secorvo
security consulting

Secorvo Security News

Januar 2007

Editorial: Nichts zu verbergen

Betrug, Diebstahl, Erpressung – nun hat auch die „gewöhnliche" Kriminalität das Internet erobert. Die Hemmschwelle Technik hat die organisierte Kriminalität durch die Verpflichtung kompetenter Programmierer inzwischen vollständig eingeebnet. Die Möglichkeit nahezu spurenloser und grenzüberschreitender Nutzung macht das Netz der Netze zum boomenden Tummelplatz für Gangster. Anders als befürchtet erweist sich allerdings nicht allein mangelnde IT-Sicherheit als Achillesferse; vielmehr bildet der nachlässige Umgang mit personenbezogenen Daten den Nährboden für gänzlich neue kriminelle Geschäftsmodelle.

Suchmaschinen und Portale geben persönliche Details preis: Arbeitgeber und Ausbildung (Alumni-Portale), Berufs- und Privatkontakte sind dort für jedermann einsehbar; persönliche Webseiten vervollständigen das Bild mit Hobbys und Urlaubsfotos. Zugehörige Adressen, Familienstand und Geburtsdatum lassen sich auf anderem Weg leicht herausfinden (Telefonbuch, Sportverein, social engineering). Mit diesen Daten lässt sich, genügend Fantasie und kriminelle Energie vorausgesetzt, manch geld-werte Erkenntnis gewinnen.

Dass solche Befürchtungen nicht an den Haaren herbeigezogen sind, zeigte eine am 07.12.2006 veröffentlichte Warnung des amerikanischen FBI vor einer anonymen, via Spammer verbreiteten Morddrohung: Darin wurden die Empfänger zur Zahlung mehrerer tausend Dollar Lösegeld aufgefordert, um ihre Ermordung abzuwenden, die angeblich einer ihrer Freunde in Auftrag gegeben hatte.

Falls Sie noch immer überzeugt sind, dass Sie als unbescholtener Bürger nichts zu verbergen und daher auch nicht um Ihre Privatsphäre zu fürchten haben – dann sei Ihnen das jüngste Werk von John Katzenbach („Der Patient") ans Herz gelegt: „Wir haben Angst davor, getötet zu werden. Dabei ist es viel schlimmer, vernichtet zu werden. Das Schlimmste aber ist, innerhalb von wenigen Tagen seine Identität zu verlieren." Eine nicht nur höchst spannende, sondern auch erkenntnisreiche Lektüre für lange Winterabende.

Inhalt

secorvo
security consulting

Security News

Zero Day Bounty

So genannte „zero day exploits“ sind Werkzeuge zur Ausnutzung von gerade erst veröffentlichten Schwachstellen. Unabhängig von der andauernden Diskussion, ob eine Schwachstelle erst dem Hersteller gemeldet oder so früh wie möglich publiziert werden soll (z.B. in Bugtraq), ist klar, dass derartige Exploits in Ermangelung von Gegenmaßnahmen bei Angreifern besonders beliebt sind. Inzwischen gibt es einen regelrechten Markt für diese Exploits, bis hin zur (halb-) öffentlichen Versteigerung.

Eine legale Möglichkeit, mit solchen Schwachstellen Geld zu verdienen, bietet iDefense seit dem 08.01. 2007. Das Unternehmen belohnt im Rahmen einer vierteljährlichen „Vulnerability Challenge“ aufgedeckte Schwachstellen in Windows Vista und IE 7 mit bis zu 12.000 US$. Auch das Snosoft Research Team hat am 17.01.2007 ein Exploit Aquisition Programm aufgelegt, und durch ein Teammitglied eine Diskussion zum Thema „Fair Exploit Price and Purchase“ auf full-disclosure angestoßen. Die finanziellen Anreize könnten die Motivation steigern, gefundene Schwachstellen zeitnah zu veröffentlichen, um die „Bounty“ einstreichen zu können.

Falls das Konzept aufgeht, dürfte die Zahl bekannt gewordener Schwachstellen weiter ansteigen.

Adobe anfällig

Am 03.01.2007 geriet der Adobe Reader wegen einiger Cross-Site-Skripting Schwachstellen in die Schlagzeilen. Neben einem Update gab Adobe in einem Security-Bulletin Hinweise zur Problemvermeidung. Kurz darauf wurde am 06.01.2007 im Rahmen des Month of Apple Bugs (MoAB) ein Fehler in der PDF-Spezifikation aufgedeckt: Fehlerhafte Einträge im Catalog Dictionary führen zu unvorhersehbarem Verhalten verschiedener PDF-Reader und können die Ausführung beliebigen Codes ermöglichen. Dies ist nicht auf den Adobe Reader oder ein bestimmtes Betriebssystem beschränkt.

