Secorvo Security News
April 2005

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

Nr. 4, 4. Jhrg. 2005
Stand 25. April 2005

ISSN 1613-4311

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

Inhalt

Editorial: Verschwörung!

1 Security News

1.1 Datenschutz: Toll Collect

1.2 Hacken mit Google

1.3 MS Windows 2003 SP 1

1.4 Immer wieder: DNS-Gift

1.5 Un-Sicherheitsfeature

1.6 Wegmarke bei ISIS-MTT

1.7 WinZIP-Verschlüsselung

2 Secorvo News

2.1 Secorvo College aktuell

2.2 Security Awareness Symposium 2005

3 Veranstaltungshinweise

Impressum

Editorial: Verschwörung!

Die Geschichte ist schnell erzählt: Für einen großen Kongress eines Sicherheits-Bundesamtes wird ein für kritische Kommentare bekannter Informatik-Professor um einen Vortrag über biometrische Sicherheitssysteme gebeten. Der Text ist geliefert, das Programm gedruckt – da kommt die Ausladung durch den Präsidenten, begründet mit „neuen Entwicklungen“. Der Brüskierte wendet sich an die Presse.

Zunächst nur ein Vorgang grober Unhöflichkeit unter Beamten. Aber: Der Beirat des Kongresses erfährt von der Ausladung aus der Zeitung, weiß nichts von „neuen Entwicklungen“, die im Programm unterzubringen sind. Ein Schelm, wer Arges dabei denkt: Fiebert doch der Innenminister bekanntlich nach biometrischen Merkmalen im Ausweis. Sollte da auf Veranlassung von oben ein Kritiker mundtot gemacht werden? „Zensur“, schreien die Kritiker. „Zu kurz gedacht“, erwidern Besonnene: Es sei doch dumm, Kritik und Professor medial so aufzuwerten. War es dann ein schwacher Moment des Präsidenten, der Versuch, in voraus eilendem Gehorsam befürchteten Minister-Groll abzuwenden? Nein, zu billig.

Dahinter steckt mehr. Schließlich war der Vortrag perfekt platziert: Um 9 Uhr am Morgen nach dem intensiv besuchten Empfang des ersten Kongressabends – nur Unverdrossene hätten die Reihen gefüllt. Da drängt sich eine andere Erklärung auf: Der Präsident, im Herzen Biometrie-Verächter, wollte der Kritik eine größere Bühne geben, sich selbst aber aus der ministeriellen Schusslinie halten. Jedoch: Auch dieser Verdacht hinkt. Die Kritik des Kritikers ist dünn, knapp (fünf Seiten) und akademisch, keine Bedrohung für den neuen Personalausweis. Versuchte der Präsident also, die Biometriekritik durch öffentliche Aufwertung magerer Argumente zu schwächen? Ist der Kritiker gar Agent der Biometrie-Industrie?

Tatsächlich diente die Farce ganz anderen Zwecken: Sie lenkte ab vom aufkeimenden Verschwörungsverdacht zur Rolle der NSA beim SHA-1-Design! (Warum bloß ist der SHA-1 nun Thema des Ersatzvortrags ...?)

1 Security News

1.1 Datenschutz: Toll Collect

Am 19.04.2005 hat Peter Schaar, der Bundesdatenschutzbeauftragte (BfD) den 20. Tätigkeitsbericht für die Jahre 2002-2004 vorgelegt. Darin äußert er sich unter anderem ausführlich zur Umsetzung des Datenschutzes im LKW-Mautsystem Toll Collect.

Dieses von der Toll Collect GmbH im Auftrag des Bundes nach dem Autobahnmautgesetz (ABMG) errichtete und seit Januar 2005 störungsfrei betriebene Mautsystem unterliegt strengen Datenschutzanforderungen. So dürfen beispielsweise von den ca. 300 Autobahn-Mautbrücken ausschließlich mautpflichtige Fahrzeuge erfasst werden; Fotos und Kennzeichen von PKW sind sofort zu löschen. Denn das ABMG berechtigt Toll Collect nur zur Nutzung von Daten, die für die Mauterhebung erforderlich sind. Die Erfassung von Daten, mit denen sich beispielsweise Bewegungsprofile erstellen oder Fahrzeuge von Straftätern verfolgen ließen, ist nicht erlaubt. Das Gesetz lässt daran keinen Zweifel: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig“ (§§ 4 Abs. 2, 7 Abs. 2 ABMG).

Um diese datenschutzrechtlichen Anforderungen in dem hoch komplexen Mautsystem umzusetzen, das täglich durchschnittlich 700.000 mautpflichtige LKW erfasst und kontrolliert, wurden zahlreiche Löschfunktionen für nicht erforderliche oder nicht mehr benötigte Fahrzeugdaten implementiert. An der Konzeption, Umsetzung und Kontrolle dieser Datenschutzmechanismen war Secorvo maßgeblich beteiligt.

