secorvo
security consulting

Secorvo Security News

Mai 2007

Editorial: Die Bärenstrategie

Zwei Wanderer werden vom Bären verfolgt. Da stoppt der eine und zieht Laufschuhe an. Meint der andere: „Damit bist du auch nicht schneller als der Bär." Entgegnet der erste: „Ich muss ja nicht schneller sein als der Bär."

Zugegeben, eine etwas gewöhnungsbedürftige Perspektive und eine zweifellos wenig solidarische Haltung. Aber nicht nur auf der Flucht, sondern auch in der IT-Sicherheit ist diese Bärenstrategie ohne Zweifel ein Erfolgsrezept – mit einem sehr weiten Anwendungsbereich.

Denn in der Praxis genügt es in der Regel, ein etwas höheres Sicherheitsniveau zu bieten, um Phishern, Pharmern, Hackern und „Skript-Kiddies" zu entkommen. Einem Angreifer bieten die einfachsten Methoden das beste Kosten-Nutzen-Verhältnis – so wie ein Einbrecher auch das offene Balkonfenster einer verschlossenen Sicherheitstüre vorziehen wird. Der Effekt lässt sich derzeit gut bei Phishing-Attacken beobachten: Kaum führt ein Institut iTANs ein, konzentrieren sich die Angreifer auf einen Mitbewerber.

Auch bei der eigenen Prioritätensetzung hilft die Bärenstrategie: An der Stelle mit dem niedrigsten Sicherheitsniveau ist ein erfolgreicher Angriff am wahrscheinlichsten – daher verdient diese Stelle die größte Aufmerksamkeit. So sollte die konsequente Durchsetzung einer einheitlichen Mindest-Passwortqualität Vorrang vor einer Datenverschlüsselung genießen, die Reduktion überflüssiger (Administrator-) Privilegien wichtiger genommen werden als ein Intrusion Prevention System, und die Beschleunigung des Roll-Outs von Sicherheits-Patches der Einführung eines SmartCard-Logins vorgezogen werden. Nicht, dass Verschlüsselung, IPS oder SmartCards unwichtig oder gar unsinnig wären – allein: Siege werden auch in der IT-Sicherheit zuerst mit den handwerklichen „Basics" errungen.

Leider hat die Bärenstrategie einen Haken. Sie funktioniert, wenn beide Wanderer für den Bären gleich attraktiv sind. Ist der schnellere Happen der appetitlichere, retten auch die Laufschuhe nicht.

Inhalt

secorvo
security consulting

Security News

SAP im Fokus?

Im SAP Security Newsletter April 2007 reagiert SAP auf einen Vortrag bei der BlackHat Europe 2007 Konferenz vom 30.03.2007. Das Papier eines südamerikanischen Sicherheitsspezialisten beschäftigt sich mit dem in Hacker-Kreisen oft als „dunkler Kontinent" angesehenen Innenleben von SAP R/3 und analysiert das Remote Function Call (RFC) Interface. Im Rahmen dieser Analyse wurden mehrere, inzwischen von SAP behobene Sicherheitslücken aufgedeckt und mit sapyto ein Open-Source Tool für Penetrationstests von R/3-Systemen entwickelt. Dies könnte ein Indiz dafür sein, dass SAP mehr in den Fokus der Hacker-Gemeinde rückt, die dort ein weiteres Anwendungsfeld für „bewährte" Angriffstechniken vorfindet.

R/3-Anwender sollten das zum Anlass nehmen, spätestens jetzt den SAP RFC/ICF Security Guide zu beherzigen. Und wer die Einführung von SNC plant, dürfte in dem BlackHat-Beitrag ein weiteres Argument dafür finden.

AHS und Ohs

Getreu der chinesischen Weisheit, dass auch die längste Reise mit dem ersten Schritt beginnt, hat das NIST erste Aktivitäten in der bis 2012 angelegten Suche nach einer neuen sicheren Hashfunktion, dem Advanced Hash Standard (AHS) als Nachfolger für den angeschlagenen SHA-1 und die verwandte SHA-2-Familie, unternommen: Am 07.05.2007 wurden die Kommentare aus Wissenschaft und Industrie zu den im Januar vorgelegten Kriterien veröffentlicht, denen der AHS genügen soll.

Der Tenor vieler Kommentare ist, nicht nur die Sicherheit der Hashfunktion im engeren Sinne, sondern auch deren mittlerweile gebräuchliche weitere Einsatzbereiche wie z. B. als Pseudozufallsfunktion, zum symmetrischen Integritätsschutz als HMAC und zur Schlüsselherleitung für symmetrische Chiffren als Auswahlkriterium zu betrachten.

Das NIST lässt explizit offen, ob es nur einen oder mehrere unterschiedliche Hash-Algorithmen als Gewinner des AHS-Wettbewerbs geben wird – sofern genügend Vorschläge die Kriterien erfüllen.

