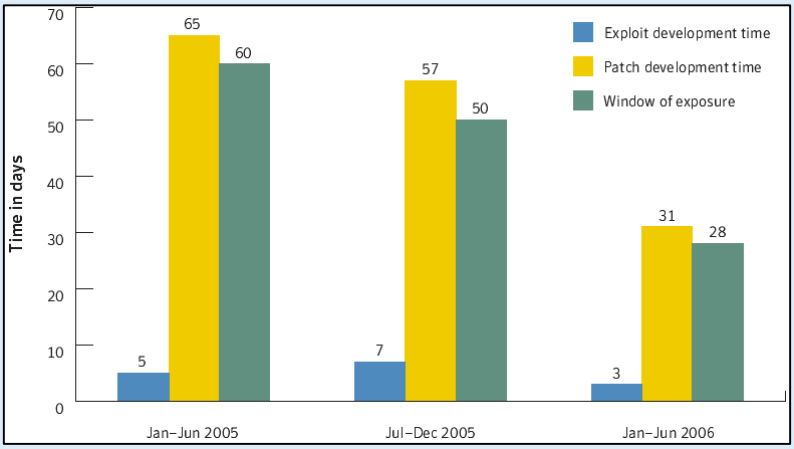
secorvo
security consulting

Secorvo Security News

November 2006

Editorial: Mo*Bing

Die Zahl gefundener sicherheitskritischer Programmfehler steigt – allen Bemühungen um sichere Software zum Trotz. Jetzt nehmen Cracker die Hersteller gar in den Schwitzkasten: Während noch diskutiert wird, ob die Veröffentlichung eines sicherheitskritischen Bugs ohne Vorabinformation des Herstellers und ohne „Anstandsfrist“ vertretbar ist, haben einige Cracker offenbar die letzten Hemmungen abgelegt: Mit der Veröffentlichung von „Zero-Day“-Bugs zwingen sie Herstellern einen Wettlauf mit den Entwicklern von Exploit-Code auf. Eine Entwicklungsabteilung, die jeden Patch für heterogene Umgebungen testen muss, bevor sie ihn ausrollen kann, hat gegen Tausende Ehrgeiz getriebene Cracker keine faire Chance – auch wenn die Hersteller die zur Patchentwicklung benötigte Zeit halbieren konnten (siehe Grafik; Quelle: Symantec).



Nun folgt gezieltes „Mo*Bing“: Nach dem Monat der Browser-Bugs (MoBB, 6/2006) und dem der Kernel-Bugs (MoKB, 11/2006) wurde für Anfang Dezember die Woche der Oracle Database Bugs angekündigt (WoODB). Gezielte Attacken mit Ansage auf selbstgerecht erwählte „Wutopfer“? Nein – kein Zweck kann die Mittel heiligen.

Inhalt

secorvo
security consulting

Security News

Datensammeln im Vorbeigehen

Die am 23.10.2006 veröffentliche Entwurfsfassung der RFID-Studie "Vulnerabilities in first-generation RFID-enabled credit cards" belegt, dass aus mit RFID-Chips ausgestatteten Kreditkarten (Anteil: ca. 6 % des US-amerikanischen Kreditkartenmarkts) führender Anbieter die Kartendaten (Name, Kartennummer und Ablaufdatum) unbemerkt ausgelesen werden können. Den Autoren gelang es sogar, mit den abgegriffenen Daten RFID-Chips zu „klonen", sofern keine kryptografischen Komponenten integriert waren.

Angesichts zahlreicher Projekte zur Einführung RFID-basierter Ausweispapiere verdichtet sich der Eindruck, dass teilweise bewährte Sicherheitstechnologien leichtsinnig abgelöst werden. Die Möglichkeit zum spurenlosen und unbemerkten Auslesen von Ausweiskarten birgt zudem die Gefahr der „informationellen Aushorchung".

