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.

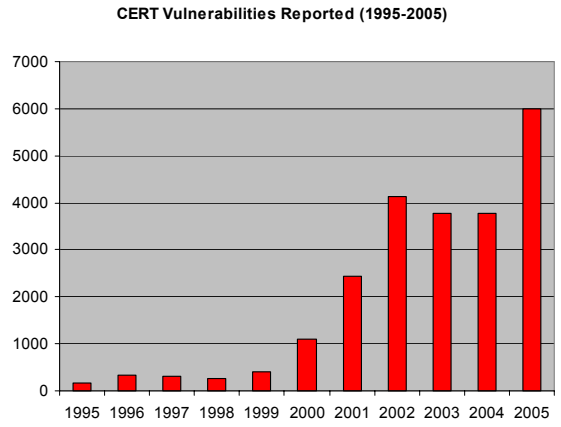
In der Roadmap sind die durchgeführten und geplanten Änderungen beschrieben. Besonders interessant sind eine Demo von Authentifizierungsmöglichkeiten im Netz, verschiedene aktuelle Angriffsdemonstrationen (u.a. Seitenkanal-Attacken und spezielle Angriffe gegen RSA) sowie neue Visualisierungsfunktionen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

Secorvo Security News
Februar 2006

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

Nr. 2, 5. Jhrg. 2006
Stand 23. Februar 2006

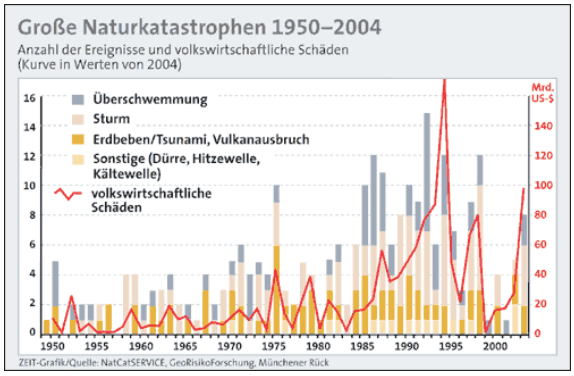
ISSN 1613-4311

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

Inhalt

Editorial: The Show must go on

Ganz oben auf der CIO-Wunschliste steht derzeit die Notfallplanung: „Business Continuity“, gefordert von zahlreichen gesetzlichen Bestimmungen zur Risikovorsorge, ist zum Top-Thema avanciert. Nach den Ursachen dieser Entwicklung muss man nicht lange suchen: Schadenshöhe und Eintrittswahrscheinlichkeit von menschen- und naturverursachten Störfällen nehmen seit 20 Jahren drastisch zu (s. Abb.).



(Quelle: DIE ZEIT/Münchener Rück)

Ein Trend, der nicht nur Versicherungen zum Handeln zwingt. Da zahlreiche Schäden nicht versicherbar sind, steigt der Druck auf das IT-Management, auch bei bislang für unwahrscheinlich gehaltenen Störfällen wie längerem Stromausfall oder Wasser- und Sturmschäden eine Betriebsfortsetzung zu ermöglichen.

Das aber ist leichter gesagt als getan. Denn selten liegt eine aktuelle Übersicht maximal tolerierbarer Ausfallzeiten vor – oft ist nicht einmal verlässlich dokumentiert, welche IT-Anwendungen und -Systeme die Geschäftsprozesse tatsächlich benötigen. Und selbst da, wo Disaster Recovery-Maßnahmen getroffen wurden, existiert meist kein erprobtes Konzept für den Notbetrieb. Was aber hilft es, wenn bei Stromausfall die Kommunikationssysteme durch Handys ersetzt werden – alle wichtigen Telefonnummern aber im CRM gespeichert sind?

Nicht zuletzt müssen die Kosten der Maßnahmen im Rahmen bleiben, denn schon *Jean-Baptiste Molière* (1622-1673) wusste:

Die meisten Menschen sterben nicht an ihren Krankheiten, sondern an ihren Medikamenten.

1 Security News

1.1 Frischzellenkur

Am 31.01.2006 erschien Version 4.0 des populären Netzwerkscanners nmap – zwei Jahre nach Veröffentlichung der Vorgängerversion 3.50. Die neue Fassung enthält mehr als 230 Änderungen. Als Highlights stechen die Neuentwicklung der Port-Scanning-Engine und des Mechanismus zum Senden von Raw-Ethernet-Frames hervor. Dabei wurden Perfomance und Portabilität verbessert; insbesondere ist nmap nicht mehr auf die Socket-Implementierung des benutzten Betriebssystems angewiesen. Zusätzlich wurde die Datenbank zur Erkennung von Zielsystemen stark erweitert.

Erste Tests hinterlassen einen guten Eindruck. So wird die Einarbeitung in die neuen Features zur Entdeckungsreise – dabei ist die überarbeitete Dokumentation sehr hilfreich.

1.2 Zertifikatsbedarf

Dieser Winter verläuft unruhig für Zertifikatsanbieter auf dem deutschsprachigen Markt. Nachdem die deutsche TC Trustcenter GmbH am 14.09.2005 Insolvenz angemeldet hat, ist sie am 18.01.2006 von dem globalen Anbieter GeoTrust übernommen worden. Damit bleibt ein nach dem deutschen Signaturgesetz akkreditierter Zertifizierungsdiensteanbieter erhalten.

Dank einer Finanzspritze der österreichischen Großbanken gibt es auch für den Dienstanbieter a.trust GmbH nach dem Ausstieg von Telekom Austria und ÖNB wieder eine Perspektive. Beide Unternehmen kämpfen mit mangelnder Nachfrage nach qualifizierten Zertifikaten, deren Mehrwert einem Großteil der möglichen Nutzer noch nicht nahe zu bringen ist. Einen Bedarf für günstige Zertifikate scheint es hingegen zu geben, wie die Statistik der gemeinnützigen Organisation CAcert zeigt: Dort wurden seit 2004 knapp 100.000 kostenlose Zertifikate basierend auf einem Web of Trust ausgestellt.

1.3 13. DFN-CERT Workshop

Dass die Zahl 13 auch positiv belegt sein kann, zeigt die 13. Ausgabe des DFN-CERT Workshops „Sicherheit in vernetzten Systemen“, der am 01. und 02.03.2006 wie gewohnt in Hamburg stattfinden wird. Auch 2006 werden wieder über 300 Teilnehmer aus Forschung, Unternehmen und Behörden die interessanten Vorträge auf sehr hohem Niveau verfolgen.

Als eingeladener Sprecher wird diesmal Bill Cheswick vortragen – Titel seines Vortrags: „My Dad's Computer, Microsoft and the future of Internet Security“. Neben weiteren interessanten Themen wird Stefan Kelm von Secorvo Erfahrungen mit „Honeypots und Honeywall in der Praxis“ vorstellen.

1.4 Neue Malware-Allianz

In jüngster Vergangenheit wurden zahlreiche neue, immer leistungsfähigere Tools für Honeypots veröffentlicht (SSN 5/2005, SSN 8/2005). Ein prominentes Beispiel ist das Tool mwcollect. Dabei handelt es sich um ein kleines, auf Linux- und BSD-Systemen laufendes Tool, das Windows-Schwachstellen simuliert und somit Viren, Würmer und andere elektronische Ferkeleien („Malware“) sammeln kann. mwcollect öffnet bestimmte, oft von Malware verwendete Ports (zum Beispiel den TCP-Port 2745, einen der „Bagle“-Ports), simuliert dort bestimmte Dienste, nimmt Netzwerkverbindungen auf diesen Ports an und zeichnet sämtliche ankommenden Pakete auf. Die protokollierten Daten können anschließend detailliert ausgewertet werden.

Am 03.02.2006 wurde nun die Gründung der „mwcollect Alliance“ angekündigt. Mitglieder dieser Gruppe, vor allem Antivirus- und Schwachstellenforscher, sammeln mit mwcollect Schadsoftware und stellen diese einander für Analysen zur Verfügung. Deren Ergebnisse helfen, das Schadenspotenzial neuer Viren und Würmer besser einzuschätzen und entsprechende Sicherheitsmaßnahmen zu treffen. An der Allianz beteiligen kann sich jeder, der bereits ist, die selbst protokollierten Daten allen anderen Mitgliedern zur Verfügung zu stellen.

1.5 Jäger und Sammler

Die Sammler haben einen Dämpfer bekommen: Am 25.01.2006 stellte das Landgericht Darmstadt in der Berufung letztinstanzlich klar, dass T-Online bei Flatrate-Kunden die IP-Adressen unmittelbar nach Beendigung einer Verbindung löschen muss – und das jeweils übertragene Datenvolumen nicht einmal erheben darf. Für Zuwiderhandlungen wurde ein Ordnungsgeld von € 100.000 festgesetzt.

Ein Sieg des Datenschutzes auf ganzer Linie, könnte man meinen. Wenn da nicht die Jäger wären: Am 21.02.2006 setzte der EU-Rat die vom Europäischen Parlament im Dezember 2005 verabschiedete EU-Richtlinie zur Vorratsdatenspeicherung von Verbindungsdaten in Kraft. Damit sind deutsche Internet-Provider in spätestens drei Jahren zur sechs- bis 24-monatigen Speicherung anfallender Verbindungsdaten verpflichtet.

1.6 GnuPG Bug

Bei einer automatisierten Signaturprüfung akzeptiert die freie, PGP-kompatible Open-Source-Implementierung GnuPG unter Umständen eine ungültige Signatur, wie am 15.02.2006 auf der GnuPG-Mailingliste bekannt gemacht wurde: Findet der Prüfalgorithmus die Signatur nicht, liefert er den Wert „0“ zurück, der ohne Kontextauswertung als „success“ interpretiert werden kann. Betroffen sind alle Versionen bis 1.4.2; ein Update (1.4.2.1) wird empfohlen.

1.7 NIST Neuigkeiten

An dieser Stelle sei auf die zahlreichen Publikationen der Computer Security Division des amerikanischen National Institute of Standards and Technology (NIST) hingewiesen. Im ITL Bulletin für Februar 2006 wurde eine erheblich überarbeitete Version der „NIST Special Publication 800-40, Creating a Patch and Vulnerability Management Program“ vorgestellt, die eine systematische Vorgehensweise für die Etablierung eines regelmäßigen und zuverlässigen Patch-Managements empfiehlt. Im Anhang finden sich umfangreiche Tabellen mit Links zu Anbietern von Patch Management Software und Patch-Quellen der verbreitetsten Betriebssysteme, Client- und Server-Applikationen.

Zu vielen weiteren aktuellen Themen der IT-Sicherheit finden sich in der Publikationsübersicht hilfreiche Dokumente, von denen einige in der letzten Zeit aktualisiert worden sind. Die wichtigsten sind auch über den security-finder erreichbar.

1.8 Anonym, aber langsam

Neben dem (in den SSN 08/2005 vorgestellten) Projekt AN.ON, das wegen des Auslaufens der Fördermittel in Bälde kostenpflichtig werden wird, gibt es seit der Konferenz Shmoocon 2006 ein weiteres Anonymitätsprojekt: Das Privacy Operating System "Anonym.OS".

Diese Distribution, die als Live-CD verfügbar und in jedem Standard-PC bootfähig ist, basiert auf dem Sicherheitsbetriebssystem OpenBSD 3.8 und ist auf die Anonymisierung und Verschlüsselung von Netzverbindungen spezialisiert. Sie verwendet Tor als Gateway für das anonymisierte Internet. Gegenüber dem Netzumfeld tarnt sich Anonym.OS als "Windows XP Service Pack 2". Damit ist erstmals eine Anonymizer-Lösung verfügbar, die es Laien mit sehr geringen technischen Grundkenntnissen ermöglicht, sich einer Anonymisierungsinfrastruktur anzuschließen.

Allein die Performance des Tor-Netzwerkes trübt die Anwendbarkeit: Man fühlt sich spontan in die Zeiten der 1200-9600 Baud-Modemanbindungen zurückversetzt. Zur Verbesserung der Anonymitäts-Bandbreite hilft nur eines: Baut Tor-Server!

2 Secorvo News

2.1 Secorvo College aktuell

Über die Winterpause wurden alle „Bestseller“-Seminare von Secorvo gründlich über-

arbeitet. Das Ziel: Eine deutliche Ausweitung des Praxisanteils.

Das erste Seminar hat die Premiere nun hinter sich: Die Neufassung des PKI-Seminars Anfang Februar erreichte mit einer Gesamtnote von 1,4 eine sehr gute Bewertung. Insbesondere die Mischung aus Theorie und Praxis mit Demonstrationen, Workshops und der praxisnahen Aufbereitung der Themen in den einzelnen Vorträgen kam sehr gut an.

Ähnlich „frisch" präsentiert sich das Seminar „Information Security Management – von A(udit) bis Z(ertifizierung)" vom 03. bis 07.04.2006. Gleiches gilt für das vollständig neu konzipierte Seminar Kommunikationsschutz und Datensicherheit – intern, extern, mobil am 25. bis 27.04.2006.

Programme und Anmeldung (auch online): http://www.secorvo.de/college

2.2 Awareness Symposium

Vom 02. bis 03.05.2006 findet das inzwischen schon vierte „Security Awareness Symposium" in Karlsruhe statt. Wie in den Vorjahren werden zahlreiche Unternehmen ihre Aktivitäten zur Sensibilisierung der Mitarbeiter für Informationssicherheit vorstellen. Das Programm ist derzeit in Abstimmung – es sind wieder ideenreiche und anregende Präsentationen und Diskussionen zu erwarten. Schon jetzt können Sie sich die Teilnahme an diesem Event durch frühzeitige Anmeldung sichern.

2.3 security-finder.de

Die vor knapp einem Jahr freigeschaltete virtuelle Online-Bibliothek security-finder.de wächst und gedeiht: Knapp 600 Dokumente zu IT-Sicherheit und Datenschutz sind darin inzwischen zu finden, kategorisiert und versehen mit einer aussagekräftigen Zusammenfassung und Bewertung.

Für Interessierte gibt es nun einen kostenfreien „Schnupperzugang" (Benutzer: gast, Passwort: gast), über den Struktur und Aufbau des security-finders und etwa 60 ausgewählte Dokumente zugänglich sind.

3 Veranstaltungshinweise

Februar 2006	
28.02. - 03.03.	Black Hat Europe 2006 (Black Hat, Amsterdam/NL)
März 2006	
01.-02.03.	DFN-CERT Workschop (DFN-CERT, Hamburg)
09.-15.03.	CeBIT 2006 (Deutsche Messe AG, Hannover)
27.-28.03.	Datenschutz und Datensicherheit – DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D*A*CH Security 2006 (GI/Bitkom/TeleTrusT, Düsseldorf)
April 2006	
03.-07.04.	Information Security Management (Secorvo College, Karlsruhe)
25.-27.04.	Kommunikationsschutz und Datensicherheit (Secorvo College)
Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
16.-18.05.	Forensic Lab (Secorvo College, Karlsruhe)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)

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

Secorvo Security News
März 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 3, 5. Jhrg. 2006
Stand 26. März 2006

ISSN 1613-4311

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

Inhalt

Editorial: Der Grüffelo

„Zum Grüffelo? Sag, was ist das für ein Tier?“
„Den kennst Du nicht? Dann beschreib ich ihn Dir...“
Axel Scheffler, Julia Donaldson

Wie alt sind Ihre Kinder? Zwischen vier und zwölf? Dann kennen Sie zweifellos das wunderschöne Kinderbuch „Der Grüffelo“. Allen anderen sei die Geschichte schnell erzählt: Auf dem Weg durch den Wald begegnet die Maus ihren ärgsten Feinden – dem Fuchs, der Eule und der Schlange. Listig schlägt sie alle drei mit der Behauptung in die Flucht, sie sei mit dem Grüffelo verabredet – einem schrecklichen Tier, das sich bevorzugt von Fuchsspieß, gezuckerter Eule und Schlangenpüree ernähre.

Überrascht muss die Maus jedoch feststellen, dass es den Grüffelo tatsächlich gibt – und er genau so aussieht, wie sie ihn den Tieren in schillernden Worten beschrieben hat. In höchster Not behauptet sie, alle Tiere im Wald hätten Angst vor ihr – und beweist es, indem sie mit ihm Schlange, Eule und Fuchs aufsucht. Die nehmen sofort Reißaus, der Grüffelo aber ist tief beeindruckt – und ergreift selbst die Flucht, als die Maus erklärt, sie verspüre plötzlich Appetit auf eine Portion Grüffelogrütze ...

Die Erfolgsstrategie der Maus ist so einfach wie entwaffnend – der japanischen Kampfkunst Aikido ähnlich, die die Kraft des Angreifers nicht blockt, sondern umlenkt. Eine Technik, der sich auch die Scam Baiter bedienen, die die Versender von Betrugs-E-Mails der „Nigeria-Connection“ in Korrespondenzen verstricken und zur Versendung eigener Fotos verleiten. Möglicherweise ist dies eine Erfolgsstrategie im rechtsvollzugsarmen Cyberspace. Man stelle sich vor: Empfänger von Phishing-Mails, die die Betrüger mit falschen TANs auf präparierte Konten locken, als vorgebliche Geldboten Polizeikonten zur Überweisung anbieten oder mit Honeypots Hackern einen Crack vortäuschen – und beim Datendownload den Sound „Hab’ mich beim Hacken erwischen lassen“ installieren.

