Secorvo Security News
März 2005

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

Nr. 3, 4. Jhrg. 2005
Stand 29. März 2005

ISSN 1613-4311

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

Inhalt

Editorial:
Vom Suchen und vom Finden

Nicht erst seit der Proklamation des „lebenslangen Lernens" wissen wir: Die Halbwertzeit unserer Kenntnisse ist oft überraschend kurz. Erst recht im Gebiet IT-Sicherheit müssen wir immer wieder feststellen, dass manch mühsam erworbene und lieb gewonnene Erkenntnis durch neue Entwicklungen Makulatur wird. Nicht nur Hashfunktionen, Verschlüsselungsverfahren und kryptoanalytische Erkenntnisse jagen einander, auch neue Technologien halten uns in Atem – und die Security-Ticker in Bewegung. Da bleibt wenig Anderes, als mit der Entwicklung zu gehen, denn Stagnation in Sicherheitsfragen kann schwer wiegende Folgen haben.

Wie aber bleibt man „auf dem Laufenden"? Unter den Bedingungen knapper Zeitressourcen helfen allein aktuelle, konzentrierte, verständliche und fundierte Informationsmaterialien. Nur: Wo findet man die?

Meist geht inzwischen der Griff zur Tastatur statt zum Buch. Das zeigt eine aktuelle Befragung von 400 DAX-30-Managern: Für 94% ist das Internet die wichtigste Informationsquelle, 84% verbringen eine bis vier Stunden wöchentlich mit der Informationsrecherche (imc, 2005).

Zwar gilt auch für das Internet das Bibelwort: *„... wer da suchet, der findet"* (Matthäus, 7. Kapitel, Vers 8). Nur findet er nicht unbedingt auch das Gesuchte. Denn eines verrät keine Suchmaschine: Ob ein gefundenes Dokument informativ, verständlich und fachlich fundiert ist. Diesem Mangel kann man nur mit viel Leseaufwand begegnen.

Auch wir mussten uns dieser Herausforderung stellen. So ist bei Secorvo ein Informationspool aus vielen hundert ausgewählten Dokumenten entstanden. Den Zugriff auf diese „virtuelle Bibliothek" ermöglichen wir nun unter http://www.security-finder.de/ – den Lesern der Security News bis zum 10. April 2005 unentgeltlich (Login: „SSN-01", Passwort: „security-finder"). Wir freuen uns auf Ihre Rückmeldungen.

1 Security News

1.1 Kollidierende Zertifikate

Für viel Wirbel hat am 01.03.2005 die Publikation eines Forscherteams gesorgt, dem es gelungen ist, zwei unterschiedliche X.509-Zertifikate zu erzeugen, die denselben MD5-Hashwert liefern. Obwohl die Existenz von MD5-Kollisionen schon seit geraumer Zeit bekannt ist, waren praktische Angriffe selten – bis jetzt: Lenstra, Wang und de Weger präsentierten zwei Beispielzertifikate mit unterschiedlichem Public Key aber demselben MD5-Hashwert.

Die praktischen Auswirkungen dieses Angriffs sind dennoch gering: Ein Angreifer müsste eine vertrauenswürdige Zertifizierungsinstanz (CA) dazu bringen, das vorbereitete Zertifikat zu signieren, ohne eine Änderung daran vorzunehmen. Jede „vernünftig“ arbeitende CA wird jedoch vor allem kritische Felder wie die Seriennummer und das Gültigkeitsdatum des Zertifikats selbst ausfüllen.

Weiter erlaubt das Verfahren nicht die Konstruktion einer Kollision zu einem bereits vorliegenden Zertifikat. Damit sind insbesondere bereits ausgestellte Zertifikate nicht auf diese Weise angreifbar. Schließlich müssen die Zertifikatsparameter eine Bitlänge besitzen, die ein ganzzahliges Vielfaches von 512 ist.

Aber vor allem: Welchen Nutzen hätte ein Angreifer von zwei Zertifikaten zu von ihm selbst konstruierten Public Keys? Schlimm wäre, wenn er Zertifikatsparameter ändern könnte, um z.B. den Public Key einer zweiten Identität zuzuordnen oder aus einem End-User- ein CA-Zertifikat zu machen – dies ermöglicht das Konstruktionsverfahren jedoch nicht.

Nach eigenen Aussagen versucht das Forscherteam jetzt, vergleichbare Zertifikate auf SHA-1-Basis zu finden. Doch obwohl SHA-1 stark „angekratzt“ ist, scheint dies deutlich aufwändiger zu sein. Wer allerdings noch immer MD5 einsetzt, ist nicht nur nicht sicher, sondern selbst Schuld.

