Secorvo Security News
Mai 2003

Dirk Fox, Stefan Gora, Stefan Kelm,
Hans-Joachim Knobloch, Dörte Neundorf

Secorvo Security Consulting GmbH

Nr. 5, 2. Jhrg. 2003
Stand 28. Mai 2003

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

Inhalt

Editorial: Entsorgung von E-Müll

Viele, vielleicht die meisten der aktuellen Probleme in der IT-Sicherheit sind „uralt“: Neben Buffer Overflows und Computerviren beschäftigen uns auch Werbe-E-Mails – neudeutsch „Spam“ – seit Jahren. Zahlreiche Anbieter durchforsten heute Webseiten und Newsgroups automatisiert nach E-Mail-Adressen und nutzen diese Millionen-Verteiler für elektronische Postwurfsendungen. Inzwischen hat Spam für viele Nutzer die Grenze einer erträglichen Belästigung überschritten. Für Endbenutzer und Administratoren ist dieser tägliche E-Müll zur zeit- und ressourcenintensiven Belastung geworden. Provider versuchen Spam einzuschränken; auch gibt es für gängige Mail-Programme Filter, mit denen E-Mails auf „verdächtige“ Textstücke untersucht werden können.

Dank der Findigkeit der Werber haben diese Maßnahmen aber nur mäßigen Erfolg. Daher befassen sich mittlerweile weltweit Gesetzgebung und Rechtsprechung mit dem Phänomen. Jüngst zogen in Florida gar E-Mail-Vermarkter gegen Anti-Spam-Organisationen vor Gericht. Einige Länder bereiten Gesetze vor, nach denen das unerwünschte Versenden von Werbe-E-Mails unter Strafe gestellt werden soll. Auch der am 06.05.2003 vom Kabinett vorgelegte Entwurf für ein neues Gesetzes gegen den unlauteren Wettbewerb (UWG) definiert „Werbung mit elektronischen Nachrichten, bei der die Identität des Absenders ... verheimlicht wird“ als „unzumutbare Belästigung“ – ignoriert aber die Tatsache, dass solche E-Mails meist aus dem Ausland kommen und das UWG somit nicht greift.

Auch auf Tagungen wird das Thema intensiv diskutiert, so jüngst auf einer „Spam Conference“ des MIT, der DuD-Konferenz (05.-06.05.2003) sowie dem Anti-Spam-Kongress des eco-Forums (21.05.2003) Von einer Lösung des Problems, das zeigen die Diskussionen, sind wir allerdings noch weit entfernt. Daher ist eine weitere Zunahme von Spam zu befürchten.

1 Security News

1.1 Signaturalgorithmen für Europa

Bereits seit Dezember 1998 werden im Rahmen der europäischen Standardisierungsinitiative EESSI Standards entwickelt, die die Umsetzung und Implementierung der EU-Direktive zu elektronischen Signaturen aus dem Jahr 1999 fördern sollen. Zu den inzwischen verabschiedeten Dokumenten zählen beispielsweise Zertifikatsprofile, Richtlinien für Zertifizierungsinstanzen und Anforderungen an sichere Signaturerstellungseinheiten.

Mit dem „ETSI Special Report“ (ETSI SR 002 176 V1.1.1), an dessen Entstehung auch Secorvo aktiv beteiligt war, wurde am 27.03.2003 nun auch die überfällige Spezifikation der „Algorithms and Parameters for Secure Electronic Signatures“ verabschiedet. Inhaltlich ist das Dokument der Publikation der „Geeigneten Kryptoalgorithmen“ durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vergleichbar, die einmal jährlich gemäß Signaturgesetz die für die kommenden sechs Jahre als geeignet anzusehenden Kryptoalgorithmen und Parameter „amtlich“ festlegt.

1.2 PKI Challenge legt Abschlussbericht vor

Noch immer ist die Interoperabilität eine der größten Herausforderungen bei Aufbau und Betrieb von Public Key-Infrastrukturen. Diesem Umstand trug die „PKI Challenge“ Rechnung, ein von der Europäischen Kommission und der Schweizer Regierung gefördertes Projekt, das im Januar 2001 unter der Führung der EEMA (European Forum for Electronic Business) initiiert wurde.

Ein Konsortium aus 13 Herstellern, Dienstanbietern, Forschungseinrichtungen und Beratungsunternehmen entwickelte eine Infrastruktur zur Untersuchung technischer Interoperabilitätsaspekte der Public Key-Zertifizierung. Darin wurden zahlreiche Produkte gegen eine Referenz-Implementation getestet, auf die man sich zuvor geeinigt hatte. Der Testplan umfasste auch die Cross-Zertifizierung von CAs sowie die Verifikation von Zertifikaten durch Endbenutzeranwendungen.