Keine Selbstjustiz – aber ein bisserl Sand im sich gerade organisierenden kriminellen Online-Getriebe könnte reinigend wirken.

1 Security News

1.1 Symantec Threat-Report

Am 07.03.2006 veröffentlichte Symantec die Ergebnisse ihres Sicherheitsreports für die zweite Jahreshälfte 2005. Danach ist ein deutlicher Anstieg der Internetkriminalität festzustellen, die vor allem professioneller und profitorientierter geworden ist. Insbesondere die Gefährdungen durch Bot-Netze und Schwachstellen in Webanwendungen haben deutlich zugenommen. Phishing bleibt eine ernst zu nehmende Bedrohung. Erschreckend: Die Entwicklung der Zahl neu entdeckter Viren und Würmer.

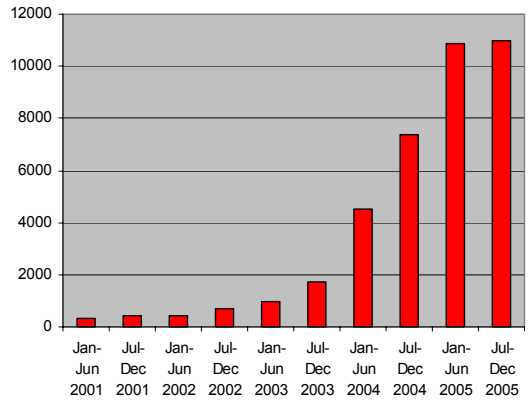


Abb.: Neue Viren und Würmer [Symantec]

1.2 Neues BSI-GSHB online

Die in den SSN 01/2006 vorgestellte aktualisierte Version des IT-Grundschutzhandbuches mit Unterteilung in IT-Grundschutz-Standards (BSI-Standard 100-1: Managementsysteme für Informationssicherheit, BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz) und IT-Grundschutzkataloge ist seit Anfang März online als PDF-Version verfügbar. Das Information Security Management basiert nun auf dem internationalen Standard ISO 27001; weite Teile des bisherigen IT-GSHB sind neu sortiert in den Katalogen zu finden. Die Änderungen wurden am 14.03.2006 auf der CeBIT vorgestellt.

1.3 Virenverseuchte Katzen?

Ja, Sie lesen richtig – mit Vogelgrippe hat dieser Beitrag allerdings rein gar nichts zu tun. Auf der diesjährigen Percom (IEEE International Conference on Pervasive Computing and Communications, 13.-17.03. 2006) wurde das Paper „Is your cat infected with a Computer Virus?" von Andrew Tanenbaum et al. zum Thema RFID-Viren mit dem Best Paper Award ausgezeichnet. Als proof-of-concept wurde ein Virus entwickelt, der sich in den 127 Zeichen fassenden Transponderspeicher eines Chips einschleusen lässt und die RFID-Middleware von Oracle infiziert.

1.4 Bürger-CERT

In seinem Newsletter vom 03.03.2006 stellt das BSI das gemeinsam mit Mcert gestartete Projekt Bürger-CERT vor. Ziel ist es, Bürger und kleine Unternehmen vor aktuellen Gefährdungen der IT-Sicherheit zu warnen und zu informieren. Die kostenlos herausgegebenen technischen Warnungen unterscheiden sich bislang jedoch kaum von anderen ebenfalls kostenfreien Diensten wie beispielsweise den DFN-CERT Advisories.

1.5 déjà-vu: Punkt im Pfad

Am 10.03.2006 berichtete Heise über eine von Reed Arvin entdeckte Möglichkeit, Berechtigungen durch ein installiertes ActiveState Perl zu eskalieren. ActiveState Perl stellt bei der Installation das Verzeichnis mit den Binaries an den Beginn des Systemsuchpfades und räumt dort allen Benutzern Schreibrechte ein. Dadurch kann ein nicht-privilegierter Benutzer einem Administrator beliebige Programme oder sogar DLLs unterschieben, die dann im Kontext des Administrators ausgeführt werden.

Dieses Verhalten ist unschön – aber alles andere als neu. Schon am 18.03.1993 wurde in der Unix-FAQ 2.13 davor gewarnt, den ´.´ (d. h. das aktuelle Verzeichnis, in dem sich beliebige Benutzeranwendungen befinden können) im Pfad zu führen. Auch 13 Jahre danach ist bei allen Betriebssys-

temen angeraten, den Pfad und darüber mögliche Kompromittierungsmöglichkeiten genau im Auge zu behalten.

1.6 Berechtigungseskalation

Ein weiteres Beispiel von Eskalations-Berechtigungen wurde von Ramon Kukla bei der Antivirensoftware Antivir von Avira (ehemals H+B EDV) festgestellt und am 11.03.2006 in full-disclosure veröffentlicht.

Die Fehlerursache liegt hier im Dienst „AntiVir PersonalEdition Classic Planer“, einem zum Virenschutz gehörenden Zeitplanungsdienst, der im System-Kontext läuft. Bei Updates wird über diesen Dienst ein Report erzeugt, der mit der Windows-Anwendung Notepad angezeigt wird – auch mit Systemberechtigungen, versteht sich. Ein Benutzer kann mit diesem Notepad System- und Konfigurationsdateien öffnen und ändern, obwohl er dazu gar keine Berechtigung besitzt. Auch die kostenpflichtige Premium-Variante der Lösung soll betroffen sein; eine Aktualisierung wird daher dringend empfohlen.

1.7 „Setzen, Sechs!“

Man könnte es für eine Satire halten: Die Washington Post berichtete am 15.03.2006 über die Ergebnisse der jährlichen Analyse der Sicherheit staatlicher Stellen in den USA. Eine der am schlechtesten bewerteten Behörden ist das Department for Homeland Security: Sie erhielt ein glattes „F“ für „failed“ – im dritten Jahr in Folge. Pikanterweise ist diese Behörde unter anderem für Terrorbekämpfung und „cyber security“ zuständig.

1.8 Datenbüchsen öffnen

Bereits im Oktober 2005 wurde der NIST Interagency Report 7250 Cell Phone Forensic Tools: An Overview and Analysis veröffentlicht. Dieser Bericht ist angesichts der am 27.02.2006 gemeldeten Handy-Trojaner brandaktuell: Er führt auf über 180 Seiten in guter und sehr detaillierter Form in die für forensische Analysen von mobilen Geräten verfügbare Software ein.

Insgesamt wurden 12 Toolkits evaluiert. Die im Dokument betrachteten Telefonie-Geräte haben teilweise einen engen Bezug zu Personal Digital Assistants (PDA), was auch durch die ihnen zu Grunde liegenden Betriebssysteme deutlich wird (Windows Mobile, Palm OS, RIM OS und Symbian).

Speziell für Manager und technische Entscheider, aber auch für Angreifer liest sich das Dokument zwischen den Zeilen wie eine Offenbarung hinsichtlich der Machbarkeit von Angriffen auf sensitive Daten in Mobiltelefonen. Bleibt zu ergänzen, dass ein starker Trend zu beobachten ist, Login/ Passwort-Kombinationen, PINs, TANs etc. auf solchen Geräten zu speichern. Zweifellos zur großen Freude derjenigen, die ein solch gut gefülltes Osterei „finden“.

1.9 Open Source Inspektion

Die ersten Ergebnissen der Open Source-Analyse der US-Regierung lesen sich auf den ersten Blick wie eine weitere Metrik, die die Welt nicht braucht. Die Ergebnisse liegen in einer Tabelle online vor und geben die Zahl der festgestellte Bugs pro 1.000 Zeilen Code an.

Die Messbarkeit im Bereich Sicherheit ist ein wichtiges, aber schwieriges Feld. Erfolgreiche Metriken erlauben konkrete Aussagen über betrachtete Entitäten. Auf den ersten Blick scheint die Metrik Fehler/ kLoC (1.000 Lines of Code) diesbezüglich wenig aussagekräftig. Sie ermöglicht zwar eine grobe Einschätzung, lässt aber keine Vergleichbarkeit zwischen den Projekten zu. Beispielsweise kann ein schwerer Fehler im Betriebssystem fataler sein als zehn leichte Bugs im Browser.

Der Ansatz der Autoren von Coverity geht jedoch über die reine Generierung von Metriken hinaus und nimmt mit den Verantwortlichen der betroffenen Projekte Kontakt auf, erläutert die festgestellten Schwachstellen und trägt so ein gutes Stück zur Verbesserung der Qualität von Open Source bei. Detailliertere Reports können auf Anfrage und nach erfolgter Registrierung bei Coverity heruntergeladen werden.

2 Secorvo News

2.1 Secorvo College aktuell

Der persönliche Kontakt zu den Referenten und die Möglichkeit, individuelle Fragestellungen in die Vorträge einfließen zu lassen, werden von unseren Seminarteilnehmern sehr geschätzt. Ein Mehrwert, dem wir mit unserem neuen Angebot Individuelles Coaching zukünftig noch mehr Gewicht verleihen. Sie erhalten im Seminarverlauf zusätzlich die Möglichkeit, individuelle Fragestellungen im „Vier-Augen-Gespräch“ mit einem ausgewählten Secorvo Security Consultant zu diskutieren.

www.secorvo.de/college

2.2 Wem die Stunde schlägt

Die Geschichte der Hans Unsicher GmbH, Ein (IT-)Drama, wie das Leben es schreibt. Sie erzählt vom Umgang des Mittelstands mit doch nicht ganz so unwahrscheinlichen Risiken („Uns wird schon nichts passieren“), vom Leichtsinn in Raten, versteckt in kleinen, alltäglichen Unternehmensentscheidungen: Ein etwas anderes Theaterstück über die ganz normalen Risiken des Unternehmerdaseins.

Uraufführung am 23.05.2006 in Rust (Anmeldung und nähere Informationen).

2.3 „DuD” im security-finder

Die von Secorvo entwickelte virtuelle Bibliothek zu IT-Sicherheit und Datenschutz erhält exklusive Inhalte: Ab dem 01.04.2006 werden Abonnenten des security-finder.de ausgewählte Beiträge aus früheren Jahrgängen der im Vieweg-Verlag erscheinenden Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) digital zugänglich gemacht – eine starke Bereicherung der inzwischen auf über 600 sorgfältig ausgewählten und kommentierten Publikationen angewachsenen elektronischen Fachbibliothek.

3 Veranstaltungshinweise

März 2006	
27.-28.03.	Datenschutz und Datensicherheit – DuD 2006 (COMPUTAS, Berlin)
28.-29.03.	D*A*CH Security 2006 (GI/Bitkom/TeleTrusT, Düsseldorf)
April 2006	
03.-07.04.	Information Security Management (Secorvo College, Karlsruhe)
25.-27.04.	Kommunikationsschutz und Datensicherheit (Secorvo College)
29.04. - 02.05.	15th EICAR Annual Conference (Eicar, Hamburg)
Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
16.-18.05.	Forensic Lab (Secorvo College, Karlsruhe)
23.05.	„Wem die Stunde schlägt“ (amec spie/Lampertz, Rust)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
30.05. - 01.06.	Web-Application Security (Secorvo College, Karlsruhe)

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

Secorvo Security News
April 2006

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

Nr. 4, 5. Jhrg. 2006
Stand 26. April 2006

ISSN 1613-4311

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

Inhalt

Editorial: Small World!

Wir kennen uns alle. Wenn nicht direkt, so über maximal sechs Ecken: Die These der „six degrees of separation" aus der 1929 erschienenen Kurzgeschichte *Chains* des ungarischen Schriftstellers Frigyes Karinthy (1887-1938) erlangte 38 Jahre später durch den Psychologen Stanley Milgram (1933-84) Berühmtheit, der dafür den Begriff Kleine-Welt-Phänomen prägte. Seitdem beschäftigt sie nicht nur Forscher wie Duncan J. Watts, die Karinthys These per Modell zu bestätigen versuchen, sondern wurde erfolgreich in Geschäftsmodelle (wie z. B. Online-Kontaktnetzwerke) umgesetzt.

Bewiesen ist Karinthys These bisher nicht, widerlegt werden konnte sie allerdings auch nicht. Selbst in OpenBC, mit einer Million Benutzern eine der erfolgreichsten Online-Kontaktbörsen, lässt sich auch zu Neu-Usern keine Kontaktkette finden, die länger ist als sechs.

Auch Vertrauensnetze wie das „Web of Trust" von PGP profitieren von kurzen Vertrauensketten – je kürzer, desto größer das Vertrauen in die Identität eines fremden Schlüsselinhabers. Voraussetzung für diese enge Vermaschung ist dabei die Verknüpfung der Beziehungsdaten: Aus mehr Beziehungen resultiert eine kürzere Kette – und damit mehr Vertrauen.

Sollten wir also mehr Beziehungswissen preisgeben, um mehr Vertrauen zu erreichen? Das zu glauben wäre ein typischer Naturalistischer Fehlschluss – ein unzulässiges Ableiten von Soll- aus Ist-Zuständen. Denn je enger wir „zusammenrücken", desto wichtiger wird der Schutz der Privatsphäre – sofern wir eine erhalten wollen.

Auch in der Online-Enzyklopädie Wikipedia wirkt das Small-World-Phänomen („Six degrees of Wikipedia"): „Kleine-Welt-Phänomen" und „Naturalistischer Fehlschluss" sind über fünf Links verbunden (Soziale Netzwerke – Soziologie – Philosophie – Sprachphilosophie – G. E. Moore). Bis zum „Datenschutz" ist die Kette allerdings einen Klick länger (Soziale Netzwerke – Herrschaft – Gesetze – Grundgesetz – Grundrechte – Informationelle Selbstbestimmung).

1 Security News

1.1 GnuPG legt nach

Am 03.04.2006 ist eine neue Version der freien Krypto-Software GnuPG erschienen. Während frühere Versionen in erster Linie Sicherheitslücken bereinigten, enthält Version 1.4.3 etliche interessante neue Features: Neben dem deutlich verbesserten Management von GPG-Schlüsseln unterstützt GnuPG nun einige der DNSSEC-Erweiterungen direkt. Dabei geht es in erster Linie darum, kryptographisches Schlüsselmaterial sowie Zertifikate im DNS speichern und von dort abrufen zu können.

GnuPG kann jetzt auf diese Erweiterungen zugreifen. Interessant ist dies deshalb, weil DNSSEC zwar schon seit Jahren „kurz vor der Einführung steht“ (vgl. SSN 05/2004, SSN 04/2005), bis heute aber nur wenig bis gar kein Gebrauch davon gemacht wird – ein Grund dafür war die mangelnde DNSSEC-Unterstützung in den Anwendungen.

1.2 ... und keiner merkt's

Wie erst am 31.03.2006 in einem Report veröffentlicht, waren die Root-Nameserver im Februar dieses Jahres wieder einmal Ziel einer großflächigen Denial-of-Service-Attacke. Die Angreifer setzten Bot-Netze ein, um die DNS-Server mit übergroßen Paketen zu beschäftigen.

Pikanterweise versuchten die Angreifer eine recht neue Erweiterung des DNS-Protokolls auszunutzen: EDNS0 wurde erst im Rahmen der DNSSEC-Aktivitäten spezifiziert und implementiert, um die ehemals geltende Größenbeschränkung von 512 Bytes pro DNS-Paket aufzuheben, damit beispielsweise kryptographische Schlüssel via DNS transportiert werden können (s.o.).

Wie schon bei früheren Angriffen wirkte die Attacke nur bei schlecht konfigurierten Nameservern. Geholfen hätte auch diesmal die korrekte Konfiguration der Nameserver gemäß längst bekannten Best-Practice-Methoden – nicht besondere Schutzmechanismen à la DNSSEC. Interessanterweise hat jedoch auch diesen Angriff kaum ein Endbenutzer wahrgenommen...

1.3 IPv6-Werkzeugkasten

Seit der cansecwest/core06 ist das dort Anfang April 2006 vorgestellte „IPv6 Attack Toolkit“ von THC/VH auch für die Allgemeinheit zur praktischen Verwendung verfügbar. Die darin enthaltenen 12 Spezialwerkzeuge und die zu Grunde liegende „IPv6 packet factory library“ demonstrieren u. a. Schwachstellen in IPv6, die auf Angriffsstrategien wie Denial-of-Service und Man-in-the-Middle beruhen. Die Packet Library selbst sowie der verfügbare Sourcecode (derzeit noch auf Linux beschränkt) ermöglichen sowohl die einfache Erstellung weiterer „Werkzeuge“, als auch die Änderung der Paketsignaturen, um Intrusion Detection Systemen zu entwischen.

Mit diesem Werkzeugkoffer existiert erstmals eine abgestimmte Tool-Sammlung für Netzwerksicherheitsanalysen von IPv4 mit parallel zugelassenem IPv6.

1.4 VM Based Rootkits

Eine neue Variante von Rootkits wurde von Forschern der Michigan University und Microsoft Research vorgestellt: Durch die Kombination von Rootkits mit der Technik virtueller Maschinen entstehen perfide aber auch technisch anspruchsvolle Angriffsmöglichkeiten. Die im Rahmen des Projekts „SubVirt“ auf Basis von VirtualPC und VMware entwickelten Tools übernehmen dabei komplett die angegriffenen Systeme unter Windows XP oder Linux und emulieren das ursprüngliche Betriebssystem innerhalb einer virtuellen Maschine. Eine zweite virtuelle Maschine kann für beliebige Angriffszwecke wie beispielsweise den Betrieb eines Phishing Webservers verwendet werden.