Bugs mit Ansage

Am 01.11.2006 startete die Kampagne „Month of Kernel Bugs". War der „Month of Browser Bugs" im Juli 2006 eher zum „Warmlaufen", steht jetzt das Allerheiligste der Betriebssysteme im Fokus. Jeden Tag im November wird auf der Webseite der Kampagne ein neuer Kernel-Bug publiziert. Der Initiator mit dem Pseudonym „LMH", einer der Forscher des Metasploit-Projekts, wird einen großen Teil davon aus seiner Sammlung bisher unveröffentlichter Bugs beitragen. Gefunden hat er sie mit Hilfe einer Technik aus dem Jahr 1989: Fuzzing, dem Füttern von Anwendungen mit automatisch erzeugten, pseudo-zufälligen Eingaben.

Dass bei dieser Art des Black-Box-Testings überhaupt Fehler in Betriebssystemen gefunden werden, ist ernüchternd – zeigt es doch, dass viele Softwarehersteller nach wie vor erheblichen Nachholbedarf in Sachen Softwarequalität haben. Dabei findet man mit Fuzzing nur vergleichsweise triviale Fehler. Wie mag es da erst um das Security-Engineering dieser Anwendungen bestellt sein?

Preisgekrönte Verlierer

Zum siebten Mal wurden am 20.10.2006 Institutionen, Organisationen und Einzelpersonen mit den Big Brother Awards 2006 prämiert – Auszeichnungen, zu deren Verleihung die Preisträger in der Regel nicht erscheinen. Einen Award erhält, wer in den Augen der Jury zu den Zeitgenossen zählt, die auf besonders kritikwürdige Weise mit personenbezogenen Daten umgehen. Dies kann, muss aber nicht automatisch ein Gesetzesverstoß sein.

Die jährlich wachsende Zahl der Vorschläge, aus denen die Jury die Preisträger auswählt, spricht für sich: In diesem Jahr mussten Unterlagen zu 350 potenziellen Preisträgern gesichtet und beurteilt werden, darunter zunehmend Meldungen verärgerter und enttäuschter Verbraucher, die sich über datenschutzfeindliche Praktiken zahlreicher Unternehmen beschweren.

Der Gesamtverband der deutschen Versicherungswirtschaft stand ganz oben in der Publikumsgunst für den intransparenten Betrieb seiner inhaltlich fragwürdigen Warn- und Hinweisdateien. Leicht abgeschlagen folgte die Kultusministerkonferenz für ihre Bemühungen, ohne die Berücksichtigung von Zweckbindung und anderen datenschutzrechtlichen Erfordernissen eine lebenslang gültige Schüler-ID einzuführen. Weitere Preisträger waren SWIFT (für die Durchbrechung des Bankgeheimnisses durch die Übermittlung von Überweisungsdaten an US-Behörden), die Philips GmbH (für die Vorgabe, dass CD-Brenner ihre eindeutige Seriennummer auf den Rohling schreiben und damit eine Rückverfolgbarkeit von Datenträgern zum Brenner ermöglichen), der Landtag von Mecklenburg-Vorpommern (für die Erlaubnis zum Abhören und zur Tonaufzeichnung an öffentlichen Plätzen, in öffentlichen Gebäuden und in öffentlichen Verkehrsmitteln) und die Innenministerkonferenz (für den Beschluss zur Einrichtung einer Anti-Terror-Datei).

Top 20 Internet Security Targets

SANS hat am 15.11.2006 die sechste jährliche Liste der 20 „Spitzenreiter" kritischer Security-Bedrohungen publiziert. Die Aufzählung fehlerhafter Cross-Plattform-Anwendungen führen diesmal die Web-Applikationen an. Erstmals berücksichtigt die Liste nicht nur Software, sondern enthält auch eine Rubrik „Security Policy and Personnel", in der nicht genehmigte Devices (wie USB Flash Drives), extensive Nutzerrechte, Phishing und unautorisierte Software vier der 20 Spitzenplätze belegen. Als Sonderrubrik wurden „Zero-Day"-Exploits aufgenommen, da sich hier ein bedenklicher Trend abzeichnet: Die Rubrik verzeichnet 20 Patches für verbreitete Betriebssysteme und Office-Programme, zu denen vor Veröffentlichung des Patches Exploits kursierten. Auch VoIP Server und Telefone haben die Aufnahme in die Top 20 geschafft.

