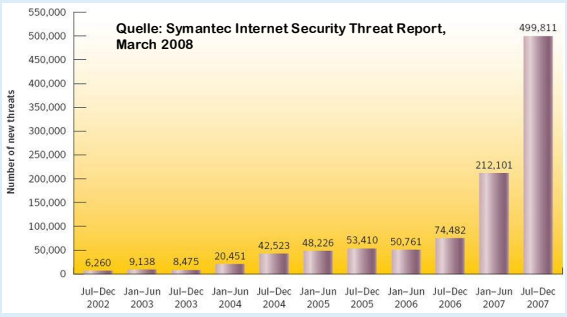
Juli 2008

Editorial: Geburtstagstorte

Wer Kinder hat, kennt Pettersson und Findus – den alten, schrulligen, liebenswerten Bauern mit seinem quirligen sprechenden Kater in grüner Hose, detailreich gezeichnet von Sven Nordqvist. „Eine Geburtstagstorte für die Katze“ heißt das 1984 erschienene erste Bilderbuch der Kultserie. Die Geschichte ist fix erzählt: Findus beschließt, Geburtstag zu haben – denn dann gibt es Pfannkuchentorte. Das ist jedoch leichter gesagt als getan: Das Mehl ist ausgegangen, und das Fahrrad hat einen Platten. Pettersson muss es reparieren, bevor er zum Einkaufen fahren kann – das Werkzeug aber liegt im verschlossenen Schuppen, und den Schlüssel entdeckt Findus im Brunnen. Um ihn herauszufischen braucht er die Angel vom Dachboden, aber an der Leiter lehnt ein schlafender Stier. Also muss Findus mit einer Gardine den Matador geben, reißt aber dabei den Eierkorb um.

Natürlich kommt der Kater doch noch zu seiner Geburtstagstorte. Aber das war jedenfalls für meine Kinder ganz unwichtig – gebannt verfolgten sie die immer neuen Widrigkeiten und deren kreative Beseitigung. Der Umweg war das Ziel, und die Torte bestenfalls die Belohnung für die erfolgreiche Problemlösung.

Sehr ähnlich müssen die Autoren von Malware empfinden. Wie anders ist zu erklären, dass sie sich weder von immer besseren Schutzmaßnahmen noch von schärferen Strafgesetzen abschrecken lassen? Statt dessen ersinnen sie raffiniertere Angriffsmethoden. Offenbar spornt der Widerstand an, das belegen die Zahlen. Und dahinter steht heute meist ein Investor, der auf die Torte scharf ist.



Inhalt

secorvo
security consulting

Security News

BSI-Krypto-Richtlinie

Seit Inkrafttreten des deutschen Signaturgesetzes vor mehr als 10 Jahren erstellt das BSI jährlich eine aktuelle Übersicht geeigneter kryptographischer Algorithmen und Schlüssellängen für digitale Signaturen. Verschlüsselungsverfahren spielen darin naturgemäß keine Rolle – gleichwohl sind sie in der Praxis viel verbreiteter als digitale Signaturen.

Mit der Veröffentlichung einer technischen Richtlinie „Kryptographische Verfahren: Algorithmen und Schlüssellängen“ (TR 02102) hat das BSI am 20.06. 2008 nun auch bei Verschlüsselungsverfahren, Authentisierungsmechanismen, Zufallszahlengeneratoren und Schlüsselvereinbarungsprotokollen Farbe bekannt. Eine wertvolle Orientierung für die Praxis.

Survival of the Fittest

Am 14.07.2008 veröffentlichte Torsten Holz in seinem Blog die Ergebnisse einer 12monatigen Honeynetanalyse zur Überlebenszeit ungepatchter IT-Systeme. Untersucht wurde die Dauer einer erfolgreichen Kompromittierung durch autonome Malware, die alte, lange bekannte Schwachstellen ausnutzen. Ergebnis: Im Schnitt überlebt ein System ca. 12 Minuten, etwas länger als die vom Internet Storm Center gemessenen knapp fünf Minuten.

Die Analyse, die auf den Vorarbeiten von Laura Itzel aufbaut, weist eine erhebliche Abhängigkeit der Überlebenszeit vom jeweiligen Internet Service Provider nach: ISPs, die bevorzugt von Malware genutzte Ports sperren, erhöhen die Überlebenszeit angeschlossener Systeme um ein Vielfaches. Angesichts des deutlich größeren Zeitfensters zwischen Bekanntwerden einer Schwachstelle und Verfügbarkeit des Patches („Window of Exposure“) erscheint es jedoch in keinem Fall angeraten, eine Internet-Verbindung ohne gut konfigurierte Personal Firewall aufzubauen.