Das Fatale an dieser Technik ist, dass die Übernahme für den Benutzer nicht erkennbar ist: Da die Benutzermaschine durch die VM-Umgebung kontrolliert wird, fanden die Forscher in ihren Untersuchungen lediglich den deutlich verlängerten Bootvorgang und

eine verminderte 3D-Leistung als Indizien. Da solche Virtual Machine Based Rootkits (VMBRs) sogar Shutdown-Prozesse emulieren und das System in standby versetzen, ist selbst ein Neustart des Benutzersystems unter Kontrolle des Rootkits. Nur wenn das System wirklich „aus“ ist, kann von einem alternativen Medium gebootet und das Rootkit festgestellt werden.

Die Ergebnisse der Forschungen und weitere Schutzmaßnahmen sind im Paper „SubVirt: Implementing malware with virtual machines" zusammengefasst, welches für das diesjährige IEEE Symposium on Security and Privacy eingereicht wurde.

1.5 Selbsthilfe-Ecke

Gegen Spam gibt es eine Reihe von technischen Gegenmaßnamen wie Spamfilter und Greylisting. Eine der wirksamsten Methoden ist aber immer noch, Vorsicht bei der Preisgabe oder Weitergabe seiner E-Mail-Adresse walten zu lassen.

Aber was tun, wenn man sich Informationen zusenden lassen oder auf einer Website registrieren will? Ein Weg ist die Nutzung von Einmal- oder Wegwerf-E-Mail-Adressen, vorgeschlagen von Stefan Kelm auf dem Anti-Spam-Symposium 2003. Dabei helfen Angebote wie Spamgourmet: Dort können temporäre E-Mail-Adressen eingerichtet werden, die eingehende E-Mails an die „echte“ eigene E-Mail-Adresse weiterleiten. Nach einer zuvor festgelegten Zahl eingegangener E-Mails wird die Adresse vom Anbieter automatisch gelöscht. Dem Anbieter muss man allerdings vertrauen, dass er die echten Adressen keinem Dritten preisgibt.

1.6 Kapitulation

Das Bundeskabinett hat am 25.04.2006 einen Gesetzentwurf aus 16 Einzelmaßnahmen zum „Abbau bürokratischer Hemmnisse insbesondere der mittelständischen Wirtschaft“ verabschiedet. Darunter: Die Anhebung des Schwellwerts für die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten. Die soll zukünftig nur noch bestehen, wenn mindestens 10 (und nicht wie bisher fünf) Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt sind. Schon am 22.07. 2005 hatten die Länder Hessen und Niedersachsen einen Gesetzentwurf im Bundesrat eingebracht, der das Quorum auf mindestens 20 Arbeitnehmer anheben will; am 23.09.2005 winkte der Bundesrat diesen Entwurf durch. Die Festlegung des Kabinetts auf ein Quorum von 10 riecht verdächtig nach Formelkompromiss – eine inhaltliche Begründung gibt es nicht.

Tatsächlich wirkt die vermeintliche Entbürokratisierungsmaßnahme wie eine Kapitulation vor dem faktischen Vollzugsdefizit in kleinen und Kleinstunternehmen: Die wenigsten kommen bisher der seit 1978 bestehenden Pflicht zur Berufung eines betrieblichen Datenschutzbeauftragten nach, und selbst das oft nur pro forma.

Allerdings war es noch nie ein Ausdruck besonderer Weisheit, bedauernswerte Ist-Zustände zu Soll-Zuständen zu erheben (siehe Editorial). Zwar würden durch diese Regelung über 90 % der deutschen Unternehmen von der Verpflichtung befreit – so viele der insgesamt knapp drei Millionen Betriebe beschäftigen maximal 10 Mitarbeiter. Bestehen bleiben jedoch alle anderen Verpflichtungen: die Auskunftspflichten gegenüber den Betroffenen, die Festlegung und Einhaltung von Löschfristen, die Prüfung der Rechtmäßigkeit und Ordnungsmäßigkeit der Verarbeitung, die Schulung und Verpflichtung der Mitarbeiter auf das Datengeheimnis sowie eine gesetzmäßige Vertragsgestaltung bei Auftragsdatenverarbeitung und Übermittlung in Drittländer. Wer aber wird zukünftig in diesen Unternehmen die Sachkunde besitzen, für die Einhaltung des BDSG zu sorgen?

Bedenklich ist, dass hier mit dem Argument der Entbürokratisierung der Schutz des zentralen Grundrechts der freien Entfaltung der Persönlichkeit geschwächt wird. Denn außer Frage steht, dass die Konstruktion des betrieblichen Datenschutzbeauftragten in Deutschland erheblich zum international vergleichsweise hohen Schutz personenbezogener Daten beiträgt.

2 Secorvo News

2.1 Secorvo College aktuell

Gleich zwei neue Seminare stehen im Mai auf der Agenda von Secorvo College:

- IT-Sicherheitsaudits in der Praxis führt am **09.-10.05.2006** in die Grundlagen aussagefähiger Sicherheitsanalysen ein – von der Planung über die technische und organisatorische Prüfung bis zu Tools, rechtlichen Rahmenbedingungen und Praxiserfahrungen.
- IT-Outsourcing sicher gestalten trägt der wachsenden Bedeutung von Sicherheitsfragen bei der Auslagerung von IT-Prozessen Rechnung. Rechtsfragen, die Gestaltung von SLAs und die Einbindung in das Sicherheitsmanagement stehen im Zentrum des eintägigen Seminars am **11.05.2006**.

Programme und Online-Anmeldung:
www.secorvo.de/college

2.2 Security Awareness

Am 02.-03.05.2006 findet das inzwischen vierte „Security Awareness Symposium“ statt – mit Praxisberichten von Areva NP, DAK, SwissRe und T-Systems und einem intensiven Erfahrungsaustausch. Für Kurzentschlossene empfehlen wir die Online-Anmeldung – es gibt nur noch wenige freie Plätze.

2.3 Honeypots betreiben

Honeypots und Honeynets sind bereits seit einiger Zeit als effektive Sicherheitskomponente bekannt; dennoch waren viele Unternehmen sehr zurückhaltend, wenn es um den Aufbau entsprechender Honeypot-Umgebungen innerhalb der eigenen Infrastruktur ging. Dies scheint sich jetzt zu ändern: immer mehr Nachfragen haben uns veranlasst, die von Secorvo bereits seit einiger Zeit angebotenen Dienstleistungen in diesem Bereich in einem Leistungsangebot zusammen zu stellen und zu veröffentlichen.

2.4 Veranstaltungshinweise

Mai 2006	
02.-03.05.	Security Awareness Symposium 2006 (Secorvo, Karlsruhe)
09.-10.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
10.-11.05.	Datenschutzkongress 2006 (Euroforum, München)
11.05.	IT-Outsourcing sicher gestalten (Secorvo College, Karlsruhe)
23.05.	„Wem die Stunde schlägt“ (amec spie/Lampertz, Rust)
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
30.05. - 01.06.	Web-Application Security (Secorvo College, Karlsruhe)
Juni 2006	
06.-09.06.	ETRICS 2006 (Univ. Freiburg)
20.-22.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
21.-22.06.	Midvision 2006 (Karlsruher Messe)
25.-30.06.	Annual FIRST Conference 2006 (FIRST, Baltimore/US)
27.-28.06.	Lotus Notes Security (Secorvo College, Karlsruhe)
29.06.	Lotus Notes Security – advanced (Secorvo College, Karlsruhe)
Juli 2006	
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)

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

Secorvo Security News
Mai 2006

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

Nr. 5, 5. Jhrg. 2006
Stand 22. Mai 2006

ISSN 1613-4311

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

Inhalt

Editorial: Zauberlehrlinge

Seine Wort und Werke merkt ich und den Brauch
und mit Geistesstärke, tu ich Wunder auch.

Sie erinnern sich – es war einmal... Nein, nicht Ihre Deutschstunde, sondern die Diskussion der Entwürfe des deutschen Signaturgesetzes. Zehn Jahre ist es her, dass sich die Hoffnungen des deutschen eCommerce auf die vertrauensbildende Wirkung des 10-seitigen Gesetzestextes richteten. Noch im Evaluierungsbericht schrieb die Bundesregierung dem Signaturgesetz „eine Lokomotivfunktion für den Einsatz und die Verbreitung digitaler Signaturen“ zu.

In der Erwartung von Millionen Signaturzertifikaten wurden seitdem erhebliche Summen in Trust Center investiert, die „elektronische Form“ im BGB verankert und eine eigene Aufsichtsbehörde geschaffen.

Immer neue Güsse bringt er schnell herein,
Ach! und hundert Flüsse stürzen auf mich ein.

Allein: Der erhoffte Durchbruch blieb aus – die Lokomotive zog nicht. Darauf reagierte der Bund mit konfusen neuen Signatur-Kreationen (SSN 02/2003), verstärktem Aktionismus wie dem Signaturbündnis und der Erfindung vermeintlicher Killer-Applikationen wie der elektronischen Steuererklärung Elster (tatsächlich mit SSL realisiert) oder der Konzeptidee Jobcard – ohne Erfolg.

Ein verruchter Besen, der nicht hören will!
Stock, der du gewesen, steh doch wieder still!

Sieben akkreditierte Zertifizierungsdiensteanbieter existierten zu Hochzeiten. Nun stoppte auch die Datev die Ausgabe qualifizierter Zertifikate: Der Nutzen war „schwer zu vermitteln“, die wenigen ausgestellten Zertifikate rechtfertigten die Kosten nicht.

Herr, die Not ist groß!
Die ich rief, die Geister werd ich nun nicht los.

Die Reaktion des Marktes ist unzweideutig: Fortgeschrittene Signaturen genügen in der Praxis fast immer, das Restrisiko wiegt die erforderliche Mehrinvestition in qualifizierte meist nicht auf. Zeit zur Einsicht und zum Umsteuern: Regulatives Beharren wird den Erfolg nicht herbeizwingen – und ist in einer Marktwirtschaft nie eine gute Idee.

"In die Ecke, Besen, Besen! Seids gewesen.“

1 Security News

1.1 Sicherheitsstudie 2006

Seit 1991 wird – gesponsert durch das Department of Trade and Industry (DTI) – alle zwei Jahre eine Studie zu Sicherheitsvorfällen in Großbritannien erstellt (SSN 04/2002). Diese Studien dienen Unternehmen als Informationsquelle und zur Einschätzung des unternehmensrelevanten Risikos.

Der aktuelle, von PwC erstellte „Information Security Breaches Survey 2006“ wurde Ende April veröffentlicht. Obwohl die Zahl betroffener Firmen gegenüber dem Vorjahr gesunken ist, stiegen die Anzahl der insgesamt gemeldeten Sicherheitsvorfälle und der Mittelwert der Schäden (um 20 % auf 12.000 £). Bei „worst-case incidents“, insbesondere in Konzernen, lag der Mittelwert sogar bei 90.000 £. 68 % der befragten Unternehmen erwarten eine Zunahme der Sicherheitsvorfälle.

1.2 DoD-Sicherheitslücken

Wie das Pentagon am 28.04.2006 in einer Stellungnahme einräumte, wurde in ein öffentliches System der vom Militär genutzten Krankenversicherungsanwendung TRICARE eingebrochen. Dabei konnten zahlreiche, auch personenbezogene Daten abgezogen werden. Alle potentiell betroffenen Personen wurden informiert und über die Gefahr aufgeklärt, möglicherweise Opfer eines Identitätsdiebstahls zu werden.

Eine erneute Peinlichkeit, nachdem das Department for Homeland Security im März für ihr Sicherheitsniveau das dritte „failed“ in Folge kassiert hatte (SSN 03/2006). Immerhin kündigte das Department of Defense (DoD) an, weiterte Schutzmaßnahmen zu ergreifen.

1.3 IT-Grundschutz News

Nach den aktuellen BSI-Standards (SSN 01/2006) wurden im April auch die Grundschutzkataloge (Bausteine, Maßnahmen, Gefährdungen) auf den Webseiten des BSI im HTML-Format online gestellt. Die vollständigen Grundschutzkataloge können jetzt auch als ZIP-Datei geladen werden.

Zur Erleichterung der Zuordnung von ISO 27001 und IT-Grundschutz publizierte das BSI Ende April eine tabellarische Gegenüberstellung (19.04.2006). Die umfassende Tabelle stellt zum Einen dar, wie die neue Struktur des IT-Grundschutzhandbuchs die Inhalte der ISO 27001 abdeckt. Zum Anderen erleichtert die Tabelle das Auffinden der jeweils zugehörigen Bausteine und Maßnahmen.

1.4 Codename Secure Blue

Am 10.04.2006 gab IBM die Entwicklung einer „Secure Blue“ genannten Sicherheitsarchitektur bekannt, die die ressourcenaufwändige Ver- und Entschlüsselung von Daten direkt im Prozessor durchführen soll. Ein weiterer konsequenter Baustein des „Trusted Computing“, das das Ziel verfolgt, mehr Sicherheitsfunktionen in manipulationsichere Hardware zu verlagern, um bösartigem Code die Angriffsfläche zu entziehen.

Mit der Ankündigung, „die Sicherheit von Daten in Elektronikprodukten wie Konsumer-Elektronik, Medizintechnik und Digital-Media-Produkten“ zu verbessern, wurde jedoch auch die seit Jahren andauernde Kritik am Trusted Computing wieder lauter, die spekuliert, dass es dabei nur um die Durchsetzung kommerzieller Kopierschutzinteressen im Unterhaltungssektor geht (SSN 02/2003, SSN 04/2003).

Die Qualität von „Secure Blue“ wird sich sicher an dem komplexeren Schlüsselmanagement und der noch immer erforderlichen Entschlüsselung der Daten vor der Nutzung durch den Anwender erweisen.

1.5 GPG-Schutz für E-Mails

Das Open-Source-Projekt GnuPG hat Zuwachs bekommen: Pünktlich zum Linux-Tag wurde vom BSI am 26.04.2006 Version 1.0.1 des Gnu Privacy Guard for Windows (gpg4win) veröffentlicht. Es umfasst

neben Schlüsselmanagement-Tools ein Plugin für Outlook. Die Lösung setzt dabei allerdings auf die Mitwirkung des Anwenders – ein „Auslaufmodell“, denn unsere Erfahrungen haben gezeigt, dass Plugins in Punkto Benutzerakzeptanz weit hinter transparenten Gateway-Lösungen liegen.

Eine attraktive „Mischlösung“ bietet GPG-relay (aktuell Version 0.959): Es sorgt anhand eines konfigurierbaren Regelsatzes als lokaler POP3/IMAP-Proxy zuverlässig für eine transparente Ver- und Entschlüsselung aller ein- und ausgehenden E-Mails – unabhängig vom E-Mail-Client.

1.6 Behörden-Desktop

Im Rahmen des BSI-Projekts ERPOSS – Erprobung des Einsatzes von Open Source Software – wurde von der credativ GmbH ein Desktop auf Basis von Debian GNU/Linux 3.1 (sarge) und KDE 3.3 entwickelt. Seit dem 28.04.2006 steht er zum Download bereit. Der Desktop bietet eine Verschlüsselung des Dateisystems, eine vorkonfigurierte Personal Firewall, einen E-Mail-Client mit Virenschutz und Spamfilter und unterstützt die vom BSI entwickelte Verschlüsselungslösung Ägypten.

1.7 Hase und Igel Reloaded

Nach der iTAN – die inzwischen von zahlreichen Banken zum Schutz des Online-Banking vor Phishing eingeführt wurde – bietet die Postbank ihren Kunden als erste Bank bundesweit die mTAN an. Dafür wirbt sie seit dem 18.04.2006 mit einem TÜV-Gütesiegel, dessen proprietäre Prüfgrundlagen dem Zertifikat zu entnehmen sind.

Beim mTAN-Verfahren erhält der Kunde zu jeder beauftragten Transaktion eine SMS mit einer einmalig gültigen, transaktionsspezifischen TAN. Zusätzlich werden Zielkontonummer und Betrag in der SMS mitgeschickt. Die Sicherheit des Verfahrens ist hoch, wenn die hinterlegte Mobilfunknummer vor Phishing-Tricks gefeit ist.

Während viele Banken die Bedrohung durch Phishing schrittweise reduzieren, spielen die Phisher Hase und Igel und erfinden ständig neue Angriffsmethoden: Inzwischen versuchen sie, Kunden die Telefon-Banking PIN zu entlocken, z.B. über die Aufforderung zur Eingabe der Telefon-PIN auf gefälschten Webseiten.

Auch der Wechsel des Kommunikationsmediums wird zum Ausspähen der persönlichen Informationen genutzt. So gibt es Angriffe, die dazu auffordern, Rufnummern anzurufen, hinter denen sich ein fingiertes Phone-Banking System verbirgt.

Den besten Schutz vor derartigen Angriffen bietet – Technik hin, Technik her – immer noch die Aufmerksamkeit der Nutzer. Denn Banken fordern Kunden grundsätzlich nicht per E-Mail zur Preisgabe vertraulicher Informationen auf. Auch sollte bei E-Mails der Absender überprüft werden – die Postbank versucht dies durch das Signieren von E-Mails zu vereinfachen.