Hilfreich ist die Liste, an deren Erstellung mehr als 50 Security-Experten und -Institutionen mitwirkten, nicht nur für die Priorisierung von Überprüfungen der eigenen Infrastruktur. Sie enthält auch Links auf alle Updates und Patches der gelisteten kritischen Systeme, die im Laufe des vergangenen Jahres veröffentlicht wurden.

Sysinternals reloaded

Das am 09.11.2006 publizierte neue Microsoft-Tool Process Monitor (v1.01, 913 kB) – nicht zu verwechseln mit dem Werkzeug „Process Explorer“ – zeigt nicht nur, wie der Name vermuten lässt, laufende Prozesse an, sondern kombiniert auch die Eigenschaften der beiden Monitoring-Tools Filemon und Regmon in einer Oberfläche. Process Monitor kann sowohl helfen, Systemproblemen auf die Spur zu kommen, als auch bei forensischen Echtzeit-Analysen komplexe Vorgänge abbilden. Gegenüber den bereits vorhandenen Tools verbesserte Microsoft insbesondere Filter- und Export-Möglichkeiten.

Unabhängigkeitsverluste

Im September und Oktober vollzogen sich einige wesentliche Änderungen der Security-Landschaft. Am 25.09.2006 gab die kalifornische Firma Breach Security Inc. die Akquisition von Thinking Stone Ltd. bekannt, dem Hersteller von modsecurity (Apache Modul und Basis vieler Web Application Firewall-Architekturen). Der Innovationsbereitschaft scheint das zunächst keinen Abbruch getan zu haben: Am 16.10.2006 erschienen neue Major-Releases von modsecurity: für Apache (2.0.4), Core Rules (2.0) und Console (1.0.0).

Knapp einen Monat später, am 20.10.2006, hatte IBM die am 23.08.2006 angekündigte Übernahme des in Atlanta ansässigen Sicherheitsspezialisten Internet Security Systems abgeschlossen. Und wenige Tage danach gab die 1999 von Bruce Schneier gegründete Counterpane Internet Security Inc. am 25.10.2006 ihre Unabhängigkeit auf – das Unternehmen gehört nun zu British Telecom (BT).

Wie schon die Übernahme von RSA durch EMC^2 sind dies deutliche Anzeichen für eine beginnende Konsolidierung des (amerikanischen) Sicherheitsmarkts, bei der selbst erfolgreiche Spezialisten unter die Fittiche großer Unternehmen schlüpfen – für den Preis der Aufgabe ihrer Unabhängigkeit.

Phrowsers Phisherschutz phisht phrischer

Der seit 01.11.2006 verfügbare Internet Explorer 7 arbeitet zur Abwehr von Phishing mit einer lokalen Whitelist von mehreren tausend seriösen Websites, parallel führt Microsoft eine zentrale Blacklist. Demgegenüber verwendet die seit dem 25.10.2006 erhältliche Firefox 2-Version eine lokale Blacklist von gemeldeten Phishing-Websites.

Entscheidend für die Filterung von Phishing-Websites ist die Aktualität der verwendeten Blacklist. Da hat das Modell der zentralen Blacklist, die wie beim IE 7 online angefragt wird, klare Vorteile gegenüber einer lokalen Blacklist (Firefox 2.0), die in regelmäßigen Zeitabständen aktualisiert wird.