Phishing-Windows-Aktivierung

Eine neue Phising-Variante erscheint uns eine Erwähnung wert: Wie am 27.04.2007 von Symantec berichtet ist derzeit eine Trojanerversion in Umlauf, die beim ersten Systemstart nach der Infektion eine Aktivierung der Windows-Installation mit Eingabe einer gültigen Kreditkartennummer fordert.

Da das System herunter gefahren wird, wenn man keine Nummer einträgt, und Nutzern von illegalen Betriebssystemkopien ein solcher Mechanismus glaubwürdig erscheinen könnte, wird sich wohl der eine oder andere Anwender zur Eingabe verleiten lassen. Die Kartennummern werden an Systeme in Russland übermittelt und beispielsweise über einschlägige Foren verkauft – ein weiteres Beispiel für die zunehmend kriminellen Motive hinter verbreiteter Schadsoftware.

Des Kaisers neue Kleider

Mit der seit dem 01.05.2007 verfügbaren Produktklasse „Forefront" bündelt Microsoft seine bis dato unterschiedlichen (selbst entwickelten und zugekauften) Lösungen für Sicherheitssoftware und präsentiert als Roadmap eine Client, Server und „Edge" umfassende Strategie. Damit entwickelt sich Microsoft zunehmend zum Anbieter von Sicherheitslösungen – zum Schutz vor hausgemachten Sicherheitsproblemen.

In der nun überarbeiteten Lösung „Forefront - Security für Exchange Server" (ehemals Antigen für Exchange) beispielsweise können von neun enthaltenden Antivirus-Engines bis zu fünf parallel für Prüfprozesse von E-Mail genutzt werden. Durch diesen integrativen Ansatz wirkt damit das Know How von AV-Mitbewerbern zusammen (darunter Kaspersky, Norman, CA).

Derzeit laufen Forefront-Services wie z.B. FSC-Controller, FSCMonitor, FSCStatisticsService, FSEIMC, FSEMailPickup auf Exchangeservern mit absoluten Systemprivilegien (LocalSystem) – ein schwieriger Kontext für ein nachvollziehbares Audit. Vielleicht sollte sich Microsoft auf seine bereits im Juni 2005 propagierte Sicherheitsphilosophie besinnen, Dienste mit möglichst geringen Privilegien laufen zu lassen.

Alte Erkenntnisse - neu belegt

Am 24.04.2007 hat McAfee eine in Zusammenarbeit mit Datamonitor erstellte Studie mit dem Titel „Datagate: The Next Inevitable Corporate Disaster?" veröffentlicht. Diese Studie beschäftigt sich mit Ursachen für und Folgen von Datenverlust insbesondere durch Entwendung. Es wurden über 1.400 Unternehmen mit mehr als 250 Mitarbeitern befragt, darunter 75% mit mehr als 1.000 Angestellten. Es überrascht nicht, dass über 60% der Unternehmen in den vergangenen zwölf Monaten Vorfälle zu verzeichnen hatten und gerade einmal 6% von sich behaupten, in den vergangenen beiden Jahren keine Probleme gehabt zu haben. Immerhin glaubt

ein Drittel aller Teilnehmer, dass sie einen größeren Vorfall nicht überleben würden.

Die Studie berichtet, dass 23% der Firmen angaben, beobachtete Vorfälle seien bösartiger und vorsätzlicher Natur gewesen. 32% haben grob fahrlässige Vorfälle verzeichnet (z. B. Kopien vertraulicher Daten auf ungeschützten USB-Sticks) und in 45% aller Fälle sind die Vorfälle fahrlässig herbeigeführt worden (z. B. Verlust eines Laptops mit unverschlüsselten Daten). Die geografische Lage eines Unternehmens spielt hingegen keine Rolle für die Risiken von Datenverlust: Die Untersuchungsergebnisse unterschieden sich in Australien, Frankreich, UK und den USA nicht signifikant.

Die Studie stellt einige wichtige Best-Practices zum Umgang mit sensiblen Daten vor. Dem Fazit der Studie können wir uns nur anschließen: „... we know that technology ist not always the answer."

Professionelles Social Engineering

Die schweizerische „Melde- und Analysestelle Informationssicherung" (MELANI) hat am 30.04.2007 ihren vierten Halbjahresbericht „Informationssicherung – Lage in der Schweiz und international" herausgegeben. Wieder einmal enthält der Bericht sehr interessante Informationen zu aktuellen Bedrohungen sowie Aussagen zu zukünftigen Trends der Informationssicherheit. Die MELANI-Studie zeichnet dabei aus, dass sie nicht nur die aktuelle Situation beschreibt, sondern konkrete Vorfälle – in der Schweiz sowie international – aufzeigt, welche die einzelnen Probleme noch einmal verdeutlichen.