Realistische Hoffnung auf eine Verschnaufpause für Banken und Kunden besteht allerdings nur, wenn es den Banken gelingt, Mechanismen zu etablieren, durch die der Aufwand für Phisher so ansteigt, dass er den Nutzen des Betrugs überwiegt, z.B. aufgrund einer niedrigen Erfolgsquote.

1.8 Zukunftsblick

Am 06.-09.06.2006 wagt die Konferenz „ETRICS 2006“ an der Universität Freiburg einen Blick in die Zukunft der Informations- und Kommunikationssicherheit. Allein 19 international renommierte Keynote-Speaker lassen spannende und erkenntnisreiche Tage erwarten: Professor Acquisti (Carnegie Mellon University) beleuchtet, was der Datenschutz von der Verhaltensökonomie lernen kann, David Gavrock (Intel) gibt Insider-Einblicke in Trusted Computing und Professor Kemmerer (University of California) zieht Lehren aus 30 Jahren Computer Security.

Das gesamte Programm umfasst 70 Vorträge, zahlreiche Workshops, Tutorien und ein attraktives Begleitprogramm – für einen Teilnahmebeitrag von 150 € (Studenten) bis 350 €. Noch sind Anmeldungen möglich.

2 Secorvo News

2.1 Secorvo College aktuell

Dem Hacker über die Schulter schauen – und dann sogar selbst Hand anlegen und live Systeme attackieren: völlig legal und ohne schlechtes Gewissen. Das bietet Ihnen das „Live Hacking Lab“ am **20.-22.06.2006**: Drei Tage, in denen wir Sie in die aktuellen Hacking-Technologien einweihen. Schließlich sollten Sie wissen, was Ihre Gegner können, wenn Sie Ihre IT-Infrastruktur schützen wollen.

Wenn du weder den Feind noch dich selbst kennst,
wirst du in jeder Schlacht unterliegen.
Sunzi, Die Kunst des Krieges (ca. 500 v. Chr.)

2.2 SAS 2006 – Nachlese

Dass Security Awareness bei vielen Unternehmen hoch im Kurs steht, belegt die steigende Teilnehmerzahl des von Secorvo veranstalteten „Security Awareness Symposium“, das in diesem Jahr schon zum vierten Mal die Plattform für einen intensiven Erfahrungsaustausch bot. Die engagierten Praxisberichte lieferten zahlreiche Anregungen, Denkanstöße – und sicherlich auch den einen oder anderen Motivationsschub. Die Unterlagen aller Awareness-Symposien (2003 bis 2006) sind für Interessierte auch auf CD erhältlich.

2.3 Wer haftet?

In Kooperation mit der Neuen Messe Karlsruhe findet das nächste Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am Abend des ersten Messetags der Midvision 2006 statt: Am 21.06.2006 wird Professor Dr. Michael Bartsch von der renommierten (Kanzlei des Jahres 2003/2004 in Baden-Württemberg) und im IT-Recht besonders ausgewiesenen Kanzlei Bartsch und Partner zum Thema „Risiken, Pannen, Schäden – und wer haftet?“ vortragen. Beginn 18 Uhr, anschließend Networking am Büfett (bei Live-Übertragung der Spiele Niederlande-Argentinien und Elfenbeinküste-Serbien/Montenegro auf Großleinwand). Um Anmeldung wird gebeten.

3 Veranstaltungshinweise

Mai 2006	
28.05. - 01.06.	Eurocrypt 2006 (IACR, St. Petersburg/RU)
29.05.	Linux-Sicherheit (eco AK Sicherheit, Frankfurt)
Juni 2006	
06.-09.06.	ETRICS 2006 (GI, Freiburg)
20.-22.06.	Live Hacking Lab (Secorvo College, Karlsruhe)
21.06.	Risiken, Pannen, Schäden (KA-IT-Si, Karlsruher Messe)
21.-22.06.	Midvision 2006 (Karlsruher Messe)
25.-30.06.	18th Annual FIRST Conference (FIRST, Baltimore/USA)
27.-28.06.	Lotus Notes Security (Secorvo College, Karlsruhe)
29.06.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
Juli 2006	
13.-14.07.	DIMVA 2006 (GI, Berlin)
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/USA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/USA)

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

Secorvo Security News
Juni 2006

Dirk Fox, Stefan Gora, Kai Jendrian,
Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 6, 5. Jhrg. 2006
Stand 19. Juni 2006

ISSN 1613-4311

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

Inhalt

Editorial: Weltmeister

Bei der wichtigsten Nebensache der Welt zählt Deutschland auch 2006 allen Unkenrufen zum Trotz zu den Favoriten. Nicht nur da: Im internationalen Vergleich liegen wir bei Telefonüberwachungen (Abhöranordnungen je Bürger) auf Rang vier, hinter Italien, den Niederlanden und der Schweiz.

Durch das mit der Verbreitung von Handys geänderte Nutzerverhalten sind auch immer mehr Kontaktpersonen von Abhörmaßnahmen betroffen. Die Wahrscheinlichkeit einer Gesprächsüberwachung ist hier inzwischen 30 mal so hoch wie in den USA.

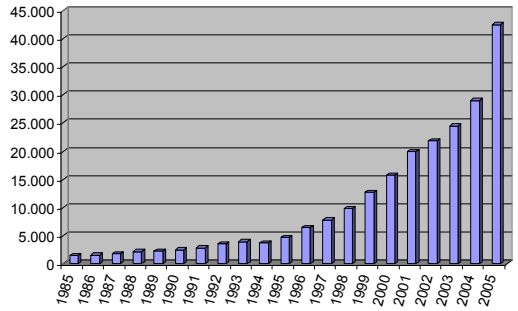


Bild: *Telefonüberwachungsanordnungen*

Erschreckend sind die durch Studien belegten Seiteneffekte dieser Entwicklung: Die schiere Zahl der Anordnungen macht die Durchbrechung des grundrechtlich geschützten Fernmeldegeheimnisses zur Formsache: Von 300 untersuchten richterlichen Beschlüssen entsprachen drei Viertel nicht den gesetzlichen Vorgaben, die Hälfte der Richter unterschrieb einfach den Beschlussentwurf des Staatsanwalts.

„Weder Staatsanwälte noch Richter mochten sich die Ansicht zu eigen machen, dass der Richtervorbehalt als eine besondere Form des Grundrechtsschutzes für die Betroffenen anzusehen sei“ (Backes et.al.). Die vorgeschriebene Benachrichtigung der Betroffenen erfolgte entweder gar nicht (66 %, Albrecht et.al.) oder beschränkte sich auf die Beschuldigten – „es fehlte jede Sensibilität dafür, dass es sich hierbei um Grundrechtseingriffe handelt.“

Dann doch lieber ein Weltmeistertitel für eine Leistung, auf die man stolz sein darf.

1 Security News

1.1 Admin – nein danke!

Hatte Microsoft noch im April 2004 berichtet, dass ca. 95 % aller Angestellten lokale Administrator-Rechte besitzen, so deuten aktuelle Bemerkungen darauf hin, dass sich dieses Verhältnis jetzt umkehren könnte. Das würde die Aussagen Microsofts in einem aktuellen White-Paper zur Information Security bei Microsoft bestätigen – dort wird unter „Lessons Learned and Best Practices“ gefordert: „consolidate local administrator accounts“.

Derzeit verursacht ein Verzicht auf lokale Administrationsrechte häufig Probleme. Für deren Analyse und Behebung hat Microsoft am 23.05.2006 den „Microsoft Standard User Analyzer“ zur Verfügung gestellt.

Der Trend, Administrator-Rechte nicht als Statussymbol, sondern als Sicherheitsrisiko zu betrachten, ist positiv zu bewerten. Halbherzige Work-Arounds sollte man dabei allerdings tunlichst vermeiden (siehe SSN 09/2005). Ein konsequenter Entzug von Admin-Rechten bei Microsoft könnte die Beseitigung von Problemen in diesem Zusammenhang deutlich beschleunigen: „Go, Microsoft, go!“

1.2 Un-SSL-Zertifikate?

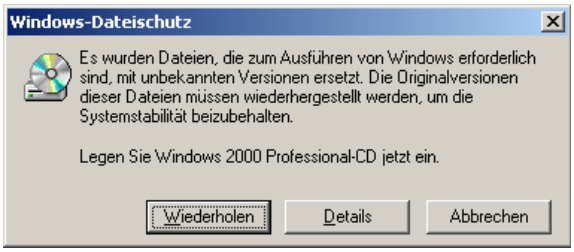
Für ein wenig Aufregung sorgte die Meldung vom 03.06.2006, zukünftige Versionen der populären Mozilla-Browser würden Root-Zertifikate der israelischen StartCom-CA beinhalten. Diese waren Anfang 2006 ins Gerede gekommen, nachdem bekannt wurde, dass man bei StartCom Zertifikate ohne Identitätsprüfung beantragen konnte.

Die Aufregung erscheint unangemessen: Einerseits erlauben die Listen der vorinstallierten Root-Zertifikate *sämtlicher* Browser seit jeher keinerlei Rückschlüsse auf die Qualität der ausgestellten Zertifikate. Und andererseits haben auch andere CAs wie Verisign schon 1996 Zertifikate für E-Mail-Adressen wie root@localhost ausgestellt.

Auch den Mozilla-Entwicklern ist die Problematik längst bekannt, wie interne Diskussionen zeigen. Schon jetzt enthält beispielsweise Firefox (v1.5.0.4) Root-Zertifikate von gut drei Dutzend Firmen, denen man mit der Installation des Browsers automatisch vertraut. Um die Zertifikate bewerten zu können, hilft also nur ein Blick in die Zertifizierungsrichtlinien der jeweiligen CA.

Da kein Anwender sämtliche CA-Policies kennen dürfte, erscheint die Aufregung über die StartCom-Zertifikate ungerechtfertigt. Oder wissen Sie, wie „NetLock Halozatbiztonsagi Kft.“ und „The Go Daddy Group, Inc.“ die Identifikationsprüfung durchführen?

Besonders vorsichtige Zeitgenossen empfehlen daher das Löschen aller vorinstallierten Root-Zertifikate. Dies führt allerdings unter Windows 2000 dazu, dass das komplette System instabil wird:



1.3 Security Focus: Apple

Seit dem 31.05.2006 gibt es nun auch eine Mailingsliste zur Diskussion von Sicherheitsfragestellungen zu Apple's Hard- und Software. Durch eine E-Mail an focus-apple-subscribe@securityfocus.com kann die Aufnahme in den Verteiler initiiert werden. Sicherheitsschwachstellen werden weiterhin über Bugtraq gemeldet.

1.4 Datenklau bei US-Armee

Am 22.05.2006 hat das US-amerikanische Department of Veterans Affairs (zuständig für die medizinische und finanzielle Versorgung von Veteranen) die Serie peinlicher und brisanter Sicherheitsvorfälle in amerikanischen Bundesbehörden (siehe SSN 05/2006) um ein weiteres Highlight ergänzt.

Danach wurde einem Mitarbeiter zu Hause ein Laptop mit über 26 Millionen unge-

schützten Datensätzen von Militärangehörigen (9 % der US-Bevölkerung, davon ca. 2,2 Millionen Aktive) entwendet. Die Daten umfassen Name, Social Security Number und Geburtsdatum – alles, was in den USA zum Identitätsmissbrauch benötigt wird.

Die private Aufbewahrung des Laptop verstieß gegen die Security Policy. Daher wurden nach diesem Vorfall alle Mitarbeiter per Direktive zu einem jährlichen Privacy and Security Training verpflichtet. Denn neben geeigneten technischen und organisatorischen Maßnahmen ist auch ein hohes Sicherheitsbewusstsein im Umgang mit sensiblen Daten unverzichtbar.

1.5 Office im Visier

Am 10.05.2006 meldete Microsoft eine MS-Word Schwachstelle im Microsoft Security Advisory (919637). Sie ermöglicht einem Angreifer, der sein Opfer zum Öffnen präparierter Word-Dokumente verleiten kann, beliebigen Code mit den Berechtigungen des Opfers zur Ausführung zu bringen. Das ist an sich nichts grundsätzlich Neues – allerdings dauerte es über einen Monat, bis Microsoft am 13.06.2006 mit einem Patch im Microsoft Security Bulletin MS06-027 eine zielgruppengerechte Lösung veröffentlichte. Alle zuvor publizierten Workarounds von Trendmicro, Microsoft, US-CERT u. a. setzen zu viel Detailwissen voraus oder sind für den Arbeitsalltag nicht geeignet (Einsatz von WordViewer). Microsoft bewertete die Schwachstelle als „nicht kritisch“; erst im aktuellen Bulletin wurde die Bewertung auf „kritisch“ korrigiert.

Es ist dringend angeraten, den Patch einzuspielen und sich nicht nur auf den aktuellen Virenschutz zu verlassen.

Übrigens: Nicht nur Microsofts Office-Suite steht im Fokus. Am 31.05.2006 hat Kaspersky einen Proof-of-Concept Virus für StarOffice/OpenOffice veröffentlicht. In einer Stellungnahme relativierte das OpenOffice-Team am 02.06.2006 die Bedrohung durch diesen Virus.

1.6 ... back to the Future

BackTrack 1.0, eine Live-Linux-Distribution auf einer bootfähigen CD (oder einem USB-Stick) enthält eine umfassende Sammlung von Netzwerksicherheits- sowie Penetration-Testing-Tools und Exploits. Die neue, am 26.05.2006 freigegebene Distribution enthält sehr aktuelle Programmversionen dieser Werkzeuge (z. B. Metasploit 2.6). Darin laufen die Entwicklungslinien von Auditor Security Linux und WHAX (davor Whoppix) zusammen. Erstmals wurde auch ein eigener Bereich für Datenbankscanner integriert. Ob die Distribution auch die bewährte Robustheit und Funktionsfähigkeit ihrer Vorgänger erreicht, muss sich noch in der Praxis erweisen.

1.7 Big Brother Awards

Ganz ohne Fernsehen und Container werden seit 1998 in inzwischen 17 Ländern jährlich die Big Brother Awards für besondere Verdienste um Datenschutz feindliche Techniken und Datenerhebungen verliehen. In Deutschland organisiert seit dem Jahr 2000 der FoeBuD e. V. in Bielefeld die Nominierung der Preisträger und die Verleihung der „Oscars für Datenkraken“.

Die Nominierung von Preisverdächtigen ist noch bis zum 31.07.2006 möglich. Die diesjährige Verleihung der Awards erfolgt am 20.10.2006 im historischen Saal der Ravensberger Spinnerei im Zentrum von Bielefeld.

2 Secorvo News

2.1 Secorvo College aktuell

Nach der Sommerpause startet Secorvo College im September mit

- dem aktuellen Grundlagenseminar IT-Sicherheit heute (**19.-21.09.2006**) und
- einem Intensivseminar zu Public Key Infrastrukturen (PKI) (**26.-29.09.2006**).

Programme, weitere Seminarangebote, Preise und Online-Anmeldung unter http://www.secorvo.de/college

2.2 Gemalte Städte

Der Künstler Thitz, einigen von Ihnen durch Secorvo-Weihnachtskarten oder einem Besuch in Karlsruhe bekannt, zeigt seine „Gemalten Städte“ noch bis zum 29.10. 2006 in der Staatlichen Kunsthalle Karlsruhe.

2.3 KA-IT-Si @ Midvision

Die Karlsruher IT-Sicherheitsinitiative ist auf der Midvision 2006 am 21. und 22.06.2006 in der Messe Karlsruhe mit einem eigenen Stand vertreten. Auch die KA-IT-Si-Partner AMEC SPIE System Integration und Lampertz sind dabei und zeigen aktuelle Sicherheitslösungen.

Am **21.06.2006** wird um 18:30 Uhr Herr Professor Dr. Bartsch von der renommierten, auf IT-Recht spezialisierten Karlsruher Kanzlei Bartsch und Partner im Foyer der Messe über „Risiken, Pannen, Schäden – und wer haftet?“ sprechen. Anmeldung zu diesem KA-IT-Si-Event bitte über die Webseite (Anfahrtskizze).

Zum Vormerken: Ihren fünften Geburtstag wird Deutschlands älteste IT-Sicherheitsinitiative am **18.10.2006** im Saal Baden der IHK Karlsruhe angemessen feiern. Die Key Note wird Herr Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) halten.

3 Veranstaltungshinweise

Juni 2006	
21.06.	"Risiken, Pannen, Schäden – und wer haftet?" (KA-IT-Si, Messe Karlsruhe)
21.-22.06.	Midvision 2006 (Messe Karlsruhe)
25.-30.06.	18th Annual FIRST Conference (FIRST, Baltimore/USA)
Juli 2006	
13.-14.07.	DIMVA 2006 (GI, Berlin)
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/US)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)

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

Secorvo Security News
Juli 2006

Dirk Fox, Stefan Gora, Kai Jendrian,
Stefan Kelm, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 7, 5. Jhrg. 2006
Stand 19. Juli 2006

ISSN 1613-4311

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

Inhalt

Editorial: FlieWaTüüt

Eine Lieblingsgeschichte meiner Kindheit, „Robbi, Tobbi und das FlieWaTüüt“ von Boy Lornsen, hat wahrscheinlich den Ingenieur in mir geweckt. Die phantastischen Abenteuer des kleinen Erfinders Tobbi mit einem Roboterjungen und seinem selbst entworfenen „FlieWaTüüt“, einer Kreuzung aus Mini-Wasserhubschrauber und dreirädriger Piaggio-APE, waren für mich der Jules Verne des 20. Jahrhunderts. (Die spektakuläre WDR-Verfilmung von 1972 gibt es übrigens seit 2005 auf DVD.)

