Secorvo Security News
Juni 2004

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

Nr. 6, 3. Jhrg. 2004
Stand 25. Juni 2004

ISSN 1613-4311

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

Inhalt

Editorial: Chefsache

„IT-Sicherheit ist Chefsache“: Eine oft genutzte, als Slogan missbrauchte, zur Phrase gedroschene – aber tatsächlich zutreffende Behauptung. Allerdings meist falsch oder sogar gänzlich unverstanden. Über 55% der Befragten einer aktuellen Studie von silicon.de bewerten sie als „wichtig“ oder sogar „sehr wichtig“ (32%). Da lohnt ein kritischer Blick.

Zunächst einmal ist die Aussage trivial: Handelt es sich bei IT-Sicherheit um eine Angelegenheit, um die sich ein Unternehmen kümmern muss, dann liegt die Verantwortung dafür natürlich bei der Unternehmensleitung – wo auch sonst.

Tatsächlich hat die Aussage größere Tragweite. Kaum ein Unternehmen, bei dem heute nicht zumindest einzelne, wenn nicht zentrale oder gar alle Geschäftsprozesse in erhebliche Abhängigkeit von Teilbereichen der eingesetzten Informationstechnik geraten sind. Die zuvor verwendeten (manuellen) Prozesse wurden fast immer vollständig abgelöst – daher existieren nur noch sehr selten Ersatzprozesse für den Fall des Ausfalls. Nur noch wenige Unternehmen würden heute einen eintägigen IT-Ausfall problemlos „wegstecken“, fast alle könnte ein einwöchiger Ausfall in eine Existenz bedrohende Schieflage bringen.

Nur: Die wenigsten Unternehmen kümmern sich um dieses Problem so, wie es die „Sorgfalt eines ordentlichen Geschäftsmanns“ (§ 43 GmbHG) „und gewissenhaften Geschäftsleiters“ (§ 93 AktG) gebieten. Das Aktienrecht fordert sogar explizit und zwingend die Einrichtung eines Überwachungssystems zur Erkennung von „den Fortbestand des Unternehmens gefährdenden Entwicklungen“ (KontraG, § 91 AktG).

Zwar kann die Geschäftsleitung das Thema delegieren. Wählt sie jedoch nicht sorgfältig geeignete Mitarbeiter dafür aus, gibt sie die für die Umsetzung erforderlichen Mittel nicht frei oder kontrolliert sie nicht die Qualität des Ergebnisses, verletzt sie ihre Sorgfaltspflicht – und haftet im Schadensfall.

1 Security News

1.1 „Phishing“ auf dem Vormarsch

Die Fälle von Betrugsversuchen durch so genanntes „Phishing“ nehmen auch im deutschsprachigen Raum zu. E-Mails, die angeblich von E-Business-Angeboten wie z. B. Ebay oder einer Direktbank stammen, fordern den Benutzer dazu auf, seine Accountdaten zu überprüfen. Klickt der Empfänger auf den in der E-Mail enthaltenen Link, landet er auf einer Webseite, die wie die Originalseiten aussieht – tatsächlich aber von Betrügern angelegt wurde. Dabei nutzen einige „Phisher“ Sicherheitsschwächen von Browsern, wie z. B. die am 18.06. 2004 gemeldete Schwachstelle von Opera, mit der die dem Benutzer angezeigte URL manipuliert werden kann.

Fällt der Empfänger auf den Bluff herein und gibt bereitwillig Konto- oder Kreditkartennummer, PIN und womöglich eine TAN ein, kann der Angreifer selbst auf den Account zugreifen. Dabei lassen sich „Phishing“-E-Mails leicht erkennen: Seriöse Anbieter versenden grundätzlich keine E-Mails dieser Art.

1.2 Studie von silicon.de

Nach einer Pause von drei Jahren hat silicon.de am 04.06.2004 eine zweite umfangreiche Studie zur IT-Sicherheit auf der Basis von über 1.000 Fragebögen vorgelegt. Zahlreiche Ergebnisse sind wenig überraschend, interessant allerdings das eine oder andere Detail:

- Dramatisch erscheint der Anstieg der Angriffe mit Trojanischen Pferden: Gaben in der ersten Studie nur 20% der Befragten Sicherheitsvorfälle mit Trojanern an, stieg die Zahl in der aktuellen bereits auf 42%.
- Direkt auf den Schutz des Netzwerks folgt als zweitwichtigster Faktor einer effektiven IT-Sicherheit das Sicherheitsbewusstsein der Mitarbeiter: fast 90% der Befragten stuften es als „sehr wichtig“ (63%) oder „wichtig“ ein. Auch die große Resonanz auf das 2. Deutsche Security Awareness Symposium (29.-30.06.2004) bestätigt diesen Trend.
- Als „Daumengröße“ zur Abschätzung des Investitionsvolumens für IT-Sicherheit scheint sich ein Wert von 5-10% des IT-Budgets einzuschwingen: Mehr als ein Drittel der befragten Unternehmen liegt in diesem Bereich, ein weiteres Drittel knapp darüber oder darunter.