Adobe empfiehlt in einem Security Bulletin vom 09.01.2007 dringend ein Update auf Version 8 des Acrobat Reader – dieser ist von der Schwachstelle nicht betroffen. Nutzer von KDE finden seit dem 15.01.2007 einen Fix für kpdf und KOffice. Anwender anderer Reader sollten sich möglichst bald nach Sicherheitsupdates umschauen – und bis dahin nur PDF-Dokumente aus vertrauenswürdiger Quelle öffnen.

Auch hier zeigt sich, dass ein über lange Zeit als sicher angenommenes Dokumentformat verborgene Schwachstellen besitzen kann. Die Faustregel der sicheren Softwareentwicklung, dass Fehler im Design schwer zu finden und nur teuer zu beheben sind, wurde wieder einmal bestätigt.

Gläserne Passagiere

Der Europäische Gerichtshof hatte am 30.05.2006 den Beschluss des EU-Rates vom 17.05.2004 über die Weitergabe von Fluggastdaten an die USA sowie die Entscheidung der EU-Kommission über die Angemessenheit des Schutzes dieser personenbezogenen Daten in den USA auf Antrag des EU-Parlaments für nichtig erklärt. Die Vereinbarung lief damit am 30.09.2006 aus. Am 06.10.2006 einigten sich die EU und die USA auf ein neues Abkommen, das nun bis 31.07.2007 gilt: Danach werden die bis zu 34 Einzelangaben umfassenden Datensätze aller Fluggäste von Transatlantik-Flügen nun auf Anfrage zahlreichen US-Behörden zugänglich gemacht.

Zu den übermittelten Daten zählen die Namen der Mitreisenden, Kreditkarten- oder Kontonummern, E-Mail-Adresse, Telefonnummern, Sonderwünsche wie vegetarisches Essen oder Sperrgepäck, ggf. Ausweisnummer, Geburtsdatum und Wohnort.

Wer vor dem Hintergrund dieser Entwicklung nicht auf USA-Reisen verzichten kann oder will, dem bleibt die schwache Hoffnung, dass die Zugriffsbefugnisse der US-Behörden auf diese Passagierdaten in der noch ausstehenden endgültigen Vereinbarung wirkungsvoll beschränkt werden.

23C3

Vom 27. bis 30.12.2006 fand der 23. Chaos Communication Congress in Berlin mit über 4.000 Teilnehmern statt. Im Verlauf von vier Tagen wurden in mehr als 120 Vorträgen, Workshops und Veranstaltungen unterschiedlichste Themenbereiche abgedeckt: Angefangen bei der Privatsphäre im Web 2.0 über ein mögliches Ende der Tor-Anonymität, verbesserte Bluetooth-Angriffe und Verkehrsüberwachung bis hin zur Suche nach Softwarefehlern in Binärcode. Weiter wurden innovative Ansätze zur Überwachung aus der Luft mit Microdrones vorgestellt – wehe dem Nachbarn, der Böses plant.

Aufschlussreich war auch der Bericht von Manfred Fink über Gästeüberwachung in Hotels durch professionelle Informationsbeschaffer – so Manches geht in der „analogen Welt“ viel einfacher. Aus der Welt der Pentester wurde Grundwissen über das Audit von Backbonerouters und die kreativen Möglichkeiten vermittelt, Paketflüsse zu steuern.

Wer diese inzwischen bei weitem größte deutsche Sicherheitskonferenz verpasst hat, kann sich anhand einiger Videostreams nachträglich ein Bild machen.

Veteran streicht Segel

Am 19.12.2006 hat die von dänischen Freiwilligen betriebene Open Relay Database (ORDB) ihre Dienste eingestellt. Seit dem 31.12.2006 ist auch die zugehörige ORDB-Webseite nicht mehr erreichbar.

Die ORDB-Betreiber reagierten damit auf die Veränderungen in der SPAM-Welt: Kam vor einigen Jahren noch mehr als 90% des SPAMs von offenen SMTP-Relays, wird der Löwenanteil heute über Drohnen in Botnetzen verschickt. Daher empfehlen die ORDB-Macher nicht, die ORDB-Verweise auf aktiven E-Mail-Servern durch alternative Real-Time-Blacklists (RBLs) wie Spamhaus oder Spamcop zu ersetzen, sondern auf eine Kombination aus Greylisting-Techniken und inhaltsbasierter Analyse, wie z. B. SPAM-Assassin umzustellen.