Begeistert hat mich die Vision eines Fahrzeugs, das alle wesentlichen Funktionen vereint. Heute gibt es ein Wort dafür: Konvergenz – das Zusammenwachsen unterschiedlichster technischer Lösungen. Standardisierte anwendungsneutrale Basistechnologien wie PC, Internet und digitale Ton- und Bilddaten ermöglichen heute verschiedenste Funktionen auf einem Gerät.

So mutiert das mobile Telefon mit Fotoapparat, Radio, Armbanduhr, MP3-Player, Spielekonsole und mobilem Fernseher zum „TelMusKlick“. Als Smartphone enthält es Adressbuch, Taschenrechner, Terminkalender, E-Mailer, Notizblock und Internet-Browser, erlaubt es die Bearbeitung von Office-Dokumenten, schickt Präsentationen an einen Beamer und navigiert durch unbekannte Städte. Es ist Informationsdienst und Online-Auskunft, Vorleser, Fremdenführer und Dolmetscher in einem.

Bald sucht es sich automatisch die günstigsten Netze (UMTS, WLAN oder Bluetooth), synchronisiert seine Daten mit zentralen Adress- und Datenservern über das Internet, ersetzt Privatbibliothek, Tageszeitung und Musiksammlung. Es öffnet und verschließt Türen und Fahrzeuge und steuert Jalousien und Haushaltsgeräte.

Ein Alleskönner für die Hosentasche – und ein gefundenes Fressen für Angreifer. Firewall-freie Kommunikationsverbindungen und sensibelste Daten mit komplexer (ergo fehleranfälliger) Softwarekonzentration in den Händen unkundiger Nutzer – hätte Jules Verne das geahnt, wäre daraus ein spannender Science Fiction geworden.

1 Security News

1.1 BCM-Standard

Am 03.07.2006 hat das British Standards Institute (BSI) eine Vorabversion des Standards BS 25999-1 *Guide of Practice for Business Continuity Management (BCM)* zur Kommentierung bis zum 31.08.2006 und zur Diskussion veröffentlicht.

In der Tradition des BS 7799 gibt das BSI mit diesem Standard auf Best Practices beruhende Richtlinien und Empfehlungen heraus. Das Dokument liefert eine gute Einführung in BCM-Begriffe und Vorgehensweisen. Für BCM-Interessierte ist daher schon die Vorabversion des Standards eine Lektüre wert.

1.2 Security Tool Hitparade

Von Fyodor, dem Entwickler des bekannten Port-Scanners nmap wurde am 21.06. 2006 das Ergebnis seiner Umfrage zum Thema Security Tools auf der Mailing-Liste Nmap Hackers veröffentlicht. Aus den 3243 Antworten wurde eine repräsentative Rangliste von Security Tools erstellt und unter SecTools.Org publiziert. Die Liste ist eine wahre Fundgrube und gibt Auskunft über die Popularität eines Tools, den kommerziellen Status, das Abschneiden im Vergleich zur letzten Umfrage 2003 und die unterstützten Betriebssysteme. Sie enthält eine kurze Zusammenfassung der Funktionsweise und einen Link auf das Tool.

1.3 Operational Risk Survey

Am Henley Management College wird derzeit eine anonyme Online-Befragung über den Zusammenhang zwischen operationellen Risiken und Informationssicherheit in der Praxis durchgeführt. Zur Teilnahme sind Sicherheitsexperten mit Praxiserfahrung aufgerufen. Der Fragebogen umfasst 44 Multiple-Choice-Fragen und Statements und lässt sich in wenigen Minuten beantworten. Auf Wunsch erhalten Teilnehmer das Summary der Studie zugesandt.

1.4 Mehr Glück als Verstand

... könnte das Fazit des Datendiebstahl-Vorfalls bei der US-Armee sein, über den wir in den SSN 06/2006 berichtet haben: Am 29.06.2006 wurden der Laptop und die betroffene externe Festplatte sichergestellt; Untersuchungen des FBI ergaben, dass ein Zugriff auf die betroffenen Daten mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.

Erwähnenswert ist der offizielle Bericht des Office of Inspector General der betroffenen Behörde. Das Dokument ist lesenswert für jeden Sicherheitsverantwortlichen, da hier auf über 40 Seiten ein GAU beim Umgang mit einem Sicherheitsvorfall schonungslos dokumentiert wird.

1.5 SSL Revisited

„Trau, schau, wem!“ war das Fazit des Artikels „Un-SSL-Zertifikate?“ aus den SSN 06/2006. Die negativen Erfahrungen mit dem Entfernen aller CA-Zertifikate unter Windows 2000 veranlassten uns zu untersuchen, welche Zertifikate gefahrlos aus dem Zertifikatsspeicher gängiger Browser entfernt werden können, um sie auf eine individuell vertrauenswürdige Sammlung zu reduzieren. Dazu wurden die gängigen Versionen von Internet Explorer, Firefox und Opera unter Windows 2000 untersucht. Als Ergebnis lässt sich festhalten, dass Windows 2000 nur die sechs von Microsoft zwingend vorgeschriebenen CA-Zertifikate benötigt. Bemerkenswerterweise sind von diesen bereits vier abgelaufen. Ein Windows XP System startete auch ohne diese sechs CA-Zertifikate fehlerfrei; zumindest für den Bootvorgang ist Microsofts Vorgabe an Minimalzertifikaten unter Windows XP demnach nicht erforderlich. Aus den Browsern Firefox und Opera ließen sich alle lokalen CA-Zertifikate ohne funktionale Einschränkung entfernen.

„Trau, schau, wem!“ bleibt also auch nach den Tests die Botschaft im Umgang mit SSL-Zertifikaten. Wer daher nicht blind jeder SSL-Verbindung trauen mag, sollte alle CA-Zertifikate löschen, deren Vertrauenswürdigkeit ihm nicht gesichert erscheint.

1.6 SAP-Baustein IT-GSHB

Auf den Webseiten des BSI wurde am 20.06.2006 eine Vorabversion des neuen Bausteins „B 5.13 SAP System“ für das IT-Grundschutzhandbuch bereit gestellt. Der recht umfassende Baustein (133 Seiten) gibt einen Überblick der potentiellen Gefährdungen sowie der relevanten Maßnahmen auf Basis von IT-Grundschtz. Die Maßnahmen sind recht gut beschrieben und wurden durch Kontrollfragen ergänzt. Somit wird nun mit SAP eine weitere wesentliche Anwendung und Plattform abgedeckt.

1.7 bDSB-Handreichung

Für den betrieblichen Datenschutzbeauftragten hat der Arbeitskreis Datenschutz des BITKOM am 21.04.2006 zwei wertvolle Handreichungen veröffentlicht: Einen Praxisleitfaden zum Verfahrensverzeichnis nach BDSG, der neben einigen wichtigen Klarstellungen, konkreten Beispielen und Formblättern für die Datenerhebung auch eine tabellarische Gegenüberstellung von Tools zur Gestaltung des Verfahrensregisters enthält. Eine wertvolle Hilfestellung zur Umsetzung des BDSG in der Praxis.

Das zweite Dokument zur Datenschutzproblematik bei grenzüberschreitender Datenübermittlung macht die nicht ganz einfache Rechtslage transparent und gibt konkrete Empfehlungen für die Praxis.

1.8 PIN-Reset bei O2 (UK)

Im aktuellen Cryptogram vom 15.07.2006 stellt Bruce Schneier das vereinfachte PIN-Reset-Verfahren von O2 in Großbritannien zur Diskussion. Danach kann nach einer Sperrung der SIM-Karte ein PUK (Personal Unlocking Key) ohne weiter gehende Authentifizierung allein mit Angabe der Handynummer beantragt werden.

In Ermangelung eines britischen Kartenvertrags konnten wir dies nicht verifizieren; nach den Angaben von Bruce Schneier wurde aber von O2 zu den Risiken des Verfahrens wie folgt Stellung genommen:

- Ist das gestohlene Handy ausgeschaltet, kann die Telefonnummer nicht in Erfahrung gebracht und so auch keine PUK beantragt werden.
- Ist das Handy eingeschaltet, kann ein Dieb auch ohne PIN/PUK telefonieren.

Das Risiko wird von O2 daher als gering eingestuft, da in beiden Fällen der Provider ohnehin umgehend über den Verlust informiert und die SIM-Karte sperren würde.

Von O2 wurden jedoch nicht alle denkbaren Fälle bedacht. Uns sind mindestens drei Denkfehler aufgefallen. Ihnen auch? Dann senden Sie Ihre Überlegungen bis 15.08.2006 an sommerquiz@secorvo.de. Unter allen Einsendern verlosen wir einen kostenlosen Zugang zum security-finder für ein Jahr. Die kreativsten Angriffsideen werden in den nächsten SSN veröffentlicht.

1.9 Spyware by Microsoft

Die aus Microsofts „Windows Genuine Advantage“ (WGA) Programm hervorgegangene Lizenz-Validation wurde am 27.06. 2006 zu einer WGA-Notification erweitert, die sich nach der Installation wie Spyware verhält: wiederholte Starts (bei jedem Windows Logon und alle 24 Stunden), Untersuchung von Hard- und Software (MAC-Adresse, IP-Adresse, Informationen zum Benutzerkontext), unaufgeforderte Anzeige von Informationen (Popups), Übermittlung von Daten ohne Autorisierung und Wissen des Endbenutzers an externe Microsoft-Server.

Das Unterschieben der erweiterten Funktionalität als sicherheitskritisches Update im Rahmen des (ggf. automatischen) Windows-Update Services führte insbesondere auf Privatsystemen zu einer starken Verbreitung. Allerdings handelt es sich bei diesem Update inhaltlich nicht um System-Sicherheit, sondern um Lizenzkontrolle. Für ein ähnliches Verhalten wurden Spyware-Anbieter unlängst rechtkräftig verurteilt (Smartbot.Net und Odysseus).

Auch wenn die bisherigen Stellungnahmen von Microsoft eine Identifizierung der Endbenutzer verneinen, bleibt eine negativer

Beigeschmack, da das Tool Informationen in der Privatsphäre des Nutzers erhebt und an Microsoft sendet.

2 Secorvo News

2.1 Secorvo College aktuell

Das Seminar IT-Sicherheitsaudits in der Praxis wurde auf Anregung zahlreicher Teilnehmer zu einem dreitägigen Seminar ausgebaut. Das Vortragsprogramm wird nun ergänzt durch drei Workshop-Teile; für das Thema „Rechtliche Rahmenbedingungen und Datenschutz“ ist mehr Raum vorgesehen.

2.2 Business Continuity

In Folge der insbesondere im Kontext von KontraG, SOX und Basel II verstärkten Bemühungen aller Unternehmen um Compliance, d.h. die Übereinstimmung der Form der Geschäftsausübung mit gesetzlichen Anforderungen aller Art, rückt neben dem Datenschutz auch die Beschäftigung mit denkbaren Notfällen in den Fokus der Informationssicherheit.

Aus mehreren Projektarbeiten ist nun eine ausführliche Darstellung unseres Leistungsangebots im Gebiet Business Continuity und Disaster Recovery entstanden.

2.3 5 Jahre KA-IT-Si

In diesem Jahr jährt sich die Gründung der Karlsruher IT-Sicherheitsinitiative zum fünften Mal. Dieses Jubiläum wird die KA-IT-Si am **18.10.2006** feiern – im **Saal Baden der IHK Karlsruhe**, dem Ort, an dem am 25.01.2001 die KA-IT-Si aus der Taufe gehoben wurde. Die Key Note wird Herr Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) halten, flankiert von anschaulichen Praxisberichten zur „Herausforderung IT-Sicherheit im Mittelstand“, einer Ausstellung der Sicherheitslösungen der KA-IT-Si-Partner und einem anschließenden „Net(t)-working-Büfett“. Online-Anmeldung unter www.ka-it-si.de.

3 Veranstaltungshinweise

Juli 2006	
31.07. - 04.08.	USENIX Security Symposium (USENIX, Vancouver/CA)
August 2006	
02.-03.08.	Black Hat USA 2006 (Black Hat, Las Vegas/USA)
04.-06.08.	DEFCON 14 (Defcon, Las Vegas/USA)
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/USA)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
04.-05.10.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)

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

Secorvo Security News
August 2006

Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, Natalie Mareth, Jochen Schlichting
Secorvo Security Consulting GmbH

Nr. 8, 5. Jhrg. 2006
Stand 17. August 2006

ISSN 1613-4311

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

Inhalt

Editorial: Feine Freunde

Das Wettrüsten zwischen den Entwicklern von Sicherheitstechnologien und den Erfindern von Penetrations- oder Umgehungsmöglichkeiten, gemeinhin „Hacker" genannt, durchzieht die Geschichte der IT-Sicherheit wie ein roter Faden.

Zwar stimuliert Wettbewerb bekanntlich die Qualität eines Produkts, und zweifellos wären ohne ein solches Stimulans weder Firewalls noch Hackingtools, weder Virenscanner noch Trojaner so leistungsstark und bedienungsfreundlich. Dennoch ist die Wirkung dieses Wettrüstens eher destruktiv und verursacht Kosten und Schäden.

Konnte man dem Wettkampf früher wenigstens in Ansätzen noch etwas Sportliches abgewinnen, da Viren und Würmer in der Regel keine komplexen Schadfunktionen enthielten und eher den Charakter eines „proof of concept" besaßen, haben kriminelle Interessen aus dem Wettkampf inzwischen eine Schlacht gemacht. Mit Spammern, Bot-Netzen, Warez-Servern und Phishing lässt sich Geld verdienen – oder zumindest waschen.

Aber nicht nur der Kampf ist härter geworden. Auch die Fronten verschwimmen. So verbreiten Softwarehersteller Copyright-Schutzmechanismen, die sich mit Stealth-Techniken im System verstecken oder wie Spyware verhalten (SSN 7/2006). Banken verwenden eigenartige Domain-Namen und führen wenig intuitive „Sicherheitsmerkmale" für ihr Online-Banking ein, die ein wechselndes und befremdliches Erscheinungsbild hervorrufen – und sich kaum mehr von einer Phishing-Seite unterscheiden lassen. Marketiers verschicken HTML-E-Mails mit versteckten URLs (um Empfängerreaktionen zu analysieren). Und Entwickler von Peer-to-Peer-Anwendungen wie Skype „perforieren" Firewalls trickreich mit dem verbindungslosen UDP-Protokoll – und etablieren so Kommunikationsverbindungen, die komplett an der Filterung vorbeilaufen.

Damit werden Hacking-Techniken zu Produkt-Features. Wer solche Freunde hat, braucht keine Feinde mehr.

1 Security News

1.1 Offene Fenster

Zum Patchday am 08.08.2006 wurden von Microsoft zwölf Sicherheits-Hotfixes veröffentlicht, von denen besonders die Sicherheitslücke im Server-Service und die so genannten RemoteExecution Schwachstellen erhebliche „Nachwirkungen“ haben dürften. Fatal ist, dass diese Lücken in fast allen Versionen der Windows-Familien 2000 / XP / 2003 inklusive Service Packs existieren – alle installierten Windows-Systeme, bei denen dieser Dienst ungeschützt aktiv ist, können derzeit automatisiert übernommen werden.

Die auf der Mailingliste Full Disclosure publizierte Schwachstelle im /proc-Filesystem, die lokalen Benutzern mit shell-Zugriff eine Privilegieneskalation bis auf root-Ebene erlaubt, erscheint dagegen fast als „harmloser“ Sonderfall.

Trotz Microsofts Paradigmenwechsel von der „Featuritis“ zur Softwaresicherheit als erster Priorität nimmt die Anzahl kritischer Schwachstellen nicht ab. Ohne sauber konfigurierte (Personal) Firewalls und ein konsequentes Patch-Management ist ein ausfallfreier IT-Betrieb inzwischen völlig undenkbar geworden.

1.2 Compliance

Am 07.07.2006 hat Microsoft seine zahlreichen Dokumente zu verschiedenen Themen der IT-Sicherheit um den Regulatory Compliance Planning Guide ergänzt. Darin werden auf 71 Seiten Maßnahmen zur Umsetzung der organisatorischen und technischen Anforderungen von Gesetzen und Standards mit Microsoft-Technologien und -Produkten dargestellt.

Vorgestellt und berücksichtigt werden Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), EG-Datenschutzrichtlinie sowie die ISO 17799 (2005). Zwar ist das Dokument mit „Microsoft-Brille“ geschrieben, enthält aber wertvolle Hinweise und Beispiele.

Es steht in engem Kontext anderer lesenswerter Microsoft-Dokumente zum Thema IT-Security wie dem Security Risk Management Guide, dem Security Monitoring and Attack Detection Planning Guide und dem etwas technischeren Windows Server 2003 Security Guide.