1.3 Happy Birthday, Diffie!

Der (Mit-) Entdecker der Public Key Kryptographie Whitfield Diffie feierte am 05.06. 2004 seinen 60. Geburtstag. Auch von uns ein herzliches Prosit auf Diffie, der – mittlerweile in der Funktion des Chief Security Officer von Sun – seit seiner bahnbrechenden Entdeckung zusammen mit Martin E. Hellman Mitte der 70er Jahre weder seine Haarpracht noch seinen Spaß an (Datenschutz-motivierten) Cracks verloren hat.

1.4 Hilfe bei Wurmbefall

Nach Feststellung eines Viren- oder Wurmbefalls stellt sich die Frage „Was tun?“ Aus Sicherheitsperspektive ist die Empfehlung eindeutig: System-Image bzw. Backup zurückspielen oder das System neu aufsetzen. In manchen Fällen können die Schädlinge auch durch das Starten des Betriebssystems im abgesicherten Modus und anschließendem manuellen Entfernen beseitigt werden.

Alternativ können spezielle Virus Removal Tools wie Stinger des Herstellers NAI hilfreich sein – die sicherste Methode bleibt aber ein Neuaufsetzen der betroffenen Systeme. Das effektivste Verfahren ist jedoch der vorbeugende Einsatz aktueller Virenscanner und die regelmäßige Aktualisierung der zugehörigen Viren-Informationsdatenbank.

1.5 MS Antivirus-Guide

Von Microsoft wurde am 15.06.2004 ein „Antivirus Defense-in-Depth Guide“ zur Verfügung gestellt. Warum das englischsprachige, 90seitige pdf-Dokument als ausführbare MSI-Installer-Datei zum Download angeboten wird, entzieht sich allerdings dem Verständnis.

Das umfassende Werk enthält nicht sehr viel Neues: Neben den hinlänglich bekannten Standardmaßnahmen werden einige sinnvolle weitere Schutzmöglichkeiten wie z. B. der Einsatz von Software Restriction Policies aufgezeigt.

1.6 Fluggastdaten in die USA

Am 17.05.2004 hat die EU-Kommission entgegen den Protesten von Datenschützern und dem Europäischen Parlament der vom US-Kongress zum Schutz vor Terroristen geforderten Übermittlung von Flugpassagierdaten an die USA zugestimmt, die bereits seit Monaten praktiziert wird. 34 Datenfelder je Passagier dürfen nun 3,5 Jahre von den zuständigen US-Behörden gespeichert werden – nach Ansicht der Kritiker ein eklatanter Verstoß gegen die EG-Datenschutzrichtlinie.

1.7 PC/SC Draft 2.0

Totgesagte leben länger: Die 1997 mit der Vision eines vereinheitlichten und Plattform-unabhängigen Standards für Smart-Cards, Lesegeräte und Anwendungen angetretene PC-SC-Workgroup veröffentlichte schon im Dezember 1997 die erste Spezifikation PC/SC v1.0. Seitdem war es ruhig um diesen wichtigen Standard. Anfang Juni 2004 wurde nun Version 2.0 der Spezifikation zum „public review“ frei gegeben.

1.8 WLAN-Router-Attacken

Viele der mittlerweile weit verbreiteten DSL- und WLAN-Router werden ohne weiter gehende Sicherheitseinstellungen betrieben. Den Benutzern ist dabei offenbar nicht klar, dass sie so ein „Bürgerfunknetz“ betreiben, das ohne ihr Wissen auch von Dritten verwendet und für Angriffe missbraucht werden kann. Treten im ersten Fall „nur“ zusätzliche Verbindungskosten auf, ist der zweite wesentlich schwerwiegender. Denn kann ein Unternehmen als Quelle eines Angriffs mit Hilfe seines Providers einen ungeschützten DSL-Zugang identifizieren, wird sich der Geschädigte mit Klagen und Schadensersatzforderungen zunächst an den Betreiber des Anschlusses wenden.