1.2 Haftungsrisiken

Vom Bitkom ist am 10.03.2005 ein Leitfaden zum Thema Haftungsrisiken erschienen. Das Dokument stellt recht übersichtlich die wichtigsten rechtlichen Anforderungen zusammen und unterscheidet insbesondere nach strategischen, konzeptionellen und operativen Aufgaben. Für verschiedene Zielgruppen wie Geschäftsführung/-Vorstand und IT-Leitung/-Sicherheitsbeauftragte werden in einer Matrix die jeweiligen Pflichten und der Bedarf den Rechtsgrundlagen, potentiellen Schäden und Ansprüchen Dritter gegenüber gestellt. Der Leitfaden bietet einen guten Einstieg in das Thema und zeichnet sich durch klare Strukturierung und übersichtliche Darstellung aus.

1.3 NIST SP 800-53

Am 07.03.2005 wurde die NIST Special Publication 800-53 „Recommended Security Controls for Federal Information Systems“ veröffentlicht. Sie stellt in guter, sehr detaillierter und umfassender Form die möglichen Ausprägungen von Sicherheitsmaßnahmen dar, die im Rahmen der Sicherheitsarchitektur einer Organisation notwendig sind. NIST SP 800-53 korrespondiert dabei mit dem im Dezember 2003 publizierten Standard FIPS-199 „Standards for Security Categorization of Federal Information and Information Systems“.

Das 121 Seiten starke Dokument differenziert Maßnahmen in den drei Kategorien Management, Organisation/Betrieb sowie Technik mit insgesamt 17 Teilbereichen. Passend dazu gibt es drei Ergänzungsdokumente, in denen die Sicherheitsmaßnahmen für drei unterschiedliche Grundsicherheitsniveaus (low/moderate/high) zusammen gestellt werden. Es ist zu erwarten, dass diese in den USA zukünftig verstärkt zur Bewertung des erreichten Sicherheitsniveaus heran gezogen werden.

Für Ende 2005 ist der Standard FIPS-200 "Minimum Security Controls for Federal Information Systems" angekündigt, der die Empfehlungen der SP 800-53 für US-amerikanische Organisationen ablösen soll.

1.4 Microsoft im Fadenkreuz

Wie bereits am 09.02.2005 vom Antivirus-Hersteller Sophos gemeldet versucht der Trojaner Bankash.A neben seiner eigentlichen „Tätigkeit", Zugangskennungen zum Online-Banking auszukundschaften, auch die am 20.01.2005 erschienene Beta-Version des Windows AntiSpyware Tools von Microsoft zu deaktivieren.

Dies könnte ein erstes Indiz sein, dass sich bei Sicherheits-Software das fortsetzt, was bei Betriebssystemen gang und gäbe ist: Andere Lösungen sind vielleicht nicht viel sicherer als Microsofts (apropos: am 12.03.2005 erschien das erste Sicherheits-update zu Firefox 1.0, am 23.03.2005 schon das zweite), aber allein auf Grund ihrer Verbreitung stehen Microsoft-Produkte im Fadenkreuz der Hacker und werden häufiger und schneller angegriffen.

1.5 Kompass der IT-Sicherheitsstandards

Auch am 10.03.2005 wurde vom Bitkom ein Leitfaden für mittelständische Unternehmen mit dem Titel „Kompass der IT-Sicherheitsstandards" veröffentlicht. Das Dokument bietet einen gelungenen Überblick wichtiger Standards wie ISO 17799, BS 7799-2, IT-Grundschutz, Cobit, ITIL sowie weiterer für spezifischere Sicherheitsaspekte. Durch ein Klassifizierungsschema ist je nach Art des Unternehmens und der IT-Relevanz sehr übersichtlich dargestellt, welche Felder der jeweilige Standard abdeckt und für welche Personen und Rollen er angewendet werden kann.

1.6 Knack' den Knacker

Das Passwort Recovery Tool Cain&Abel ist wegen seines mächtigen Funktionsumfangs und der eingängigen Bedienoberfläche bei Penetrations-Testern und IT-Forensikern vermutlich ebenso beliebt wie bei Hackern jeglicher Couleur. Ironie des Schicksals: Am 18.03.2005 wurde bekannt, dass Cain&Abel bis Version 2.65 anfällig für einen Buffer-Overflow ist, wenn es beim Abhören eines VPN-Verbindungsaufbaus auf manipulierte IKE-Pakete stößt.

Nimmt man einmal an, dass viele Angreifer es mit dem Patch-Level ihrer Werkzeuge nicht anders halten als die meisten ihrer Opfer, könnte man vor diesem Hintergrund auf die Idee verfallen, präventiv „vergiftete" Pakete im eigenen Netz auszustreuen...