1.3 Rootkits auf der Blackhat

Auf der diesjährigen Blackhat vom 29.07.-03.08.2006 in Las Vegas wurden von Dino Dai Zovi und Joanna Rutkowska Rootkits für die neuen Intel- und AMD-Prozessoren präsentiert, die deren Virtualisierungstechniken nutzen. Bisherige Hardware Based Rootkits (SSN 04/2006) benötigten eine komplette virtuelle Maschine wie VMWare oder VirtualPC; die neue Generation führt die Virtualisierung im laufenden Betrieb durch und ist nicht einmal mehr an vermeintlichen Änderungen der Hardware erkennbar.

Schutz bietet derzeit nur die Deaktivierung der Virtualisierungsfunktionen im BIOS – sofern sie nicht benötigt werden.

1.4 Defcon Rocks

Die 14. Defcon vom 04.-06.08.2006, ebenfalls in Las Vegas, war etwas chaotischer organisiert als die Blackhat und begann mit zwei Stunden Verspätung. Die gebotenen Inhalte und das wohl "most hostile network on earth" machten diesen Mangel jedoch wett. Neben den verschiedenen Hacking-Events waren einige der „0-day attacks“ sehr spannend.

Unter anderem wurde vorgestellt, wie Systeme über Schwachstellen im WLAN-Treiber übernommen (Johnny Cache) und wie bei verbreiteten SmartPhones unter Windows CE 4.2 über Multi-Media Messages (MMS) beliebige Programmcodes zur Ausführung gebracht werden können (Collin Mulliner). Auch das Thema Blackberry-Security, insbesondere die Architektur, wurde von FX (Phenoelit) ausführlich beleuchtet.

1.5 PhishPharming

Deloitte veröffentlichte am 15.06.2006 den Global Security Survey 2006, Ergebnis einer Befragung von Datenschutz- und Sicherheitsbeauftragten weltweit tätiger Finanzinstitute über Art und Anzahl von Sicherheitsattacken. Eine wesentliche Beobachtung ist, dass systematische Angriffe, die auf finanziellen Gewinn abzielen, offenbar stark zunehmen. Mehr als die Hälfte der externen Angriffe (51 %) beruhten auf Phishing oder Pharming. Auch für das laufende Jahr zählen Identitätsdiebstahl und Betrug mit gefälschten Zugangsdaten zu den größten erwarteten Bedrohungen. Bei 58 % der Befragten rangieren Schutzmaßnahmen gegen diese Risiken unter den wichtigsten fünf Sicherheitsaktivitäten.

1.6 CrypTool v1.4

Die inzwischen unter Open-Source-Lizenz verbreitete Kryptografie-Lernsoftware CrypTool steht seit dem 31.07.2006 in der Version 1.4 zur Verfügung. CrypTool ermöglicht dem Nutzer einen anschaulichen Zugang zum Verständnis von kryptografischen Verfahren und deren Grenzen. Es wurde vor allem für die Mitarbeiter-Sensibilisierung und zu Ausbildungszwecken entwickelt (zur Historie siehe SSN 3/2002).

Neu sind neben Parametererweiterungen (längere Schlüssel, größere Dateien) und neu implementierten Verfahren und Angriffen unter anderem auch sehr verständliche Java-Animationen, die Schritt für Schritt die Funktionsweise der Verschlüsselung mit Caesar, Vigenère, Nihilist oder DES demonstrieren. Außerdem gibt es das Lernspiel „Der Zahlenhai“, das den Umgang mit Teilern und Primfaktoren veranschaulicht.

1.7 Standard-Kompass

Am 28.06.2006 hat der AK Sicherheitsmanagement des Bitkom Version 2.0 des „Kompass der IT-Sicherheitsstandards“ herausgegeben. Aktualisierung und Überarbeitung durch viele kompetente Autoren haben zu einem sehr informativen, 90seitigen „Standard-Werk“ beigetragen.

1.8 Auswertung Sommerquiz

Zahlreiche Zuschriften haben uns zu unserem Sommerquiz (SSN 07/2006) erreicht. Der kreativste Input kam von Hanno Langeweg aus Gjøvik in Norwegen – für seine Überlegungen bedanken wir uns mit einem Jahresabo für den Security-Finder.

Die meisten Kommentare bezogen sich auf die Annahme, dass bei ausgeschaltetem Telefon die Telefonnummer nicht in Erfahrung gebracht werden könne. Wird ein Mobiltelefon gezielt gestohlen, greift diese Annahme nicht: Die Telefonnummer des Opfers ist entweder bekannt oder kann leicht ermittelt werden. Häufig ist auch die eigene Nummer im Handy (nicht auf der SIM) gespeichert oder in Unterlagen notiert, die zusammen mit dem Handy entwendet werden (Handtasche o.ä.). Erwischt der Dieb ein eingeschaltetem Handy, kann er die Telefonnummer leicht ermitteln und sich damit die PUK besorgen.

Fazit: Die eigene Telefonnummer ist ein sehr schwaches alleiniges Authentisierungsmerkmal; O2 (und jedem anderen Helpdesk) empfehlen wir einen ausgefeilteren Authentisierungsprozess.

1.9 Ruf’ mich an, Kleines

In einem Fachvortrag setzte sich Doug Mohney am 02.08.2006 auf der Blackhat mit dem Thema Stimmanalyse in Callcentern und Großunternehmen kritisch auseinander. Als Schutz vor Social Engineering Angriffen erfreuen sich Stimmanalysesysteme mit Filtermechanismen (Whitelists, Blacklists, Word Spotting) und statistischer Stimm- und Stressanalyse derzeit großer Nachfrage. Tatsächlich stellen diese Systeme nicht nur ein attraktives Ziel für Identitätsdiebe dar, wie die zunehmende Anzahl von Angriffen auf Call-Center-Infrastrukturen zeigt, sondern sind auch datenschutzrechtlich problematisch: Sie erlauben die Erstellung von „Stimmprofilen“. Von da ist es nicht mehr weit bis zu „Stimmenspuren“, die wir im Netz hinterlassen – beispielsweise via Google Voice Search – und die systematisch recherchiert und missbraucht werden können.

2 Secorvo News

2.1 Secorvo College aktuell

In den Herbst startet Secorvo College mit zwei Anfang 2006 komplett renovierten „Klassikern“: dem Grundlagenseminar „IT-Sicherheit heute“ am 19.-21.09.2006 und dem Intensivseminar „PKI – Public Key Infrastrukturen“ vom 26.-29.09.2006.

Beide Seminare sind eine ausgewogene Mischung aus Theorie (Grundlagen, Hintergründe, Zusammenhänge) und Praxis (Vorführungen, Beispiele, Best Practices). Der Bewertung eines Teilnehmers des PKI-Seminars im Frühjahr 2006 haben wir nichts hinzuzufügen: *„Sehr gut strukturiertes Seminar für alle, die im Kontext PKI auf ‚Ballhöhe’ kommen wollen, aber auch für die, die es bereits sind.“*

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

2.2 TISP @ Secorvo College

Vor drei Jahren entwickelte TeleTrusT ein europäisches Expertenzertifikat für den Bereich Informationssicherheit – den „TeleTrusT Information Security Professional“, kurz TISP. Dieses Zertifikat wurde im Unterschied zu den zahlreichen internationalen Zertifikaten auf die spezifischen deutschen und europäischen Anforderungen zugeschnitten. In 18 Themenmodule sind die Inhalte gegliedert; Ausbildung und Prüfung erfolgen in deutscher Sprache.

Seit 2004 haben mehr als 100 Security-Experten die TISP-Ausbildung und –Zertifizierung absolviert. Drei Jahre Berufserfahrung und eine erfolgreiche Prüfung mit vorausgehender fünftägiger Intensivschulung sind dafür Voraussetzung.

Secorvo, selbst seit 1998 aktives Mitglied bei TeleTrusT, hat nun die Anerkennung als „TISP-Schulungsanbieter" beantragt und wird, vorbehaltlich der endgültigen Akkreditierung, am 20.-25.11.2006 die erste TISP-Schulung mit anschließender Prüfung durchführen.

3 Veranstaltungshinweise

August 2006	
20.-24.08.	Crypto 2006 (IACR, Santa Barbara/US)
September 2006	
19.-21.09.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
26.-29.09.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo College)
Oktober 2006	
04.-05.10.	Inside Windows Security (Secorvo College, Karlsruhe)
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
06.-07.11.	IT-Risk Management 2006 (COMPUTAS, Karlsruhe)
20.-25.11.	TISP-Schulung (Secorvo College, Karlsruhe)
26.11.	TISP-Prüfung (Secorvo College, Karlsruhe)

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

secorvo
security consulting

Secorvo Security News

September 2006

Editorial: 5-50-I000

Jubiläen sind bekanntlich ebenso wichtig wie willkürlich. Wichtig, weil sie die Wurzeln in Erinnerung rufen, zugleich etwas Vollbrachtes vor Augen führen, und sowohl Ermutigung als auch Ansporn sein können. Willkürlich, weil der Termin eines Jubiläums weniger vom objektiven Zeitablauf als vom gewählten Maßsystem abhängt, wie jeder Informatiker weiß. Denn auch wenn die natürliche Beschaffenheit unseres Körpers die Nutzung des Dezimalsystems nahe legt (zehn Finger), versteht sich dies keineswegs von selbst, wie nicht zuletzt die Rechenwerke unserer elektronischen Gehilfen belegen.

Gleich drei Jubiläen feiern wir in diesem Frühherbst:

- Am 18.10.2006 begehen wir das fünfjährige Jubiläum der Karlsruher IT-Sicherheitsinitiative – mit einer halbtägigen Veranstaltung in der IHK Karlsruhe und einer Key Note des BSI-Präsidenten, zu der wir Sie sehr herzlich einladen (Anmeldung).
- Vor Ihnen liegt die 50. Ausgabe der „Secorvo Security News" – und hinter uns 50 Monate, in denen wir Nachrichten recherchiert, gefiltert, bewertet und für Sie aufbereitet haben. Ausgedruckt ein ansehnliches Büchlein von 200 Seiten.
- Am 01.09.2006 konnten wir ein besonderes Ereignis begehen: Vor I000 Jahren wurde Secorvo gegründet – in der Schnelllebigkeit des dot-com-Zeitalters ein gar „biblisches" Alter, dem die Verwendung des Dualsystems angemessen Rechnung trägt.

Das Jubiläum unserer kleinen News, deren Leserzahl ständig wächst, haben wir zum Anlass genommen, die Gestaltung einer gründlichen Überarbeitung zu unterziehen. Dabei wollten wir insbesondere den einzigen Kritikpunkt, der aus Ihren Reihen gelegentlich geäußert wurde, ausräumen: das durch die Spaltenformatierung erforderliche Vor- und Zurückblättern innerhalb einer Seite.

Und auch der security-finder hat ein neues Gesicht bekommen – schauen Sie einmal hinein. Wir freuen uns auf Ihre Rückmeldungen.

Inhalt

secorvo
security consulting

Security News

Krypto-Bug in OpenSSL

Auf der legendären „Rump Session" der diesjährigen Weltkonferenz der Kryptologen, der Crypto 2006 in Santa Barbara, präsentierte Daniel Bleichenbacher am 22.08.2006 eine Möglichkeit zur Fälschung von RSA-Signaturen, die den öffentlichen Exponenten „3" verwenden. So überprüfen die betroffenen OpenSSL-Implementierungen (bis v0.9.7j und v0.9.8b) die Füllbytes („padding") nicht korrekt. Ein Angreifer kann diese Schwachstelle relativ einfach nutzen, um eine dritte Wurzel als gültige Signatur in den überschüssigen Bytes zu verstecken. Forscher der TU Darmstadt haben einen Exploit entwickelt.

Ein am 05.09.2006 veröffentlichtes Advisory empfiehlt ein Update auf neuere OpenSSL-Versionen. Produkte, die direkt auf OpenSSL aufsetzen (z.B. BIND in Verbindung mit DNSSEC-Signaturen) sind ebenfalls betroffen, genauso die Browser Firefox (bis v1.5.0.6), SeaMonkey (bis v1.0.4), Opera (bis v9.01) sowie alle Netscape-Browser. Lachende Dritte sind diesmal der nicht betroffene Internet-Explorer (v6) und Apples Safari. Eine Alternative zu einem Upgrade ist das Entfernen von Root-Zertifikaten mit dem öffentlichen Exponenten „3" aus dem Zertifikatsspeicher des Browsers – die leider nach wie vor verwendet werden, obwohl deren Anfälligkeit für Angriffe seit mehr als 10 Jahren bekannt ist.

ISO 27001-Zertifikat für SAP SI

Den hochverfügbaren Serverzentren des Geschäftsbereichs Hosting der SAP Systems Integration AG am Standort Dresden wurde am 31.07.2006 vom BSI ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz verliehen. Diesem Beispiel werden in Kürze zweifellos weitere Unternehmen folgen, die in den beiden vergangenen Jahren eine IT-Grundschutz-Zertifizierung erfolgreich absolviert haben, da die Umstellung auf ein ISO 27001-Zertifikat auf der Basis von IT-Grundschutz mit moderatem Aufwand möglich ist.

BDSG 2006 in Kraft

Am 25.08.2006 wurde das „Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft" veröffentlicht. Es trat am 26.08.2006 in Kraft. Artikel 1 ändert das Bundesdatenschutzgesetz (BDSG): So wurde das Quorum, bis zu dem kein betrieblicher Datenschutzbeauftragter zu bestellen ist, von „höchstens vier Arbeitnehmer" in „höchstens neun Personen" geändert. Damit stellt der Gesetzgeber klar, dass es um die Zahl der Personen unabhängig von ihrem arbeitsrechtlichen Status geht – Geschäftsführer, Praktikanten, Auszubildende und externe Hilfskräfte zählen nun unstreitig dazu. Unternehmen, die unterhalb des Quorums liegen, werden damit jedoch nicht von den Pflichten des betrieblichen Datenschutzbeauftragten befreit. Die Neufassung des § 4g legt für diesen Fall fest, dass „der Leiter der Stelle die Erfüllung der Aufgaben (...) in anderer Weise sicher zu stellen" hat.

.dd -> .vmdk

Der erste Schritt in fast jeder forensischen Analyse ist das Erstellen einer Bit-genauen Kopie (Image) des zu untersuchenden Datenbestands, um die Analyse anschließend auf dieser Kopie durchführen zu können, ohne Originaldaten zu verändern. Oft kommt dabei das in der Unix-Welt verbreitete Tool „dd" zum Einsatz. Die so erstellten Images können dann einer statischen oder dynamischen Analyse unterzogen werden. Nachteil der dynamischen Analyse ist, dass dabei das Image grundsätzlich verändert wird – der Forensiker wird daher mehrere Images des Originals erstellen, damit er immer wieder auf den Ausgangszustand der Daten zurückgreifen kann.

Am 25.08.2006 wurde Live View vorgestellt, ein neuartiges Tool, das es erlaubt, dd-Images in virtuelle Maschinen zu konvertieren. Diese können anschließend mit der Software VMware analysiert werden, um beispielsweise Details über laufende Prozesse oder offene Netzwerkverbindungen auf dem zu untersuchenden Rechner zu erhalten.

Das Tool wurde im CERT-Umfeld entwickelt und setzt Java voraus. Es befindet sich noch in einem sehr frühen Entwicklungsstadium, läuft jedoch bereits recht stabil.

Besser zweimal messen ...

... als einmal vergessen. Getreu diesem Motto fand am 01.08.2006 im Rahmen des 15th Usenix Security Symposium in Vancouver der Workshop Metricon 1.0 engagierter Experten der securitymetrics.org-Community statt. Die 44 Teilnehmer diskutierten intensiv über den Sinn von Metriken, Software-Security-Metriken, Governance und insbesondere Case-Studies. Die Zusammenfassung und einzelnen Vortragsunterlagen geben einen guten Überblick über die aktuellen Entwicklungen. Dan Geer, Initiator von securitymetrics.org, hielt auf dem Symposium ein Tutorial zum Thema Measuring Security. Darin gab er einen umfassender Überblick über das Thema Metriken im Allgemein und in Bezug auf Sicherheit im Besonderen. Ein begrüßenswerter Trend zu mehr Mess- und Vergleichbarkeit in der IT-Sicherheit.

Awareness @ ENISA

Dass die Sensibilisierung von Mitarbeitern und Benutzern – neudeutsch auch „Security Awareness“ genannt – ein wichtiger Bestandteil eines übergreifenden Sicherheitskonzepts sein sollte, ist längst bekannt. Dennoch sind Konzeption und Umsetzung von erfolgreichen Awareness-Maßnahmen ein anspruchsvolles Unterfangen, wie Erfahrungsberichte auf Symposien oder in E-Books zeigen.

Diesem Umstand hat sich jetzt auch die noch relativ junge europäische Sicherheitsbehörde ENISA angenommen und am 10.08.2006 den Leitfaden “A Users' Guide: How to Raise Information Security Awareness“ veröffentlicht. Der Leitfaden enthält zahlreiche Tipps und Hilfestellungen für die Umsetzung eigener Awareness-Kampagnen und richtet sich auch an KMUs, deren Budget für derartige Projekte meist sehr begrenzt ist.

