Secorvo Security News
Januar 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Hans-Joachim Knobloch, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 42, 5. Jhrg. 2006
Stand 26. Januar 2006

ISSN 1613-4311

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

Inhalt

Editorial: 42

"I think, to be quite honest with you, is that you've never actually known what the question is."
Douglas Adams (Hitchhiker's Guide to the Galaxy)

Die Antwort von *Deep Thought* auf die „Frage nach dem Leben, dem Universum und dem ganzen Rest" ist Kult – und weckt Assoziationen. Denn mit simplen Antworten, die in keinem nachvollziehbaren Zusammenhang mit der gestellten Frage zu stehen scheinen, werden wir nicht nur in Politikerinterviews beglückt. Sie sind vielmehr zu einer unserer häufigsten Informationsquellen geworden.

Nur ein Beispiel: „Über 70% aller Angriffe kommen von innen" – eine beliebte Aussage zahlreicher Studien, begeistert aufgegriffen von Journalisten und gerne als Argument für die Durchsetzung verschiedenster Sicherheitsmaßnahmen genutzt.

Einmal abgesehen von Defiziten bei der handwerklichen Gestaltung und Auswertung der zugehörigen Studien, irritiert bei genauer Betrachtung mindestens zweierlei:

- Gefragt wurden die für IT-Sicherheit in Unternehmen Verantwortlichen – nicht etwa die Täter oder eine Fallstatistik.
- Unter „Angriff" wird meist inflationär jeder Sicherheitsvorfall (bis zum vergessenen Passwort) subsummiert.

Liest man die den Studien zu Grunde liegenden Fragebögen, kann man sich des Eindrucks nicht erwehren, dass hier die Branche begeistert ihre eigene Wichtigkeit feiert. Nicht, dass die Aussagen unwahr sind – allerdings: Wir wissen es nicht. Gerade bei Aussagen zur tatsächlichen Bedrohung, den Schäden und Täterarten wären aber belastbare Erkenntnisse sehr wichtig – und stünde mehr diesbezügliche Seriosität uns allen gut zu Gesicht.

Bleibt zu fragen, warum Douglas Adams in seinem Kult-Roman die Erde als Computer zur Formulierung der richtigen Frage bauen lässt. Ob er tatsächlich angenommen hat, dass sich diese Kompetenz hier entwickelt? Dass er die Erde vor Ablauf des Programms sprengt, lässt auf eine realistischere Sicht der Dinge schließen...

1 Security News

1.1 Pikanter Patch

Zum Jahresausklang wurde nach bereits zweiwöchiger „Verbreitung“ des zugehörigen Remote-Exploit-Codes ein Designfehler im Windows Meta File-Format (WMF) auf Bugtraq einer breiteren Öffentlichkeit zugänglich gemacht. Fatalerweise genügt bereits das Anklicken oder Anschauen einer Grafikdatei, beispielsweise auf einer Webseite, um beliebigen Code zur Ausführung zu bringen. Eine gute Demonstration findet sich beim Heise Verlag. Betroffen sind nicht nur Microsoft-Betriebssysteme, sondern auch WMF-Metadaten verarbeitende Anwendungen (u.a. Lotus Notes und Debian Linux). Auch der Wine Windows API-Emulator bildet diesen Designfehler unter Linux „ordnungsgemäß“ nach.

Obwohl für diese sehr kritische Schwachstelle bereits Software zur Ausnutzung im Umlauf war, wurde der offizielle Patch MS06-001 von Microsoft erst zwei Wochen später zur Verfügung gestellt.

Pikantes Detail: Offenbar war zunächst vorgesehen, den Patch erst zum regulären Patch-Day Mitte Januar auszuliefern. Nutzer hatten daher zur Selbsthilfe gegriffen und inoffizielle Patches (u. a. von Ilfak Guilfanov) sowie Anleitungen zur Verhinderung der Schwachstelle veröffentlicht.

Wichtig: Microsoft bietet keinen Patch für Systeme wie WindowsNT oder Win2000 SP3 an, deren „Extended Security Support“ abgelaufen ist. Ein Update auf ein aktuelleres Betriebssystem ist unvermeidlich.

1.2 GSHB heiratet BS 7799-2

Am 16.01.2006 hat das BSI in einer Pressemitteilung die Veröffentlichung der neuen Version des Grundschutzhandbuchs angekündigt. Bei dieser Version handelt es sich um eine grundlegende Überarbeitung des Handbuchs. Die wichtigste Änderung ist die Anpassung an den ISO Standard 27001 (internationaler Nachfolger des BS 7799-2).

Ebenfalls neu ist die Abspaltung von ehemaligen Bestandteilen des GSHB in eine neue Schriftenreihe, die BSI-Standards 100-1 bis 100-3. Die Standards beschreiben vorrangig Prozesse und Vorgehensweisen, während die Bausteine, Gefährdungen und Maßnahmen weiterhin in den so bezeichneten Grundschutz-Katalogen enthalten sind.