Der Abschlussbericht der PKI Challenge wurde am 29.04.2003 vorgelegt. Er enthält insbesondere technische Spezifikationen, die Beschreibung der durchgeführten Tests, der aufgetretenen Probleme sowie eine Reihe nützlicher Empfehlungen für den Aufbau von PKIs.

1.3 Signaturbündnis Niedersachsen

Das am 05.05.2003 veröffentlichte, vom Land Niedersachsen mit elf Unternehmen geschlossene „Bündnis für schnelle eSignatur-Lösungen Niedersachsen“ hat sich als Ziel gesetzt, flankierend zum Signaturbündnis der Bundesregierung bereits existierende Lösungen in Industrie und Verwaltung miteinander zu verknüpfen. Partner sind Cisco Systems, Deutsche Telekom, Microsoft Deutschland, BHW Bausparkasse, Empolis, Fujitsu-Siemens Computers, NordLB, Solvay, Volkswagen, die niedersächsischen Industrie- und Handelskammern und Sparkassen.

Mit der Initiative soll vor allem die private Nutzerakzeptanz gefördert werden. So können z. B. die mehr als 20.000 Mitarbeiterausweise der Volkswagen AG mit Signierfunktion zukünftig für elektronische Behördengänge genutzt werden.

1.4 ISIS-MTT-Compliance Criteria fertiggestellt

Die ISIS-MTT-Compliance-Criteria wurden am 26.05.2003 verabschiedet und am 27.05.2003 unter www.isis-mtt.org zum Download bereitgestellt. In diesem Dokument wird festgelegt, welche Kriterien ein Produkt erfüllen muss, um das Siegel „ISIS-MTT-konform“ und das entsprechende Logo führen zu dürfen.

Ziel der Siegelvergabe ist es, Anwendern schnell interoperable und damit einfach miteinander zu verwende Signatur- und Sicherheitsanwendungen zur Verfügung zu stellen.

Zum Erhalt des Siegels legen Hersteller oder Trustcenter-Betreiber in einem „Component Conformance Statement“ (CCS) fest, welchen Ausschnitt der ISIS-MTT-Spezifikation das Produkt erfüllt. Orientierung geben die in den Compliance Criteria festgelegten Produktklassen CA Server, OCSP Server, LDAP Server, VPN Server, Email-Client, SSL-Client, VPN-Client, Document-Signing Client, PKCS#11 Library, CSP und SigG conformant CSP. Zu den gewählten Funktionen ist ein Testbericht vorzulegen, der die mit Hilfe des von Secorvo entwickelten ISIS-MTT-Testbeds durchzuführenden Konformitäts-Tests belegt und dokumentiert.

Nach Prüfung des Berichtes durch ein zugelassenes Prüflabor (derzeit nur Secorvo) vergibt das ISIS-MTT-Board das Konformitätssiegel. Mit ersten Anträgen von interessierten Herstellern und Trustcenter-Betreibern wird in den kommenden Wochen gerechnet.

1.5 MS Windows Server 2003 Security Guide

Für Windows 2003 Server veröffentlichte Microsoft am 24.04.2003 einen „Security Guide“. In dem umfangreichen englischsprachigen Dokument werden zahlreiche ausführliche Hinweise zu Sicherungsmaßnahmen und dem Hardening von Systemen in Abhängigkeit vom Einsatzzweck (z. B. Domaincontroller, Fileserver etc.) gegeben. Sinnvolle Einstellungen werden vorgeschlagen und erläutert. Vervollständigt wird der Ratgeber durch Hilfsmittel wie Checklisten, Sicherheitsvorlagen und Skripte.

1.6 MS Patchmanagement

Das Tool HFNetChk des Herstellers Shavlik Technologies ermöglicht auf Microsoft-Betriebssystemen sowohl lokal als auch über das Netzwerk die Überprüfung des Patch-Levels. Die kürzlich freigegebene Version 4.0 erlaubt die Untersuchung einer Liste von Systemen (IP-Adressen) mit den Produkten Windows NT/2000/XP, IIS, MS-SQL Server, MS-Exchange Server, IE und MS-Office. Eine Funktion zum zentralen Download und dem Verteilen von Updates ist ebenfalls integriert.

Auf der HFNetChk-Engine basieren der Microsoft Baseline Security Analyzer (MBSA) und der Systems Management Server (SMS). Die kostenfreie Version von HFNetChkLT 4.0 kann bis zu 50 Systeme verwalten.