Doch auch vermeintlich sicher konfigurierte Systeme können anfällig sein: Der Router WG602v1 des Herstellers Netgear enthielt eine undokumentierte Hintertür in Form eines fest programmierten Administratorzugangs. Die Schwachstelle wurde am 04.06.2004 durch ein Update der Firmware behoben. Nur wenige Tage später, am 18.06.2004, wurde allerdings eine weitere Zugangsmöglichkeit über das Netzwerk-Management-Protokoll SNMP bekannt, über die die Konfiguration verändert und das System unbrauchbar gemacht werden können. Das Einspielen der aktuellen Firmware wird daher dringend empfohlen.

1.9 Home Made Router-Security

Da die Firmware zahlreicher Router und anderer Netzwerkgeräte auf Programmcode basiert, der unter der GNU General Public License (GPL) entwickelt wurde, haben sich einige Hersteller inzwischen dazu durchgerungen, Teile Ihres Quellcodes oder zumindest Bibliotheken zur Verlinkung mit eigener Software ebenfalls zu publizieren. Wer über das entsprechende technische Know-How verfügt, kann damit das Betriebssystem seines Routers anpassen und weitere, durch die Hardware unterstützte Sicherheitsfunktionen wie etwa virtuelle LANs implementieren.

So werden beispielsweise für das Modell WRT54G des Herstellers Linksys der Quellcode und zusätzliche kommerzielle und selbst entwickelte Firmware-Versionen

angeboten sowie offene Firmware-Versionen in Projekten wie OpenWRT weiterentwickelt.

1.10 SQL-Injection in Oracle E-Business Suite

Die Oracle E-Business Suite 11i ist, wie am 03.06.2004 gemeldet wurde, für einen Angriff durch SQL-Injection verletzlich. Ebenso betroffen ist Oracle Apps in allen 11er Versionen. Einem versierten Angreifer kann es so gelingen, mit seinem Browser in den Eingabefeldern SQL-Befehle absetzen, die direkt vom Applikationsserver an die Datenbank übertragen und ausgeführt werden. Zur Abhilfe werden ein Update und der Einsatz von Filterungstechniken auf Applikationsebene empfohlen.

2 Secorvo News

2.1 Secorvo College aktuell

Nach der Sommerpause in den Monaten Juli und August, die in diesem Jahr wieder zu zahlreichen internationalen Security-Events an attraktiven Urlaubsorten lädt – darunter Turku, Las Vegas, San Diego, Toulouse, Sophia Antipolis und Klagenfurt – startet das College-Programm des zweiten Halbjahrs 2004 im September mit Seminaren zu Lotus Notes Security und Public Key Infrastrukturen.

http://www.secorvo.de/college

2.2 Nexus erhält ISIS-MTT-Konformitätssiegel

Am 27.05.2004 hat der Certificate Manager 5.3 von Nexus nach Prüfung durch das Secorvo Prüflabor vom ISIS-MTT-Board das ISIS-MTT-Konformitätssiegel als CA-Server erhalten. Damit liegt nunmehr das vierte Produkt vor, dessen ISIS-MTT-Konformität in einem vereinheitlichten Testverfahren nachgewiesen wurde. Weitere Produkte werden derzeit auf ISIS-MTT-Konformität untersucht.

3 Veranstaltungshinweise

Juni 2004	
29.-30.06.	Security Awareness Symposium 2004 (Secorvo, Karlsruhe)
Juli 2004	
12.-13.07.	Foundations of Computer Security FCS'04 (Turku)
24.-29.07.	Black Hat Briefings (Black Hat, Las Vegas)
August 2004	
09.-13.08.	USENIX Security Symposium (USENIX, San Diego)
23.-26.08.	19th IFIP International Information Security Conference (Toulouse)
September 2004	
15.-17.09.	7th International Symposium on Recent Advances in Intrusion Detection – RAID (Sophia Antipolis)
20.-21.09.	Elektronische Geschäftsprozesse – EGP 2004 (Klagenfurt)
21.-22.09.	Lotus Notes Security (Secorvo College, Karlsruhe)
28.-29.09.	Public Key Infrastrukturen (PKI) (Secorvo College, Karlsruhe)
28.-30.09.	ISSE 2004 (EEMA/TeleTrusT, Berlin)

Aktuelle Veranstaltungsübersicht zu Datenschutz und Datensicherheit:
http://www.veranstaltungen-it-sicherheit.de

Impressum

ISSN 1613-4311

Herausgeber (V.i.S.d.P.): Dirk Fox
Secorvo Security Consulting GmbH
Albert-Nestler-Straße 9
D-76131 Karlsruhe
Tel. +49 721 6105-500
Fax +49 721 6105-455

Die Zusendung des Inhaltsverzeichnisses können Sie per E-Mail anfordern:
security-news@secorvo.de
(Subject: „subscribe security news")

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