Dynamische Malware-Analyse

Kostenlose Web-Dienste zur Analyse von Viren und anderen verdächtigen Dateien existieren bereits seit einiger Zeit. Viele Antiviren-Hersteller bieten auf Ihren Webseiten entsprechende Online-Schnittstellen an (z.B. norman, virustotal oder jotti). Die Ergebnisse beschränken sich jedoch im Wesentlichen auf die Information, ob die untersuchte Datei mit einem bekannten Virus oder Wurm infiziert ist.

Einen Schritt weiter geht der am 20.09.2006 öffentlich angekündigte Dienst CWsandbox: Entstanden aus einer Diplomarbeit an der Uni Mannheim wurde eine Web-Schnittstelle zum Hochladen verdächtiger Dateien entwickelt. CWsandbox unterzieht diese Datei anschließend einer dynamischen Analyse; die Datei wird in einer kontrollierten Umgebung ausgeführt und beobachtet. CWsandbox dokumentiert für den untersuchten Prozess z.B. die nachgeladenen Systembibliotheken (DLLs), das Starten und Beenden weiterer Prozesse, Verändern oder Lesen von Registry-Einträgen, das Installieren oder Starten von Diensten sowie aktive Netzwerkverbindungen. Das Ergebnis wird dem Benutzer anschließend in Form einer XML-Datei per E-Mail übermittelt – ein echter Mehrwert bei der Analyse verdächtiger Anwendungen.

Wer AN.ONymisiert, wird beschlagnahmt

Im Rahmen aktueller Vorermittlungen der Staatsanwaltschaft Konstanz gegen die Verbreitung von Kinderpornografie wurden Anfang September ca. ein Dutzend IT-Systeme beschlagnahmt, unter denen sich auch Exit-Nodes und Kaskadensysteme der Anonymisierungsdienste TOR und AN.ON befanden, darunter auch ein System des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD). Ein déjà vu – AN.ON wurde am 03.07.2003 schon einmal per Gerichtsbeschluss verpflichtet, Protokollierungsdaten an Strafverfolgungsbehörden herauszugeben, mit längerem Nachspiel.

Der Informationsgewinn über die anonymisierten Dienstnutzer dürfte gering ausfallen, da in Mix-Netzen die Kommunikationsbeziehung nur dann rekonstruiert werden kann, wenn alle Systeme eines vollständigen „Kommunikationspfads“ vorliegen. Inwieweit die Professionalisierung zukünftiger Ermittlungen auch die Recherche bereits verfügbarer Informationen umfassen wird, bleibt abzuwarten.

Als sicher dagegen kann gelten, dass die Fahndungszielgruppe einfach auf ausländische Serverknoten solcher Anonymisierungsnetzwerke ausweichen wird, und dass sicherlich auch keine Backbonerouter von großen ISPs beschlagnahmt werden, die illegalen Inhalt transportieren (genauer: durchleiten und nicht speichern). Die nächste Generation von autonomen Anonymisierungsnetzwerken wird sich wohl ohnehin über Wurm-Mechanismen automatisch verbreiten, sodass der direkte Bezug zwischen Infrastruktur und Betreiber wegfällt – wie aber beschlagnahmt man einen Wurm?

Secorvo News

Secorvo College aktuell

Der Herbst steht bei Secorvo College im Zeichen des Sicherheitsmanagements: Einen umfassenden Einstieg bietet das bewährte Seminar „Information Security Management von A(udit) bis Z(ertifizierung)“ vom 17.-18./20.10.2006. Im November folgt ein ganz besonderes Seminar: Über 3,5 Tage werden vom 06.-09.11.2006 die „Erfolgsfaktoren für IT-Security Management“ beleuchtet. Darin werden die besonderen Anforderungen an Kommunikation, Präsentation, Gruppenmanagement und Führung vertieft und geübt, denen sich IT Security Verantwortliche stellen müssen. Das Seminar wird im Januar fortgesetzt.

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

White Paper Security Management Praxis

Nach dem großen Erfolg seines Secorvo White Papers “BS 7799 – von Best Practice zum Standard“ (über 30.000 Downloads) hat Jörg Völker seine Einführung in das Sicherheitsmanagement nun um eine Case Study ergänzt, in der er an einem konkreten Fall seine Erfahrungen mit dem Aufbau zertifizierter Information Security Management-Systeme dokumentiert. Es ist als Secorvo White Paper Nr. 13 seit dem 24.09.2006 online.

Veranstaltungshinweise

Auszug aus www.veranstaltungen-it-sicherheit.de

Oktober 2006	
10.-12.10.	ISSE 2006 (TeleTrusT/EEMA, Rom/IT)
16.-20.10.	Information Security Management (Secorvo College, Karlsruhe)
17.-18.10.	DACH Mobility 2006 (GI/ÖCG/BITKOM/SI, München)
18.10.	KA-IT-Si-Jubiläumsfeier (KA-IT-Si, IHK Karlsruhe)
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
06.-09.11.	Erfolgsfaktoren für IT-Security Management (Secorvo College, Karlsruhe)
07.11.	IT Risk Management 2006 (COMPUTAS, Berlin)
14.-16.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
20.-25.11.	TISP-Schulung (Secorvo College, Karlsruhe)
26.11.	TISP-Prüfung (Secorvo College, Karlsruhe)
28.-30.11.	Kommunikationsschutz und Datensicherheit (Secorvo College, Karlsruhe)

Fundsachen

Auszug aus www.security-finder.de

Introducing a Free New Self-Service Tool That Runs Comprehensive Security Checks in Minutes, Not Days. Vorstellung des SAP-Tools "Security Optimization Self-Service", das mit dem SAP Solution Manager (ab Version 3.1) kostenfrei mitgeliefert wird. Es erleichtert Überprüfungen der Berechtigungen in einer SAP-Systemlandschaft.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, 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

secorvo
security consulting

Secorvo Security News

Oktober 2006

Editorial: Verboten

Je mehr Verbote, desto ärmer das Volk.
Laotse, Dao-de-dsching

Verbote besitzen einen unbestreitbaren Vorteil: Mit ihnen wird zielgerichtetes Handeln des Gesetzgebers demonstriert – und diese Klarheit kommt an beim Publikum. Die Wirklichkeit dagegen besitzt einen hässlichen Nachteil: Sie ist komplex – und das häufig in größerem Maße, als es der Mensch mit seiner zur Vereinfachung neigenden Wahrnehmung zu erfassen vermag. Das dürfte die tiefere Ursache dafür sein, dass klare Verbote einerseits so beliebt sind – und mit ihnen andererseits oft nicht nur nicht das angestrebte Ziel, sondern sogar dessen Gegenteil erreicht wird.

Beispielhaft lässt sich dies bei der geplanten Änderung des Strafgesetzbuches beobachten. Mit dem neuen § 202c sollen Vorbereitungshandlungen des Ausspähens und Zugänglichmachens von Daten unter Strafe gestellt werden – darunter auch die Herstellung, Verschaffung und Verbreitung von Computerprogrammen, „deren Zweck die Begehung einer solchen Tat ist". An wenigstens drei grundsätzlichen Fehlverständnissen krankt dieses Vorhaben:

1. *Ein Hacker-Tool ist von einem Sicherheits-Tool oft nicht unterscheidbar*. So wird der ehemalige Trojaner Netbus heute als Tool für die Remote-Wartung vertrieben, und Cain & Abel wird zur Wiedergewinnung verlorener Passwörter empfohlen. Eine „objektive Zweckbestimmung" ist da schwer auszumachen.
2. *Die öffentliche Verbreitung von Angriffs-Tools ist ein Sicherheitsgarant*. Nur wenn Hacker nicht im Verborgenen wirken, wissen wir, was sie wirklich können. Dies ist wesentliche Vorbedingung für das Ergreifen angemessener Sicherheitsmaßnahmen.
3. *Die Nutzung von Hacker-Tools steigert die Sicherheit von IT-Infrastrukturen* – das fordert auch das BSI und verbreitet Nessus seit dem 17.06.2005 (SSN 06/2005) über ihre BOSS-CD. Vielleicht hört die Justizministerin wenigstens auf das Bundesamt?

Inhalt

secorvo
security consulting

Security News

Schach den Wahlmaschinen

Seit einigen Jahren werden zur Vereinfachung des Auszählungsverfahrens bei Wahlen Maschinen der niederländischen Firma Nedap für die Stimmabgabe eingesetzt. Das Modell ESD1 besitzt eine Zulassung des Bundesinnenministeriums; mehr als 15 Mio. Stimmabgaben erfolgten bisher bei Kommunal-, Landtags- und Bundestagswahlen auf solchen Geräten. Geschäftsführer Jan Groenendaal preist seine Geräte als „Dedicated Special Purpose" Maschinen: „Dass man mit unserer Wahlmaschine auch Schach spielen kann, würde ich gerne vorgeführt bekommen."

Der Spott dürfte ihm am 04.10.2006 im Halse stecken geblieben sein: In einem Bericht des niederländischen Fernsehens demonstrierte eine Aktivistengruppe ihren „Nedap Schachcomputer" – der Austausch des EPROMs beim (in 90 % der Wahllokale in den Niederlanden eingesetzten und mit ESD1 weitgehend baugleichen) Wahlcomputer ES3B dauerte keine fünf Minuten, die Anbringung des Schachbretts auf der schrägen Bedienfläche war etwas aufwändiger.

Am 05.10.2006 publizierte die Gruppe eine umfangreiche Sicherheitsanalyse und schob am 10.10.2006 auf YouTube ein Video nach, das zeigt, dass die Stimmabgabe noch aus 25 m Entfernung abgehört werden kann. Tatsächlich lassen sich Manipulationen an Wahlmaschinen nur durch Geräteprüfungen verbunden mit signiertem Programmcode und versiegelten Maschinen nachweisen – eine sehr aufwändige Prozedur, die allerdings nicht vor Manipulationscode im Original-EPROM schützt.

Internet Security Threat Report

Am 25.10.2006 veröffentlichte Symantec ihren 10. Internet Security Threat Report. Darin werden auf gut 100 Seiten die von Symantec im Zeitraum vom 01.01. bis 30.06.2006 mit über 40.000 Sensoren weltweit beobachteten Bedrohungen zusammengefasst. Gegenüber früheren Reports ist bei Angriffen eine Verlagerung der Ziele von der Infrastruktur hin zu Endbenutzer-PCs und Web-Applikationen zu beobachten. Ursächlich dürfte dies auf eine Verschiebung der Interessen von Angreifern zurück zu führen sein – weg von „traditionellen" Motiven wie Geltungssucht hin zu kriminellen Interessen.

Etwa 69 % aller gefundenen Schwachstellen betreffen Web-Applikationen. Hier besteht seitens der Software-Entwickler erheblicher Handlungsbedarf – vor allem, weil diese Schwachstellen 78 % aller leicht nutzbaren ausmachen. Meist handelt es sich um längst bekannte Probleme wie SQL-Injection und Cross-Site-Skripting. Ebenfalls bemerkenswert ist der starke Anstieg von Phishing-Attacken, die im Beobachtungszeitraum um 81 % auf über 157.000 unterschiedliche Nachrichten anstiegen. Als Top-Herausforderungen sieht der Report die Entwicklungen um Web 2.0 (AJAX) und Windows Vista.

iPod spielt „Trojanisches Pferd"

Am 18.10.2006 gab Apple bekannt, dass Video-iPods mit dem Windows RavMonE.exe-Virus ausgeliefert worden waren. Erst am 13.10.2006 hatte die japanische McDonalds-Zentrale vor 10.000 im Rahmen eines Gewinnspiels verteilten, mit dem Trojaner QQPass verseuchten MP3-Playern gewarnt. Zwei Beispiele für Bedrohungen, die in Geräten aus vermeintlich vertrauenswürdiger Quelle lauern können – Trojanische Pferde im ursprünglichen Sinn.

USB Dumper

Dass *mit* USB-Sticks Viren übertragen oder unerlaubt Daten ausgetauscht werden können, ist bekannt. Die Bedrohung *von* USB-Sticks wird jedoch meist nicht gesehen: Steckt man den eigenen USB-Stick in ein fremdes System, auf dem ein Tool wie „USB-Dumper" installiert ist, so werden unbemerkt sämtliche Inhalte des Sticks auf das System kopiert. Ebenso ist es möglich, ein komplettes Image des USB-Sticks zu erstellen, mit dem selbst gelöschte Dateien wieder hergestellt werden können.

Daher ist grundsätzlich der Einsatz von Verschlüsselungslösungen für sensible Daten auf USB-Sticks, mindestens aber eines Tools zum sicheren Löschen (wie beispielsweise „Eraser") zu empfehlen.

Panzerung publik

Am 10.10.2006 berichtete die Financial Times Deutschland über einen bereits am 21.09.2006 erfolgten Diebstahl von Laptops und Flachbildschirmen aus einem VW- und Audi-Vertriebszentrum in Teltow. Das ermittelnde LKA hat den Fall als brisant eingestuft, da auf den entwendeten Systemen auch Informationen über die Sicherheitseigenschaften und -ausstattungen sowie den Aufbau der Dienstfahrzeuge hochrangiger Spitzenpolitiker gespeichert sein sollen. Die Meldung gelangte trotz Nachrichtensperre während der noch andauernden Ermittlungen in die Öffentlichkeit.

Bleibt zu hoffen, dass der Vorfall nicht nur den betroffenen Unternehmen zu denken gibt, sondern allen, die noch immer über keinen durchgängigen Schutz sensibler Daten insbesondere auf mobilen Systemen verfügen – selbst wenn es sich herausstellen sollte, dass es sich in diesem Fall um keinen gezielten Informationsdiebstahl gehandelt hat.

Überblick SAP-Ports

SAP veröffentlichte am 13.10.2006 im NetWeaver Security Knowledge Center eine Neufassung der praktischen und umfassenden Übersicht der von den unterschiedlichen SAP-Anwendungen genutzten TCP- und UDP-Ports. Allein die Zahl der Kommunikationsmöglichkeiten verdeutlicht, wie wichtig es ist, beim Einsatz von SAP-Anwendungen ein ausgereiftes Netzsicherheitskonzept umzusetzen – mit jeder Schwachstelle in der Software droht sonst ein Einfallstor.

Begrüßenswert wäre es allerdings, wenn SAP sich hinsichtlich der genutzten und publizierten Ports mit den Protocol Number Assignment Services der global anerkannten Portliste von IANA abstimmen würde.

Manipulation des Vista Kernel

Einen perfiden Angriff auf den Vista Kernel demonstrierte Joanna Rutkowska auf der diesjährigen Blackhat: Es gelang ihr, durch direkte Zugriffe auf die Festplatte das Swapfile so zu manipulieren, dass dem Vista Kernel unsignierter Code untergeschoben wurde – was die Architektur des Kernels eigentlich durch die Verwendung von Codesignaturen verhindern sollte.

Abhilfe könnte eine Verschlüsselung des Swapfiles schaffen; damit wäre der für diesen Angriff erforderliche direkte Plattenzugriff nicht mehr möglich. Alternativ könnte man auch – ausreichend physikalischen Speicher vorausgesetzt – das Swapfile komplett deaktivieren. Denn das Konzept der „Auslagerung von RAM auf Festplatte" stammt aus Zeiten, in denen Speicherbausteine noch sehr teuer waren.

Security Awareness Monitor

Das Steinbeis-Beratungszentrum Karlsruhe hat auf der Grundlage wissenschaftlicher Methoden der Marktforschung ein Tool entwickelt, mit dem die Sensibilität (Awareness) der Mitarbeiter für Belange der IT-Sicherheit gemessen werden kann – den Security Awareness Monitor (SAM). Der Monitor wurde bereits erfolgreich zur Erfolgsmessung in einer Awareness-Kampagne der T-Systems eingesetzt. Die Ergebnisse dieser Messungen hatte Professor Dr. Konrad Zerr, Leiter des Beratungszentrums, auf dem diesjährigen Karlsruher Security Awareness Symposium vorgestellt.

Secorvo News

Secorvo College aktuell

Neben der Zertifizierung zum T.I.S.P. vom **20. bis 25.11.2006** (siehe unten) gibt es in diesem Jahr noch zwei weitere Gelegenheiten, vom Wissenstransfer eines Secorvo College-Seminars zu profitieren:

- Vom **14. bis 16.11.2006** vermittelt das Seminar „IT-Sicherheitsaudits in der Praxis" unsere Best Practices aus acht Jahren Sicherheitsaudits.
- Vom **28. bis 30.11.2006** folgt ein echter Klassiker: die aktuelle Fassung eines des erfolgreichsten College-Seminare: Kommunikationsschutz und Datensicherheit – intern, extern, mobil.

Programm, Preise und Online-Anmeldung unter

http://www.secorvo.de/college

T.I.S.P. @ Secorvo College

In fünf Tagen zum zertifizierten Information Security Professional: Mit mehr als 100 Absolventen hat sich der „TeleTrusT Information Security Professional" (T.I.S.P.) in weniger als drei Jahren zu einem der verbreitetsten Security-Zertifikate „gemausert".

Dieser Entwicklung trägt Secorvo College durch das Angebot eines T.I.S.P.-„Steilkurses" Rechnung – erstmalig vom **20. bis 25.11.2006** inklusive zugehöriger Prüfung. Für diese Erstveranstaltung zahlen alle Teilnehmer den Frühbucherpreis.