1.7 Aktuelle Security Advisories von Cisco

Nicht nur bei Microsoft werden mit schöner Regelmäßigkeit immer wieder neue Sicherheitslücken entdeckt – auch Netzwerkkomponenten, die ihr Dasein aus Sicht der meisten Anwender eher im Verborgenen fristen, sind davon betroffen und müssen ebenso wie Arbeitsplätze und Server in ein Patchmanagement einbezogen werden.

So veröffentliche Cisco am 08.05.2003 Advisories und Updates u. a. zu einem Buffer Overflow in der Administrationsoberfläche des ACS Authentifikationsservers und zu verschiedenen Schwächen im VPN 3000 Concentrator, die es im schlimmsten Fall erlauben, Firewalls per VPN-Gateway zu umgehen.

1.8 Security Tools: “Top 75”

Als Ergebnis einer Umfrage in der Newsgroup des Nmap Netzwerk-Scanners wurde eine Liste der 75 beliebtesten Sicherheits-Tools publiziert. Darin werden die Tools mit Bezugsquelle vorgestellt und bewertet. Diese Security Tools ermöglichen Administratoren, die Sicherheit ihrer Systeme und Netzwerke zu überprüfen – erleichtern allerdings auch die Durchführung von Angriffen.

2 Secorvo News

2.1 Secorvo College aktuell

Erstmalig führte Secorvo College vom 12. bis 16.05.2003 ein fünftägiges Seminar zum Information Security Management von A(udit) bis Z(ertifizierung) durch. Die positiven Rückmeldungen ermutigen uns, das Seminar erneut anzubieten – das nächste Mal in der Woche vom 22.-26.09.2003.

Vor der Sommerpause gibt es noch Gelegenheit zum Besuch zweier Seminare:

- Defense Lab – Life Hacking, Angriffstechniken und Gegenmaßnahmen, **17.-18.06.2003**
- IT-Sicherheit heute – Angriffe, Konzepte, Lösungen, **24.-26.06.2003**

2.2 Secorvo erstes ISIS-MTT-Prüflabor

Im Secorvo Security Labor werden seit 1999 IT-Sicherheitsprodukte im Kundenauftrag auf Funktionalität, Interoperabilität und Sicherheit geprüft. Vor der Beschaffung, Implementierung und Konfiguration komplexer Sicherheitslösungen werden zudem Integrationstests für Kundeninstallationen durchgeführt. Dafür stehen mehr als 300 Testinstallationen führender Sicherheitsprodukte (PKI, E-Mail, VPN, Firewall, Virenscanner etc.) bereit. Eine hohe Systematik bei der Testdurchführung und Dokumentation, sowie eine strikte Trennung der zu testenden Produkte durch Image-Dateien machen die Prüfergebnisse zudem reproduzierbar und übertragbar.

Am 14.05.2003 erhielt Secorvo vom ISIS-MTT-Board als erstes (und bisher einziges) Unternehmen die Zulassung als Prüflabor. Secorvo ist damit berechtigt, Konformitätstests für Hersteller von IT-Sicherheitssoftware und Betreiber von Trustcentern durchzuführen, auf deren Basis das ISIS-MTT-Board dann das ISIS-MTT-Konformitätssiegel vergibt.

2.3 Manche mögen's heiß

Nach einer spannenden Zeitreise durch die Geschichte der IT-Sicherheit (15.05.2003) lädt die Karlsruher IT-Sicherheitsinitiative, der die LuK GmbH & Co. oHG am 12.05. 2003 als neuer Partner beigetreten ist, zum nächsten Event: Am **03.07.2003** (18 Uhr) wird Oliver Stoll, Technical Director der WEB.DE AG, aus der Praxis des IT-Sicherheitsmanagements berichten – mit anschließendem Networking-Dinner am spanischen Buffet (u.A.w.g.).

3 Veranstaltungshinweise

Juni 2003	
17.-18.06.	Defense Lab (Secorvo College, Karlsruhe)
24.-25.06.	Security Awareness Symposium 2003 (Secorvo, Karlsruhe)
24.-26.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juli 2003	
03.07.	Manche mögen's heiß! (KA-IT-Si, Karlsruhe)
09.-10.07.	Einführung in die Praxis des betrieblichen DSB (Euroforum, Ffm)

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

Impressum

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

Der Bezug der Secorvo Security News ist kostenlos. Eine Zusendung des Inhaltsverzeichnisses können Sie mit einer E-Mail (Subject: „Subscribe Security News") an security-news@secorvo.de anfordern.

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