Schlecht versteckt

Dass Blicke über den Tellerrand auch in der Kryptographie wichtig sind, belegt eine Arbeit, die Forscher der University of Washington zusammen mit Bruce Schneier am 29.07.2008 auf einem USENIX Workshop vorgestellt haben. Darin untersuchten sie die Sicherheit von „Deniable File Systems“, mit deren Hilfe die Existenz verschlüsselter Daten verschleiert werden soll – beispielsweise mit „Hidden Volumes“ des Verschlüsselungstools TrueCrypt. Aber auch versteckte Dateisysteme hinterlassen im Betriebssystem unvermeidlich Spuren, wenn sie aktiviert werden, z. B. als kürzlich geöffnete „Recent Items“. Im schlimmsten Fall findet sich, lange nach der Deaktivierung des „Hidden Volumes“, Klartext-Inhalt einer versteckten Datei im Cache von Google-Desktop.

Was des einen Leid, ist des anderen Freud’ – die Forensiker reiben sich die Hände. Einige der aufgedeckten Probleme wurden in der am 06.07.2008 erschienenen Version 6 von TrueCrypt behoben.

Evilgrade

Am 28.07.2008 veröffentlichte Francisco Amato das Framework Evilgrade. Der Schadsoftware-Baukasten nutzt als Verbreitungsmechanismus verbreitete Updatemechanismen und tarnt sich als automatischer Patch. Derzeit werden u.a. Java Plugins, Winzip, Winamp und iTunes simuliert; Schadcode kann für beliebige Zielplattformen ergänzt werden. Die Integration der am 08.07.2008 von Dan Kaminsky publizierten DNS Cache Poisoning Variante in das Metasploit-Attackframework vereinfacht die Anwendbarkeit von Evilgrade erheblich – und macht es sehr gefährlich: Fast alle DNS-Server waren bzw. sind ohne aktuelle Updates von dieser Schwäche betroffen. Wer nicht Teil des Problems sein möchte, sollte schnell patchen.

CrypTool 1.4.2x

Fast genau ein Jahr nach der Veröffentlichung von Version 1.4.10 ist am 11.07.2008 CrypTool als neues Release 1.4.21 erschienen. Neben vielen kleinen Korrekturen und akribischer Detailpflege an Bedienungsfreundlichkeit und Dokumentation wurden der Passwort-Qualitätsmesser optimiert und die Hashfunktionenfamilie SHA-2 integriert. Der Passwort-Generator erzeugt zufällige Passworte aus einem voreinstellbaren Alphabet – auch für WLANs.

Besonders erwähnenswert ist die jüngste Auszeichnung des Open Source Projekts: In einer Festveranstaltung wurde CrypTool am 22.07.2008 an der Uni Siegen im Rahmen der Kampagne „Deutschland Land der Ideen“ als „Ausgewählter Ort 2008“ ausgezeichnet.

BSI-Standards 2.0

Am 23.06.2008 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die zweite Auflage der überarbeiteten BSI-Standards 100-1 „Managementsysteme für Informationssicherheit“, 100-2 „IT-Grundschutz-Vorgehensweise“ und 100-3 „Risikoanalyse auf Basis von IT-Grundschutz“ veröffentlicht. Diese drei Standards bilden die Grundlage für den nach ISO 27001 ausgerichteten IT-Grundschutz. Die Neuauflage verschiebt den Blickwinkel von der reinen IT-Sicherheit zur Informationssicherheit; außerdem wurden die Standards um Datenschutzaspekte erweitert. Und schließlich wurde die

Fortschreibung der relevanten ISO-Standards der 2700x-Reihe berücksichtigt. Der neue BSI-Standard 100-4 zum Notfall-Management liegt nach wie vor nur als Entwurf vor.

Bluetooth Security

Zwar ist Bluetooth schon lange keine neue Technik mehr – kaum ein IT-Gerät, das etwas auf sich hält, kommt noch ohne daher. Und obwohl Security-Mechanismen und potentielle Schwachstellen schon lange dokumentiert sind, kommt es immer wieder zu fehlerhaften Implementierungen – Handys, die sich via Bluetooth Malware einfangen oder ferngesteuert werden können, oder Headsets, die aus der Ferne als Überwachungsmikrofon missbraucht werden können. Mit den 2004 und 2005 entwickelten Tools der trifinity-Gruppe – darunter Bluebug, Bluesnarf, Blueprint, Bluedump und Car Whisperer – ist das bei betroffenen Systemen ein Kinderspiel.

Nun hat offenbar auch das US-amerikanische NIST gemerkt, dass hier ein reales Risiko steckt und am 09.07.2008 einen Guide to Bluetooth Security (Draft SP 800-121) publiziert – mit der Bitte um Kommentierung bis 22.08.2008. Eine nette Urlaubslektüre ...

Link-Prefetching im Firefox

Nicht neu, aber nicht überall bekannt: Im Mozilla-Browser Firefox ist die Funktion Link-Prefetching in den Voreinstellungen aktiviert. Webseiten, die diese Funktion zum Einbinden von Links verwenden, sorgen dafür, dass die Inhalte der Links schon im Voraus geladen werden, ohne dass der Nutzer den Link angeklickt hat – in der Regel merkt er davon nicht einmal etwas.