Die wirksamste Methode zur Abwehr von SPAM ist nach unserer Erfahrung die Kombination verschiedender Ansätze – einschließlich RBLs. Allerdings müssen diese Techniken weiterentwickelt werden und neue Ansätze auf den Tisch, damit sich auch zukünftig den rasanten Entwicklungen der Spammer etwas entgegensetzen lässt. Ereignisse wie die kurzfristige Reduzierung des SPAM-Aufkommens um ca. 30% in der Zeit des Jahreswechsels sind leider keine nachhaltigen Trends.

Zero Day Pranger

Auch von anderer Seite wächst der Druck auf die Hersteller: Symantec veröffentlicht schon seit längerem in seinem regelmäßigen Internet Security Threat Report die Größe des „Window of Exposure“ (vgl. SSN 11/2006). Noch plakativer werden die Hersteller vom Schwachstellen-Management-Anbieter Eeye an den Pranger gestellt (vgl. SSN 12/2006): In einem Zero Day Tracker wird die Zeit veröffentlicht, die Hersteller seit Bekanntwerden einer Schwachstelle verstreichen ließen, ohne diese zu schließen. Auch wenn der „virtuelle Pranger“ derzeit den Fokus auf einige wenige Hersteller legt, vermittelt er einen einfachen und aktuellen Schwachstellenüberblick. Die Historie der inzwischen behobenen Schwachstellen deckt auf, wie schnell oder wie langsam der jeweilige Hersteller reagiert hat.

Doch allein mit beschleunigter Fehlerbeseitigung lässt sich die Risk Exposure Time (RET) nicht minimieren. Denn auch wenn Patches deutlich schneller zur Verfügung gestellt würden, fielen die Zeiten für Tests und den Roll-Out der Patches zusätzlich an. Strategien zum Umgang mit Schwachstellen (Schwachstellen-Management) sollten daher unabhängig von Patch-Zyklen und der Verfügbarkeit von Bug-Fixes entwickelt und optimiert werden.

DuD 2007

Am 12.-13.03.2007 findet die diesjährige Fachtagung „DuD 2007“ in Berlin statt – zwei Tage voller spannender, prominent besetzter Vorträge rund um IT-Sicherheit und Datenschutz unter der Leitung der Herausgeber der Fachzeitschrift DuD – Dr. Johann Bizer und Dirk Fox. Thematische Schwerpunkte bilden die Gestaltung von Einwilligungserklärungen, die Sicherheit von Web-Applikationen und die ID-Strategie der Bundesregierung.

Secorvo News

Secorvo College aktuell

Die starke Nachfrage nach T.I.S.P.-Schulung und -Prüfung zeigt den großen Bedarf an einem unabhängigen Expertenzertifikat in der IT-Sicherheit. Die nächste T.I.S.P.-Schulung mit anschließender Prüfung findet am 05.-09.03.2007 statt. Das bereits veröffentlichte Seminarprogramm wird um das Seminar PKI – Grundlagen, Vertiefung, Realisierung am 26.-29.03.2007 erweitert.

Programm, Preise und Online-Anmeldung unter www.secorvo.de/college

“Social Engineering” – der Film

Das vierte Awareness-Video ist nun verfügbar – diesmal über „Social Engineering“. Es thematisiert eine Bedrohung, deren Bedeutung im Zuge von Globalisierung und verschärftem Wettbewerb spürbar zunimmt: Die Informationsbeschaffung mit überwiegend nichttechnischen Methoden. Tatsächlich ist es häufig weit einfacher als angenommen, gesuchte Informationen gezielt zu beschaffen, ohne dabei technische Sicherheitsmechanismen überwinden zu müssen. Falsch verstandene Höflichkeit, Gutgläubigkeit, Furcht vor Autoritäten und Vertrauensseligkeit sind dabei meist die heimlichen Komplizen der Angreifer. Ziel des Videos, das ab sofort bestellt werden kann, ist es, das typische Vorgehen eines „Informationsbeschaffers“ zu demonstrieren, um Mitarbeiter für Angriffsversuche dieser Art zu sensibilisieren.

White Paper “Security Audits”

Im aktuellen Secorvo White Paper vom 17.01.2007 fasst Stefan Gora die Erfahrungen von Secorvo mit der Konzeption und Durchführung von “Security Audits” zusammen. Nach einleitenden begrifflichen Klarstellungen stellt er die Vorgehensweise bei Black-Box- und White-Box-Analysen vor und beschreibt die Audit-Methodik in Anlehnung an die Standards ISO 17799, BS 7799-x, BSI 100-x und ISO 27001, an das IT-Grundschutzhandbuch sowie weitere Best Practice-Ansätze.