MELANI führt als Angriffs-Schwerpunkte zunächst die „üblichen Verdächtigen" an: Spam, Daten- und Identitätsdiebstahl, sowie Malware und Angriffsvektoren. Interessanterweise wird das Social Engineering an erster Stelle genannt. So gehen die Autoren davon aus, dass „Social Engineering mit zunehmender (technischer) Sicherheit von Betriebssystemen und Applikationen weiter an Bedeutung gewinnen" wird. Sie empfehlen daher Prävention: „Regelmäßige, den aktuellsten Trends angepasste Schulungen und Tests helfen, die Angestellten zu sensibilisieren und mögliche Gefahren zu erkennen."

Awareness-Grenzen

Dass auch die beste Awareness ihre Grenzen hat, zeigen zwei aktuelle Beispiele. Der Belgier Didier Stevens berichtete am 07.05.2007 von einem „Social Engineering-Experiment": Er schaltete über mehrere Monate eine Google-Anzeige mit dem Text „Is your PC virus-free? Get it infected here!" und war erschrocken, dass tatsächlich 409 Menschen auf die (harmlose) URL geklickt hatten. Dass dieser Mechanismus bereits heute von professionellen Betrügern missbraucht wird, bestätigte am 26.04.2007 sogar Google selbst – Google-Anzeigen hatten auf maliziöse Webseiten geleitet.

Secorvo News

Secorvo College aktuell

Die Nachfrage nach einer Bestätigung der Qualifizierung im Gebiet IT-Sicherheit durch den Erwerb eines T.I.S.P.-Zertifikats ist ungebrochen. Für das zusätzliche T.I.S.P.-Seminar vom 25.-30.06.2007 gibt es nur noch wenige freie Plätze, und auch das Herbst-Seminar vom 05.-10.11.2007 füllt sich bereits. Wir freuen uns auf Ihre Anmeldung.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Innovationspreis für Video

Für das Sensibilisierungs-Video „Social Engineering" wurde Secorvo am 16.04.2007 von der Initiative Mittelstand in der Kategorie IT-Security mit dem Innovationspreis 2007 ausgezeichnet.

Security Awareness Symposium

Awareness ist „in" – das zeigen die vielen Anmeldungen zum fünften „Security Awareness Symposium" am **12. bis 13.06.2007**, auf dem u. a. das BSI, Carl Zeiss, e.on Ruhrgas, European Investment Bank, Fiducia und M. Dumont Schauberg ihre Kampagnen und Erfahrungen präsentieren.

Das Programm des diesjährigen Erfahrungsaustauschs in den Räumlichkeiten der Buhlschen Mühle in Karlsruhe-Ettlingen (ca. 10 min. vom Karlsruher Hauptbahnhof), eine Online-Anmeldung und Anfahrtskizze finden Sie unter:
http://www.security-awareness-symposium.de

KA-IT-Si über sichere Software

Kein Monat ohne Sicherheits-Patch, -Update oder -Bugfix: Das „Flicken" fehlerhafter Software ist zu einer Hauptdisziplin der IT-Sicherheit geworden. Am **28.06.2007** werden Dr. Boris Hemkemeier (Commerzbank AG) und Tom Schröer (SAP AG) die Ergebnisse des vom BMWi geförderten Projekts "Secologic" vorstellen, in dessen Rahmen u. a. „10 Goldene Regeln" für Auftraggeber entwickelt wurden, die helfen sollen, die Zahl sicherheitsrelevanter Fehler in Software systematisch zu reduzieren. Für ein angemessenes Net(t)working-Ambiente ist – wie immer – gesorgt. Online-Anmeldung über
http://www.ka-it-si.de.

Veranstaltungshinweise

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

Juni 2007	
12.-13.06.	5. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
12.-13.06.	DACH Security 2007 (Klagenfurt/A)
25.-29.06.	T.I.S.P. Schulung (Secorvo, Karlsruhe)
28.06.	Software ist fehlerfrei. Und die Erde eine Scheibe. (KA-IT-Si, Karlsruhe)
30.06.	T.I.S.P. Zertifikatsprüfung (Secorvo, Karlsruhe)
Juli 2007	
12.-13.07.	DIMVA 2007 (GI, Luzern/CH)
28.07.-02.08.	Black Hat USA 2007 (Las Vegas/US)
August 2007	
03.-05.08.	Defcon 15 (Las Vegas/US)
06.-10.08.	USENIX Security Symposium (Boston/US)
19.-23.08.	Crypto 2007 (IACR, Santa Barbara/US)

Fundsachen

Auszug aus www.security-finder.de

Internet-Suchmaschinen werden bereits seit vielen Jahren auch von Angreifern verwendet, um sensitive Informationen (z. B. Passwort-Dateien, Login-Daten) zu recherchieren und anschließend zu missbrauchen. The Google Hacker's Guide beschreibt, wie die Suchmaschine Google zu diesem Zweck von Angreifern eingesetzt wird und wie man sich dagegen schützen kann.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim-Knobloch, 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