Erfolgreiches KA-IT-Si-Jubiläum

Am 18.10. feierte die auf Initiative von Secorvo und den Karlsruher Versicherungen Anfang 2001 gegründete Karlsruher IT-Sicherheitsinitiative (kurz: KA-IT-Si) ihr fünfjähriges Bestehen – mit weit über 100 Teilnehmern, einer Key Note des Präsidenten des Bundesamtes für Sicherheit in der Informationstechnik, BSI (vertreten durch den Abteilungspräsidenten Bernd Kowalski) und Vorträge und Demonstrationen rund um ein ganzheitliches Verständnis der IT-Sicherheit.

Pünktlich zum Geburtstag stießen zwei neue Partner zur Initiative: die Karlsruher ptv AG und die CONNECT Karlsruhe Computer und Netzwerktechnik GmbH.

Die Unterlagen der Veranstaltung können von der Webseite der Sicherheitsinitiative heruntergeladen werden.

Veranstaltungshinweise

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

Oktober 2006	
23.-27.10.	Systems 2006 (Messe München, München)
November 2006	
07.11.	IT Risk Management 2006 (COMPUTAS, Berlin)
14.-16.11.	IT-Sicherheitsaudits in der Praxis (Secorvo College, Karlsruhe)
20.-24.11.	TISP-Schulung (Secorvo College, Karlsruhe)
25.11.	TISP-Prüfung (Secorvo College, Karlsruhe)
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)

Fundsachen

Auszug aus www.security-finder.de

Security Engineering –
A Guide to Building Dependable Distributed Systems
Das wegweisende Standardwerk von Ross Anderson ist nun auch online verfügbar. Obwohl fünf Jahre auf dem Markt, hat es nichts an Aktualität eingebüßt, sondern thematisiert alle für die Entwicklung von IT-Systemen relevanten Sicherheitsaspekte, von Passwörtern über Protokolle, Tamper Resistance und Telekommunikationssicherheit bis Monitoring und Management. Ein Muss für alle, die mit Design, Entwicklung oder Implementierung sicherer Systeme befasst sind.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, 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

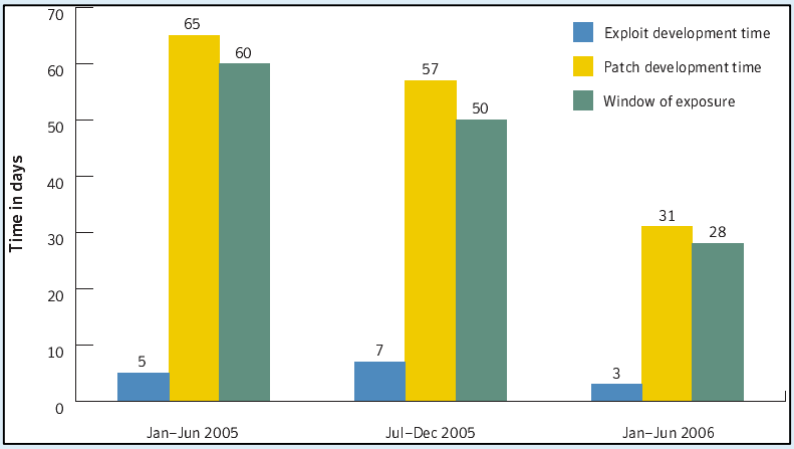
secorvo
security consulting

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

secorvo
security consulting

Secorvo Security News

Dezember 2006

Editorial: Top five

Die Tyrannei der Listen, denen Nick Hornby 1995 in „High Fidelity“ ein Denkmal gesetzt hat, beschränkt sich längst nicht mehr auf die „Top Ten“ des Musikgeschäfts. Wer heute ein Buch sucht, kommt an den einschlägigen „Bestsellerlisten“ kaum vorbei, und jeder Online-Shop, der etwas auf sich hält, bietet auf Mausklick eine Übersicht der meistverkauften Produkte. Nun haftet diesen „Best of“ ein wenig der Ruch einer Aktienempfehlung an: Hat ein Produkt den Olymp einer Top-Liste erklommen, wird die Nennung zur „self fulfilling prophecy“ (Robert K. Merton). Dabei ist deren Zustandekommen oft nicht frei von Willkür: Erst kürzlich wurde ein Plattenproduzent überführt, große Bestände einer Neuerscheinung selbst aufgekauft zu haben, um mit dem Bestseller-Status die Verkäufe anzukurbeln. Eine probate Methode, um Ladenhüter in Saisonhits zu verwandeln.

Auch in der IT-Sicherheit geht der Trend zur Liste: SANS veröffentlicht seit sechs Jahren die „Top 20“ der Internet Security Attack Targets, OWASP pflegt seit 2003 die „OWASP Top Ten“ der kritischsten Fehler in Web-Anwendungen, und auf den Webseiten aller Anti-Viren-Hersteller findet man die „Viren des Monats“.

Bei so viel Orakel-Prominenz wollen wir uns nicht drücken – daher hier die Secorvo Top Five der Security-Trends 2007:

1. ***Sichere Softwareentwicklung***: Wenn die Software-Industrie hier nicht punktet, droht eine Regulierung der EU.
2. ***Awareness***: Angesichts zunehmender Mobilität und technischer Konvergenz wird das Nutzerverhalten zum Schlüsselfaktor.
3. ***Datenschutz***: Sensibilisierte Benutzer und gestärkte Aufsichtsbehörden reduzieren das verbreitete Vollzugsdefizit.
4. ***Best Practices***: Gestiegene (Haftungs-) Risiken lassen den Ruf nach Standards, Audits und Best Practices lauter werden.
5. ***Anti-Phishing***: Gelingt es nicht, den kriminellen Onlinekonten-Zugriff zu stoppen, kann das Vertrauen in das eBusiness kippen.

Inhalt

secorvo
security consulting

Security News

BOSS reloaded

Am 01.12.2006 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Verfügbarkeit der Version 2.0 seiner Sicherheits-CD BOSS (BSI OSS Security Suite) bekannt gegeben. Sie umfasst Version 2.2.8 von Nessus mit deutsch übersetzter Oberfläche; die Nessus-Meldungen erscheinen allerdings nur in englisch. Unter den weiteren Tools zur Sicherheitsanalyse findet sich überraschend Version 0.10.10 des bekannten Sniffers Ethereal vom 11.03.2005 (statt einer aktuellen Version des Nachfolgers Wireshark).

Auch wenn die BOSS-CD aus den inzwischen zahlreichen Tool-Suites nicht signifikant hervor sticht – die Veröffentlichung ist ein Signal, dass das BSI weiterhin auf die Rechtmäßigkeit des Besitzes und der Verbreitung von Hacking-Tools setzt.

Zero-Day und Hexenjagd

Seit Anfang Dezember gibt es einen öffentlichen und übersichtlichen Informationsdienst zu Echtzeitschwachstellen (Zero-Day Tracker). Darin werden erstmals alle Schwachstellen zusammengefasst, für die bereits technische Details zur Ausnutzbarkeit bekannt sind, der Hersteller aber noch keinen Patch veröffentlicht hat. Wichtig für IT-Sicherheitsmanager, die ihre Risiken aktiv steuern, sind die Angabe, wie lange eine ungepatchte Schwachstelle bereits bekannt ist (z.B. seit 393 Tagen) und wie zwischenzeitlich improvisiert werden kann. Ob zukünftig dort auch nicht behobene Fehler von Anwendungen, Datenbanken und Netzsoftware eingestellt werden, bleibt abzuwarten.

Von den Herstellern sollte das Angebot als Ansporn zur Verbesserung der Sicherheit in der Softwareentwicklung verstanden werden. Repressalien sind sicher die falsche Antwort, wie im Fall des Boarding Pass Generators "Create your own boarding pass" für Northwest Airlines versucht: Der PhD-Student Christopher Soghoian hatte darin ein seit über drei Jahren bekanntes organisatorisches Sicherheitsloch als Proof-of-Concept in Software umgesetzt.

Final BS 25999-1:2006

Ende November 2006 wurde vom British Standards Institute (BSI) die Endfassung des BS 25999-1:2006 veröffentlicht. Dieser „Code of Practice for Business Continuity Management" gibt Empfehlungen für Notfall- und Notfallvorsorgeplanung in Unternehmen. Ein zweiter Teil, der eine Zertifizierung analog BS 7799-2 ermöglichen wird, soll 2007 folgen. Der neue Standard löst PAS 56 ab und wird ergänzt durch die im August 2006 veröffentlichten Empfehlungen PAS 77:2006 „IT Service Continuity Management".

Eine Gelegenheit zum Erfahrungsaustausch bietet vom 01.-02.02.2007 die Konferenz „3rd Annual: BUSINESS CONTINUITY 2007" in London.

Fuzzing with JBroFuzz

Am 13.11.2006 wurde im OWASP-Projekt das Fuzzing-Tool JBroFuzz veröffentlicht. JBroFuzz ist ein „stateles network protocol fuzzer" zur Aufdeckung von Schwachstellen in Netzwerkprotokollen durch halbautomatisch generierte fehlerhafte Datenpakete. Die intuitive Oberfläche von JBroFuzz erlaubt auch Anfängern, die Funktionsweise von Fuzzing nachzuvollziehen und anzuwenden. Das in Java programmierte Tool steht plattformübergreifend zur Verfügung.

Die Architekturen von Web 2.0 stellen neue Anforderungen an die Sicherheit von Online-Anwendungen. Interessant, auch im Zusammenspiel mit JBroFuzz, ist das Mozilla-Plugin Firebug, mit dem sich die Sicherheit von Web-Applikationen schnell auf vielfältige Weise untersuchen lässt.

DFN-PKI CA im Browser

Die oberste Zertifizierungsstelle des Deutschen Forschungsnetzes, die DFN-PCA, feiert 2006 ihren 10. Geburtstag. Dass sie nicht zum alten Eisen zählt, beweisen etliche Neuigkeiten, über die am Nikolaustag informiert wurde. Die spektakulärste darunter ist, dass das Root-Zertifikat der DFN-PCA ab sofort über einen direkten Zertifizierungspfad in die wichtigsten Standard-Browser verfügt.

Um dies zu realisieren wählte man nicht den teuren und aufwändigen Weg der direkten Einbindung in die Browser – vielmehr hat eine Kooperation mit der in den Browsern bereits enthaltenen Deutsche Telekom Root CA dazu geführt, dass störende Warnmeldungen, z.B. beim Aufbau einer SSL-Verbindung, der Vergangenheit angehören. Von diesem im Forschungsumfeld bislang weltweit einmaligen Schritt profitieren sowohl Endanwender mit kostenlosem Webserver-Zertifikat als auch die vielen Forschungseinrichtungen, die den Betrieb ihrer CA an die DFN-PKI ausgelagert haben.

Virtuelle Kriminalität

Am 21.02.2005 veröffentlichte McAfee den ersten Bericht zum Thema virtuelle Kriminalität. Beschrieben wurde darin der Trend zum Missbrauch des Internet für Zwecke des organisierten Verbrechens.

Am 08.12.2006 wurde der zweite Bericht der Öffentlichkeit vorgestellt. Er enthält eine Reihe kon-

kreter Fallstudien und Zitate von Security-Experten zu virtueller Kriminalität. Zu den drei wesentlichen Erkenntnissen zählen (1) die Entstehung einer neuen Generation von Kriminellen, die das Internet für Straftaten nutzt, die bislang nicht oder nur schwer durchführbar waren; (2) die Entdeckung der Missbrauchsmöglichkeiten durch die organisierte Kriminalität, die insbesondere Großereignisse wie die Fußball-WM für virtuelle Straftaten ausnutzt; sowie (3) die noch immer unterschätzte Bedrohung durch Innentäter. Nur der Titel mag nicht passen – denn virtuell ist diese Kriminalität bei Weitem nicht.

Honey-Clients

Die Honeypot-Technologie wird in der Regel server- oder netzwerkseitig – beispielsweise in Form kompletter Honeynets – betrieben. Einen interessanten anderen Ansatz verfolgen Client-Honeypots: Sie suchen selbst aktiv nach Schad-Software auf Webseiten, mit denen ungepatchte Browser angegriffen werden können.

Bereits 2005 stellte Microsoft Research mit dem Projekt „Strider HoneyMonkey“ eine Realisierung von XP-basierten Client-Honeypots vor (SSN 8/05). In den vergangenen Tagen wurden drei weitere viel versprechende Ansätze veröffentlicht:

- Bei Capture handelt es sich um einen „High Interaction Client Honeypot", der insbesondere Webseiten nach versteckten Viren, Würmern und Trojanern durchsucht und die Ergebnisse protokolliert. Capture läuft in einer virtuellen Umgebung, so dass das System nach einer Infizierung schnell „gesäubert“ werden kann.
- Wie Capture sucht auch Monkey Spider nach maliziösen Webseiten, hat eine deutlich weniger aufwändige Architektur und zählt eher zur Klasse der „Low Interaction Honeypots“. Es basiert unter anderem auf CWsandbox.
- Botspy schließlich geht einen Schritt weiter: Es beobachtet Bot-Netze, die häufig die Quelle für per E-Mail versandte Phishing- oder Viren-Nachrichten sind.

Fazit: Obwohl die Tools sich in einem frühen Entwicklungsstadium befinden, zeigen sie die Leistungsfähigkeit des Client-Honeypot-Ansatzes.

Privatsphäre mit Microsoft

Vom 16.10.2006 datieren die „Privacy Guidelines for Developing Software Products and Services“ von Microsoft (v2.1). Einige der darin postulierten Prinzipien decken sich mit dem europäischen Datenschutzrecht – wie Datensparsamkeit, Transparenz und Nutzerkontrolle. Insgesamt ist das Dokument jedoch stark „sicherheitslastig“ und betont Integrität und Zugriffsschutz, vergisst aber das Prinzip der Zweckbindung. Auch die Checklisten der gut gemeinten beispielhaften Szenarien lesen sich mit europäischen Augen eigenwillig: Für das „anonyme Monitoring“ durch einen Internet-Provider wird die „explizite Zustimmung des Nutzers“ gefordert.

Immerhin wurde die Bedeutung des Datenschutzes von Microsoft durch die Integration der Guidelines in den „Trustworthy Computing Security Development Lifecycle (SDL)“ unterstrichen.

Alle Jahre wieder...

...findet der DFN-CERT Workshop „Sicherheit in vernetzten Systemen“ in Hamburg statt – am 07.-08.02.2007 nun schon zum 14. Mal. Neben etlichen spannenden eingereichten Beiträgen bildet der eingeladene Vortrag zu „Stealth Malware – can good guys win?“ von Joanna Rutkowska ein Highlight.

Augen auf beim Weihnachtskauf

Die Warnung der bayrischen Polizei vom 24.04.2006 vor dem Kauf von Plüschtieren mit eingebauter Überwachungskamera ist laut Pressemitteilung vom 11.12.2006 von mindestens einem Käufer ignoriert worden. Diesem drohen jetzt rechtliche Konsequenzen, da nach § 90 Telekommunikationsgesetz (TKG) schon der Besitz von Sendeanlagen, „die ihrer Form nach einen anderen Gegenstand vortäuschen oder die mit Gegenständen des täglichen Gebrauchs verkleidet sind“ verboten ist. Vorsicht beim Kauf Ihrer Weihnachtsgeschenke!

Secorvo News

Secorvo College aktuell

In das Jahr 2007 startet Secorvo College mit den aktualisierten Seminarklassikern ISM – Information Security Management (23.-26.01.2007), PKI (30.01.-02.02.2007) und IT-Sicherheit heute (06.-08.02.2007), gefolgt von dem komplett überarbeiteten Seminar Erfolgsfaktoren für IT-Sicherheitsmanagement (26.02.-01.03.2007).

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

T.I.S.P.

Auf seiner Sitzung am 07.12.2006 bei Secorvo hat sich das T.I.S.P.-Board darauf verständigt, 2007 eine Weiterentwicklung des erfolgreichen T.I.S.P. Zertifikats in Angriff zu nehmen. So ist geplant zusätzliche Spezialisten-Zertifikate zu entwickeln. Die zweite T.I.S.P.-Zertifikat-Schulung mit anschließender Prüfung wird Secorvo am 05.-09.03.2007 durchführen; mehrere Anmeldungen liegen bereits vor.

Veranstaltungshinweise

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

Dezember 2006	
24.12.	Heiligabend
27.-30.12.	23. Chaos Communication Congress (CCC, Berlin)
Januar 2007	
18.-19.01.	Tutorium "IT-Sicherheitskriterien im Vergleich" (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)
Februar 2007	
06.-08.02.	IT-Sicherheit heute – Angriffe, Konzepte, Lösungen (Secorvo College, Karlsruhe)
07.-08.02.	DFN-CERT Workshop: Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
26.02.-01.03.	Erfolgsfaktoren für IT-Security Management (Secorvo College, Karlsruhe)
26.-27.02	Net-ID 2007 (Computas, Berlin)

Fundsachen

Auszug aus www.security-finder.de

Microsofts Security Risk Management Guide (v1.2) beschreibt einen vierphasigen Planungsprozess für ein effektives Security Risk Management System. Die Vorgehensweise basiert auf etablierten Industriestandards und Best Practices. Der Guide umfasst eine Sammlung von Excel-Tools.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Stefan Kelm, 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