Mit der Überarbeitung und Anpassung an ISO 27001 hat das BSI ein bereits gutes Hilfsmittel weiter verbessert und die Attraktivität einer Zertifizierung erhöht. Derzeit ist die neue Version nur in gedruckter Form über den Bundesanzeiger-Verlag oder den Buchhandel erhältlich. Eine Online-Version soll in Kürze über die Webseite des BSI zur Verfügung gestellt werden.

1.3 WAF-Auswahlhilfe

Am 14.01.2006 hat das Web Application Security Consortium (WASC), ein im Januar 2004 gegründetes internationales Expertengremium, Version 1.0 der „Web Application Firewall Evaluation Criteria“ vorgelegt. Dabei handelt es sich um eines der ersten Dokumente, in welchem Entscheidern und Firewall-Architekten ein ausführlicher Katalog wichtiger Anforderungen an eine Web-Application-Firewall (WAF) zur Verfügung gestellt wird. Diese Anforderungsliste erleichtert den Vergleich, die Bewertung und die Auswahl geeigneter WAF-Lösungsansätze und verfügbarer Produkte.

1.4 Experimentierkasten

Das bekannte, von der TU Darmstadt, der Universität Siegen und der Deutschen Bank entwickelte Lernwerkzeug Cryptool ist seit Ende 2005 als Beta-Release in der Version 1.4 verfügbar – ein schöner praktischer Einstieg in die Kryptographie.

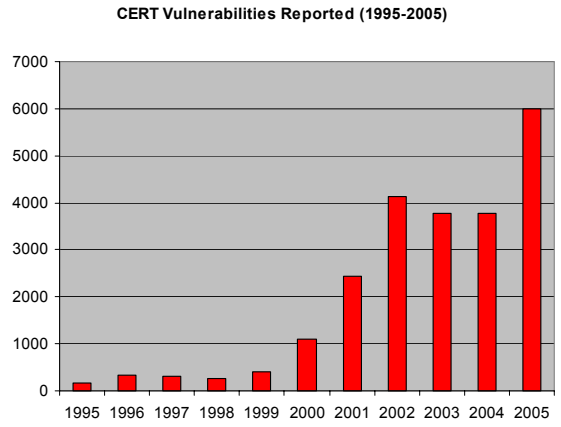
In der Roadmap sind die durchgeführten und geplanten Änderungen beschrieben. Besonders interessant sind eine Demo von Authentifizierungsmöglichkeiten im Netz, verschiedene aktuelle Angriffsdemonstrationen (u.a. Seitenkanal-Attacken und spezielle Angriffe gegen RSA) sowie neue Visualisierungsfunktionen (u.a. animierte

Veranschaulichungen von Algorithmen und 3D-Visualisierung großer Mengen von Zufallszahlen).

Vor der Publikation der Endfassung freuen sich die Autoren über kritische Beta-Tester.

1.5 CERT/CC Statistik

Das CERT Coordination Center an der Carnegie Mellon University (CERT/CC) führt eine Statistik der jährlich entdeckten (und gemeldeten) Sicherheitsschwachstellen (Vulnerabilities). Beunruhigend sind die Zahlen aus 2005:



Nach einem explosionsartigen Anstieg Anfang des Jahrtausends hatten sich die Softwarefehler 2002-2004 bei rund 4.000 eingependelt. 2005 ist die Zahl trotz der verstärkten Bemühungen vieler Hersteller um sichere Softwareentwicklung um fast 60% angestiegen.

1.6 Wendung zum Besseren

Seit dem 22.12.2005 ist das von ISACA entwickelte und erstmals 1996 veröffentlichte CobiT-Framework in der Version 4.0 verfügbar. CobiT (Control Objectives for Information and Related Technology) ist ein internationales Modell von Kontrollzielen speziell für IT-Prozesse.

In der neuen Version wurden Redundanzen zwischen allgemeinen und spezifischen Kontrollen beseitigt, so dass die Anzahl der Control Objectives von 318 auf 215 reduziert werden konnte. Weiter wurde der zentrale Fokus der IT Governance innerhalb einer Corporate Governance vertieft. Im Rahmen der inhaltlichen Ergänzung der „Detailed Control Objectives“ wurden im Bereich „Plan & Organise“ insgesamt 16 Control Objectives ergänzt, im Bereich „Aquire & Implement“ sind es sechs und im Bereich „Delivery & Support“ acht. Schließlich wurde auch der Bereich „Monitor & Evaluate“ überarbeitet.

Bei eingehender Lektüre lässt sich feststellen, dass die Homogenität des CobiT-Ansatzes verbessert wurde und die praktische Arbeit mit dem Framework deutlich leichter fällt.