Der BfD kommentiert das Ergebnis seiner Überprüfung des Datenschutzes bei Toll Collect in seinem Tätigkeitsbericht abschließend wie folgt: „Ich habe mich davon überzeugt, dass die Grundlagen für eine Umsetzung der datenschutzrechtlichen Anforderungen des Gesetzes in den Funktionalitäten des Systems auch geschaffen wurden.“ (S. 181). Wie sagt der Schwabe: „Ned gschumpfe isch gnug globd.“

1.2 Hacken mit Google

Bereits in den späten 1980er-Jahren diskutierten Sicherheitsexperten, dass damals aktuelle Suchmaschinen wie Gopher oder FTPsearch auch von Angreifern zur Recherche sensitiver Informationen – beispielsweise Passwortdateien – missbraucht werden könnten. Obwohl heutige Suchmaschinen wie Google ungleich mächtiger sind als ihre virtuellen Vorfahren, wurde diese Gefahr lange nicht untersucht.

Inzwischen betreibt der Sicherheitsexperte Johnny Long seit einiger Zeit eine viel beachtete Webseite, auf der Hunderte von Beispielen dafür zu finden sind, wie Google zum Suchen und Finden von z.B. Passwortdateien, versteckten Verzeichnissen, Logdateien, Software- und Betriebssystem-Schwachstellen, Login-Portalen, Datenbanken, Kreditkarteninformationen, oder Netzwerkdruckern, teilweise sogar automatisiert eingesetzt werden kann. In einem White Paper beschreibt Long die wichtigsten Beispiele und effektive Gegenmaßnahmen. Weiter geht sein soeben erschienenes Buch „Google Hacking for Penetration Testers“, das in keiner Bibliothek fehlen sollte.

1.3 MS Windows 2003 SP 1

Der am 30.03.2005 von Microsoft veröffentlichte Service Pack 1 (SP1) für Windows 2003 Server integriert alle sicherheitsrelevanten Patches der Jahre 2003-2005 bis einschließlich MS05-015. Darunter finden sich der Security Configuration Wizard (SCW) für eine vereinheitlichte und prozessorientierte Sicherheitsadministration, die Post-Setup Security Updates (PSSU) zur Blockade von Netzwerkverkehr bei einer Erstinstallation (schützt bis zur Patcheinspielung), die Windows Firewall (WF), die für jedes Interface über Group Policies administrierbar ist und die Data Execution Prevention (DEP) zum Schutz vor Speicherüberläufen.

Des weiteren wurden die Standard-Sicherheitseinstellungen restriktiver vordefiniert; damit sind Windows Server zukünftig hoffentlich auch sicherer konfiguriert.

1.4 Immer wieder: DNS-Gift

Seit dem 03.03.2005 gingen beim SANS-Institut zahlreiche Berichte über erfolgreiche „Cache Poisoning"-Angriffe auf diverse DNS-Server ein. Wieder hatten Angreifer die schon auf der USENIX 1995 publizierte DNS-Schwachstelle ausgenutzt. Neu war indes die Art der Angriffe: Gezielt wurden bekannte Lücken verschiedener Anwendungen genutzt: Zunächst wurden anfälligen DNS-Servern unter Windows NT4 bzw. 2000 sowie Gateways von Symantec gefälschte DNS-Einträge (Zuordnung von Hostnamen zu IP-Adressen) „untergejubelt". Anschließend wurden für bestimmte Hostnamen die IP-Adressen von Webservern geliefert, die dann über Schwachstellen des Internet Explorer versuchten, Spyware zu installieren. Vom SANS existiert eine detaillierte Analyse (deutsche Fassung), die auch Gegenmaßnahmen für Betroffene beschreibt.

Dieser Angriff zeigt nicht nur, dass unzureichendes Patch-Management immer wieder die Ausnutzung lange bekannter Schwachstellen ermöglicht. Sondern er lässt auch die Rufe nach DNSSEC wieder lauter werden. Mehrere Studien, u.a. von Secorvo und vom BSI, beschäftigten sich in den vergangenen Jahren mit der globalen Einführung von DNSSEC, rieten aber aus organisatorischen und technischen Gründen zur Zurückhaltung. Einige der identifizierten Mängel wurden jüngst in aktuellen RFCs korrigiert – mittelfristig führt sicherlich kein Weg an DNSSEC vorbei.

1.5 Un-Sicherheitsfeature

Ein am 01.04.2005 online veröffentlichter (und ernst gemeinter) Beitrag in der Zeitschrift c't ruft in Erinnerung, dass Zugriffsschutz und Denial-of-Service zwei Seiten einer Medaille sein können. So unterstützen viele Festplatten die im ATA-Standard vorgesehene Möglichkeit, den Zugriff auf die gespeicherten Daten durch ein Passwort in der Firmware des Laufwerks zu sperren. Dieses Passwort soll automatisch vom BIOS des Rechners, in dem die Festplatte eingebaut ist, gesetzt und verwendet werden. Weil jedoch viele BIOS-Hersteller das ATA-Passwort nicht unterstützen, wird nicht nur der mögliche Schutzeffekt nicht erzielt, sondern Trojanern & Co. die Möglichkeit gegeben, die Festplatte durch den Eintrag eines eigenen Passworts nahezu irreversibel zu sperren. So gesehen ist es ein Pluspunkt, dass der Schutz durch das ATA-Passwort nicht unüberwindbar ist...

