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

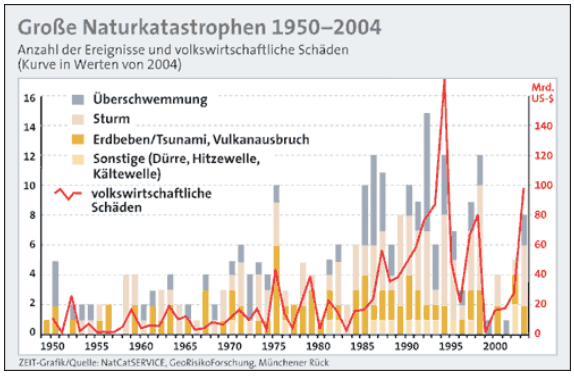
ISSN 1613-4311

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