Phishing-Blacklists haben bekanntermaßen (ähnlich Blacklists von Mailservern, die E-Mail-Adressen und Domänen von Spammern enthalten) das Problem, dass Firmen und Organisationen, die irrtümlich oder durch Denunzierung auf die Liste gerieten, nur schwer wieder gelöscht werden. Welche Prüfungen Microsoft oder Mozilla (via Google) durchführen, bevor eine Website auf eine solche Blacklist von Phishing-Websites gelangt, ist nicht bekannt. Nicht bekannt ist weiter, wie sorgfältig die Überprüfung der gemeldeten Websites überhaupt durchgeführt werden kann, sobald das System allgemein genutzt wird, da eine Phishing-Website im Schnitt nur eine „Lebenserwartung“ von vier bis sechs Tagen hat.

Derzeit dürfte das Vertrauen in eine von Google geführte Blacklist vermutlich höher sein als die Akzeptanz einer von Microsoft verwalteten Liste.

Core Wars

Die am 18.10.2006 von SecureWorks vorgestellte und am 13.11.2006 ergänzte Analyse lässt das Entstehen eines darwinistischen Überlebenskampfes unter Trojanern um ihren Lebensraum befürchten. Offenbar setzen Trojaner gezielt Sicherheitssoftware zur Löschung konkurrierender Malware und zur Verhinderung einer erneuten Reinfektion ein. So wird der Trojaners SpamThru (Botnetz und Spamgenerator) über seine Control Server mit einer Routine versorgt, die eine raubkopierte Antivirensoftware installiert. Der Kampf um die Kernel hat begonnen.

Secorvo News

Secorvo College aktuell

Im Januar startet das Seminarprogramm 2007 mit **Information Security Management** (23.-26.01. 2007), gefolgt von den „Klassikern“ **PKI** (30.01.-02.02.2007) und **IT-Sicherheit heute** (06.-08.02. 2007).

Die nächste Möglichkeit zur Zertifizierung Ihres Security-Know-Hows bietet Ihnen das **T.I.S.P.-Seminar** am 05.-09.03.2007 (Prüfung am 10.03.).

Programm, Preise und Online-Anmeldung unter

http://www.secorvo.de/college

Video “Social Engineering”

Der wachsenden Bedeutung von “Social Engineering” bei Wirtschaftsspionage und Hacking-Attacken tragen wir durch ein neues Sensibilisierungsvideo Rechnung. Das Video ist ab Mitte Dezember in deutscher und (als Netzlizenz) englischer Sprache erhältlich (www.secorvo.de/video).

Veranstaltungshinweise

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

November 2006	
28.-30.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)
Dezember 2006	
04.-05.12.	IsSec / ZertiFA 2006 (COMPUTAS, Berlin)
27.-30.12.	23. Chaos Communication Congress (CCC, Berlin)
24.12.	Weihnachten (Weihnachtsmann, weltweit)
Januar 2007	
18.-19.01.	Tutorium "IT-Sicherheitskriterien im Vergleich" (DFN-CERT Services GmbH, Hamburg)
18.-19.01.	Tutorium "DFN-PKI in der Praxis" (DFN-CERT Services GmbH, Hamburg)
23.-26.01.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College, Karlsruhe)
30.01.-02.02.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo College, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de (Webanwendungen)

Sicherheit von Webanwendungen – Maßnahmenkatalog und Best Practices: Die aktuelle BSI-Studie (Stand 11.09.2006) enthält eine umfangreiche Zusammenstellung von Maßnahmen zur Sicherung von Webapplikationen und Best Practice Ansätzen sowie einen Leitfaden für die Erstellung sicherer Webanwendungen, der für Projektleiter, Entwickler und ggf. auch Auditoren interessant sein dürfte.

Impressum

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

ISSN 1613-4311

Redaktion: Petra Barzin, Dirk Fox, Stefan Gora, Kai Jendrian, Jochen Schlichting, Karin Schuler

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