Hersteller sollten daraus lernen, Anwendern konfigurierbare Sicherheitsfunktionen nur zugänglich zu machen, wenn diese bekannt und einfach konfigurierbar sind – sonst droht Missbrauch durch Angreifer.

1.6 Wegmarke bei ISIS-MTT

Am 14.04.2005 wurde im Rahmen einer Präsentation beim Bundeswirtschaftsministerium (BMWA) das im Jahr 2001 als „Public-Private-Partnership" gestartete Projekt ISIS-MTT in die „Obhut" der Wirtschaft übergeben.

Das mit einem Auftrag des BMWA an TeleTrusT e.V. in Kooperation mit T7 e.V. im Jahr 2001 gestartete Projekt zielte auf eine bessere Interoperabilität von PKI-Anwendungen. Seitdem wurden – unter Mitwirkung von Secorvo – die ISIS-MTT-Spezifikation weiter entwickelt, ein Testbed auf Open-Source-Basis konzipiert und realisiert sowie für inzwischen sechs Produkte ISIS-MTT Siegel vergeben, deren Standard-Konformität vom anerkannten ISIS-MTT-Prüflabor bei Secorvo bestätigt wurde.

1.7 WinZIP-Verschlüsselung

Immer wieder wird die im Kompressionsprogramm WinZIP integrierte Verschlüsselungsfunktion als Alternative zu einem Dateiverschlüsselungsprogramm eingesetzt. Früher war das riskant: Der PKZIP-kompatible Verschlüsselungsalgorithmus war 1994 von Biham und Kocher, 2001 mit einem verbesserten Verfahren von Stay erfolgreich attackiert worden.

Mit der Anfang 2004 publizierten Version 9 wurde die Verschlüsselung auf AES umgestellt (128 bzw. 256 bit Schlüssellänge) und HMAC-SHA-1 zur Integritätssicherung eingeführt. Seither gilt die Verschlüsselung als

kryptographisch stark. Dennoch ist Vorsicht geboten, wie Tadayoshi Kohno in einer Analyse vom 08.05.2004 zeigt: Er identifizierte zahlreiche Sicherheitsmängel der Implementierung (unverschlüsselte Dateiinformationen, Mischung verschlüsselter und offener Dateien, fehlerhafte Ableitung des AES-Keys von der Passphrase), die spezielle Angriffe ermöglichen.

2 Secorvo News

2.1 Secorvo College aktuell

Speziell für Administratoren haben wir zwei neue Seminare entwickelt, die sich dem Thema „Sichere IT-Administration“ widmen. Im Wechsel von Theorie, Workshop und Übung werden technische Anleitungen zur sicheren IT-Administration gegeben:

IT-Sicherheit für Admins (Windows) am **07.-08.06.2005**

IT-Sicherheit für Admins (Unix) am **09.-10.06.2005**

http://www.secorvo.de/college

2.2 Security Awareness Symposium 2005

Zum dritten Mal veranstaltet Secorvo am **21. und 22.06.2005** das “Security Awareness Symposium”. Es hat sich in den vergangenen Jahren zur Plattform für den Erfahrungsaustausch entwickelt. Security-Awareness-Aktivitäten leben von guten Ideen – und damit auch von einem aktiven Ideenaustausch. An den Symposien 2003 und 2004 wirkten u.a. BMW, die Münchener Rück, SAP, RWE Systems, Finanz-IT, die schweizerische Armee, BASF und T-Systems mit Erfahrungsberichten mit. Auch in diesem Jahr werden wieder mehrere deutsche Unternehmen mit einem Erfahrungsbericht vertreten sein; das Programm ist derzeit in Abstimmung. Das vorläufige Programm und ein Anmeldeformular finden Sie unter

http://www.security-awareness-symposium.de

3 Veranstaltungshinweise

April 2005	
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
10.-11.05.	Datenschutzkongress 2005 (Euroforum, München)
10.-12.05.	IT-Sicherheitskongress 2005 (BSI, Bonn)
22.-26.05.	Eurocrypt 2005 (IACR, Aarhus/DK)
23.-25.05.	Spurensuche im Web (Secorvo College, Karlsruhe)
31.05. -02.06.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
Juni 2005	
01.-02.06.	Einführung in die Praxis des DSB (Euroforum, Wiesbaden)
06.-07.06.	IT-Risk Management 2005 (COMPUTAS, Karlsruhe)
13.- 14./17.06.	Information Security Management (Secorvo College, Karlsruhe)
21.-22.06.	Security Awareness Symposium (Secorvo, Karlsruhe)

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
Ettlinger Straße 12-14
D-76137 Karlsruhe
Tel. +49 721 255 171-0
Fax +49 721 255 171-100

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