1.7 BlackBerry Bugs

Auf dem 22. Chaos Communication Congress des CCC (22C3) am 27.-30.12.2005 wurden von FX (Phenoelit) mehrere BlackBerry-Bugs vorgestellt. Die meisten der gefundenen Schwächen (u.a. Buffer Overflow bei JAD-Files, fehlerhafte TIFF-Anhänge) betreffen die Endgeräte und sind klassische Programmierfehler, wie sie fast täglich für zahlreiche Smartphones und PDAs gemeldet werden. Da ist es ein Qualitätsmerkmal, dass für BlackBerry-Handhelds bislang nur sehr wenige Bugs dieser Art entdeckt wurden.

Unschön könnten die von FX erwähnten Protokollfehler sein – leider gibt es bislang keine publizierten Unterlagen oder valide CERT-Meldungen dazu.

Alle anderen Schwachstellen betreffen ausschließlich die Funktionsfähigkeit von Spezialdiensten und sind schlimmstenfalls lästig, keiner davon aber sicherheitskritisch. Kein Grund zur Beunruhigung also – zumal man sich durch Software-Updates oder Sperrung dieser Dienste leicht vor solchen Angriffen schützen kann.

2 Secorvo News

2.1 Secorvo College aktuell

Die Bosch Sicherheitssysteme GmbH ist nach SAP, T-Systems und dem BSI seit dem 18.01.2006 neuer Ausbildungspartner.

Die nächste Gelegenheit zum Besuch eines Secorvo-College-Seminars bietet sich am 07.-10.02.2006 – vier Tage Intensivkurs rund um Public Key Infrastrukturen.

http://www.secorvo.de/college

2.2 ISO 27001-AaBvITG

Seit dem 19.01.2006 ist Stefan Gora vom BSI lizenzierter ISO 27001-Auditor auf Basis von IT-Grundschutz (AaBvITG).

2.3 KA-IT-Si wird fünf

Vor fast exakt fünf Jahren wurde die „Karlsruher IT-Sicherheitsinitiative" von den Karlsruher Versicherungen und Secorvo aus der Taufe gehoben. Das Ziel: Verbesserung der IT- und Informationssicherheit vor allem mittelständischer Unternehmen der TechnologieRegion Karlsruhe. Seitdem hat die Initiative, die von zahlreichen Unternehmen gefördert wird, darunter Amec Spie, Junctim, Lampertz, L-Bank, neef it solutions, SAP, Sparkassen Informatik, Vogon und Würth Phönix, 17 Veranstaltungen mit über 400 Teilnehmern zu Themen der IT-Sicherheit durchgeführt.

Die Initiative hat sich nicht nur etabliert, sondern lockt immer wieder Interessierte aus ganz Deutschland nach Karlsruhe. Den fünften Geburtstag wird die KA-IT-Si mit einer Veranstaltung am 21.03.2006 feiern.

2.4 „DuD 2006" – 27.-28.03.

Der Klassiker – zum achten Mal treffen sich am 27.-28.03.2006 Autoren und Leser, Koryphäen und Verantwortliche auf der Jahrestagung der Fachzeitschrift „Datenschutz und Datensicherheit (DuD)" in Berlin. Auch in diesem Jahr stehen spannende Themen auf dem Programm – von Blackberry Security über Honeynets, die Privacy-Initiative von Microsoft bis hin zu Whistleblower-Systemen. COMPUTAS wird wieder für ein angemessenes Ambiente Sorge tragen.

3 Veranstaltungshinweise

Januar 2006	
30.-31.01.	Net-ID 2006 (COMPUTAS, Berlin)
Februar 2006	
07.-10.02.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
14.-15.02.	Inside Windows Security (Secorvo College, Karlsruhe)
20.-21.02.	IT Governance 2006 (COMPUTAS, Köln)
20.-22.02.	Sicherheit 2006 – Schutz und Zuverlässigkeit (GI, Magdeburg)
28.02. - 03.03.	Black Hat Europe 2006 (Black Hat, Amsterdam/NL)
März 2006	
01.-02.03.	DFN-CERT Workshop (DFN-CERT, Hamburg)
09.-15.03.	CeBIT 2006 (Deutsche Messe AG, Hannover)
21.03.	KA-IT-Si-Geburtstagsfeier (KA-IT-Si, Karlsruhe)
27.-28.03.	Datenschutz und Datensicherheit – DuD 2006 (COMPUTAS, Berlin)
27.-31.03.	Information Security Management (Secorvo College, Karlsruhe)
28.-29.03.	D*A*CH Security 2006 (GI/Bitkom/TeleTrusT, Düsseldorf)

Aktuelle Veranstaltungsübersicht:
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. +49 721 255 171-0
Fax +49 721 255 171-100

Zusendung des Inhaltsverzeichnisses:
security-news@secorvo.de
(Subject: „subscribe security news")

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