Dafür liegt der möglicherweise rechtswidrige Inhalt der verlinkten Seite im Cache. Auch aus Sicherheitsperspektive ist diese Funktion nicht unbedenklich: Da sich Trojaner angesichts immer wirksamerer Spam- und Virenscanner in wachsendem Umfang über präparierte Webseiten statt per E-Mail verbreiten, können Angreifer Prefetching-Links auf eine einzige mit Schadcode versehene Webseite auf vielen unzureichend geschützten Seiten Dritter verstecken und so zahlreiche Systeme unbemerkt infizieren. Vorteil für den Angreifer: Schadcode-Updates muss er nur auf einer Webseite einspielen, und zur Spurenverwischung genügt die Entfernung genau dieses Codes. Abhilfe ist jedoch einfach: Zum Deaktivieren muss unter der URL „about:config“ der Wert des Parameters „network.prefetch-next“ durch Anklicken von true auf false gesetzt werden.

WAF-Pflicht

Die Anforderungen des Payment Card Industry (PCI) Data Security Standard V.1.1 vom 15.04.2008 an den Schutz von Web-Applikationen (Abschnitt 6.6) sind seit dem 30.06.2008 keine Empfehlung mehr, sondern eine verbindliche Vorgabe: Code-Reviews, eine automatisierte Schwachstellen-Analyse und die Nutzung von Web Application Firewalls (WAF) sind nunmehr Pflicht. Ein ergänzendes Dokument des PCI Security Standards Council erläutert die Anforderungen stichwortartig auf wenigen Seiten – für einige Anbieter sicher eine Herausforderung.

Secorvo News

Secorvo College aktuell

Nach der Sommerpause startet das Programm von Secorvo College am **08.–12.09.2008** mit einer T.I.S.P.-Schulung in das zweite Halbjahr – gefolgt von einer komplett unabhängigen Zertifikats-Prüfung durch iSQI am 13.09.2008 in den Räumen von Secorvo. Es folgt ein Klassiker in aktuellem Gewand: PKI – Grundlagen, Vertiefung, Realisierung am **23.–25.09. 2008** – baldige Anmeldung empfohlen.

Schon jetzt möchten wir Sie auf unser Forensik-Seminar vom **11.–13.11.2008** hinweisen. Die „Premiere“ im Juli war ausgebucht – und wurde von den Teilnehmern euphorisch gelobt („Mit dem Seminar hat sich Secorvo selbst übertroffen. (...) Ich kann jedem, der mit IT-Security zu tun hat, dieses Seminar nur wärmstens empfehlen. Drei Tage voller Information, Spannung, Überraschungen, Aha-Effekte und optimaler Mischung aus Theorie und Praxis.“ – Matthias Grund, Siemens AG).

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

Symposium Wirtschaftsspionage

Schutzmassnahmen gegen die ungezielte Bedrohung durch Schadsoftware und Hacker sind bei Unternehmen heute eine Selbstverständlichkeit. Seit etwa zwei Jahren belegen Studien jedoch einen unheilvollen Trend: Im Schatten wachsender Spam- und Trojaner-Wellen nehmen gezielte Spionageattacken zu – nicht nur unter Nutzung technischer Hilfsmittel.

Das "Symposium Wirtschaftsspionage" von Econo und Secorvo wird sich am **03.09.2008** diesem Thema widmen. Ulf Tietge, Chefredakteur von Econo, wird das Symposium moderieren, auf dem sowohl Fachexperten (u. a. Dr. Udo Ulfkotte und Hans Schlumpberger vom Landesamt für Verfassungsschutz BaWü) als auch Unternehmen die tatsächliche Bedrohungslage analysieren und ihre Schutzmaßnahmen vorstellen (vollständiges Programm, Online-Anmeldung und Anfahrtskizze).

Veranstaltungshinweise

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

August 2008	
17.-21.08.	Crypto 2008 (IACR, Santa Barbara/US)
September 2008	
03.09.	Symposium Wirtschaftsspionage (Secorvo, Ettlingen)
08.-12.09.	T.I.S.P.-Schulung (Secorvo College)
23.-26.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
23.-25.09.	IMF 2008: 4th International Conference on IT-Incident Management & IT-Forensics (GI, Mannheim)
Oktober 2008	
07.-09.10.	ISSE 2008 (EEMA/TeleTrusT, Madrid/ES)
07.-10.10.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College)
28.-30.10.	IT-Sicherheitsaudits in der Praxis – Konzeption, Durchführung, Bewertung (Secorvo College)

Fundsache

Das Verizon Business RISK Team hat im 2008 Data Breach Investigations Report die Ergebnisse seiner forensischen Analysen der letzten vier Jahre ausgewertet und zusammengefasst. Dabei wurde neben der Komplexität der Angriffe analysiert, wie der Datendiebstahl zu Stande kam und wer der Urheber war. Abweichend von der verbreiteten Überzeugung, dass Insider die meisten Angriffe verursachen, zeigt die Auswertung, dass in fast 80% der untersuchten Fälle der Zugriff von außen erfolgte, dabei allerdings häufig Geschäftspartner involviert waren.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian,
Hans-Joachim Knobloch, Natalie Mareth, Jochen Schlichting

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