1.7 Data-Mining the NSA

Dem österreichischen Verein Quintessenz ist es nach eigenen Angaben aufgrund eines Konfigurationsfehlers gelungen, ein vollständiges Archiv der „Biometrics Consortium List" zur erlangen, welches ca. 60 MB Text sowie 2 GB an Fachdokumenten und Präsentationen enthält. Insgesamt haben 2.500 Personen bzw. Organisationen an der Mailingliste mitgewirkt.

Unter dem Aufmacher „Datamining the NSA – Part I" wird derzeit mit Hilfe von Werkzeugen des Data-Minings höchst aufschlussreich und sehr detailliert nachgewiesen, in welchem Ausmaß über die letzten zehn Jahre hinweg mit dieser Mailingliste von US-amerikanischen Organisationen versucht wurde, den Biometriebereich systematisch zu beeinflussen. Die Diagnose: Ziel war ein patentfreier, universaler Standard, der eine technologische Unabhängigkeit der USA von nicht-amerikanischen Patentgebern sicherstellt.

Laut Quintessenz ist die Auswertung bisher erst bis zum Jahre 1996 erfolgt; daher kann noch nicht beurteilt werden, inwieweit die Entwicklung biometrischer Technologien und der Einsatz in Deutschland und Europa in den letzten Jahren „Impulse" durch diese Mailingliste erfahren haben.

2 Secorvo New

2.1 Secorvo College aktuell

Zusammen mit dem Schweizer Spezialisten Compass Security – Gewinner des 24-Stunden-Hacker-Contest 2004 des Schweizer Fernsehens – bieten wir Ihnen im April und Mai in vier technisch aufwändigen

Labor-Schulungen einen vertieften Einblick in die wichtigsten aktuellen Angriffsmethoden auf IT-Systeme – live und unter Ihrer aktiven Beteiligung vorgestellt. In den vier Labor-Seminaren wechselt die Arbeit im Übungslabor mit Referatsblöcken, in denen die wesentlichen theoretischen Hintergründe und Schutzmethoden vermittelt werden:

- Live-Hacking Lab (**26.-28.04.**)
- Live-Hacking Spezial (**29.04.**)
- Web Application Security (**02.-04.05.**)
- Spurensuche im Web (**23.-25.05.**).

2.2 security-finder.de

Seit Mitte März 2005 bietet Secorvo einen neuen Service: Den Zugang zur über mehr als zehn Jahre gewachsenen Secorvo-eigenen Know-How-Datenbank mit vielen Hundert ausgesuchten Dokumenten zu Fragestellungen der Datensicherheit und des Datenschutzes. Getreu dem Anspruch der Security News, eine „Schneise in die Informationsflut“ zu schlagen, bietet der Security-Finder den Zugang zu nach Wichtigkeit und Aktualität ausgewählten Dokumenten – jeweils mit Kategorisierung, inhaltlicher Zusammenfassung und Bewertung.

„Finden statt suchen“: Statt mühsamen Durchforschens von Suchmaschinenergebnissen führt der Security-Finder strukturiert direkt zum passenden Dokument. Besonders wertvolle Funde können per Mausklick in die private Bibliothek übernommen werden, und regelmäßig wird per E-Mail über Neuzugänge informiert.

Der Preis für den Zugang zum Security-Finder orientiert sich am Modell einer Loseblattsammlung: Der Zugang zum „Grundwerk“ kostet einmalig 299 €, das Jahresabonnement 149 €. Bis zum 30.06.2005 kostet der Zugang nur 249 € (Grundwerk) und das Jahresabonnement 124 €. (Preise für Unternehmenszugänge auf Anfrage).

Leser der Security News erhalten bis zum 10.04.2005 freien Zugang unter der ID „SSN-01“ (Passwort: „security-finder“).

3 Veranstaltungshinweise

April 2005	
05.-08.04.	Sicherheit 2005 (GI, Uni Regensburg)
12.-13.04.	Lotus Notes Security (Secorvo College, Karlsruhe)
14.04.	Lotus Notes Security advanced (Secorvo College, Karlsruhe)
18.-19.04.	Datenschutz und Datensicherheit – DuD 2005 (COMPUTAS, Berlin)
19.-20.04.	Inside Windows Security (Secorvo College, Karlsruhe)
26.-28.04.	Live Hacking Lab (Secorvo College, Karlsruhe)
29.04.	Live Hacking Spezial (Secorvo College, Karlsruhe)
Mai 2005	
02.-04.05.	Web-Application Security (Secorvo College, Karlsruhe)
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)

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