secorvo
security consulting

Secorvo Security News

Juni 2010

Unqualifiziert qualifiziert

Damit eine elektronische Signatur als „qualifizierte“ gilt, muss sie bekanntlich etliche Voraussetzungen erfüllen. Eine davon ist, dass sie mit technischen Komponenten erstellt wurde, deren Sicherheit durch eine von der Bundesnetzagentur (BNetzA) anerkannte Stelle überprüft und bestätigt wurde.

Seit dem 19.12.2008 besitzt der Chipkartenleser „Kobil KAAN TriB@nk“ eine solche Bestätigung. Am 17.04.2010 veröffentlichte ein Unbekannter unter dem Pseudonym ‚Colibri’ eine Dokumentation, die zeigt, wie eine manipulierte Firmware in diesen Leser geladen werden kann. Damit ließen sich zumindest theoretisch nicht nur die PINs von Karteninhabern abfangen, sondern auch heimlich weitere Signaturen erzeugen.

Der Fehler: Der Leser validierte beim Update zwar die Signatur des Herstellers über die übertragenen Datenblöcke, prüfte jedoch nicht, ob die Blöcke auch in der richtigen Reihenfolge an der beabsichtigten Stelle im Speicher landen. Dass diese (inzwischen gepatchte) Lücke bei der Prüfung des Geräts übersehen wurde, zeigt, wie auch Prof. Dr. Rainer W. Gerling von der Max-Planck-Gesellschaft kommentierte, dass selbst eine standardisierte Zertifizierungsprüfung letztlich auf individuellem Geschick und Erfahrung des Prüfers basiert.

Am 07.06.2010 erklärte die BNetzA die Sicherheitsbestätigung des Geräts für ungültig – mit Wirkung zum Veröffentlichungstag des Angriffs. Damit schuf sie unvermeidlich zwei neue Klassen von elektronischen Signaturen (vgl. SSN 04/2009): Alle zwischen dem 17.04. und 07.06.2010 mit dem TriB@nk-Leser erstellten Signaturen wurden rückwirkend zu „dann doch nicht ganz so qualifizierten Signaturen“, alle zwischen dem 19.12.2008 und dem 17.04.2010 erstellten zu „qualifizierten, die möglicherweise gefälscht sein könnten“.

Bleibt ein profanes Problem: Woran erkennt man, sofern man möchte, bei der Prüfung einer Signatur, mit welchem Chipkartenleser sie erstellt wurde?

Inhalt

secorvo
security consulting

Security News

WLAN-Haftung

Anspruch auf Unterlassung, aber kein Schadensersatz – das ist das Ergebnis der mit Spannung erwarteten BGH-Entscheidung vom 12.05.2010 zur Haftung von Anschlussinhabern für von Dritten verübte Schädigungen über unbefugt genutzte WLANs.

Nach der seit dem 07.06.2010 vorliegenden Begründung treffen den Anschlussinhaber Prüfpflichten hinsichtlich der von ihm ergriffenen Sicherheitsmaßnahmen. So sind mindestens die zum Zeitpunkt des Routerkaufs marktüblichen Sicherungen zu ergreifen; ein kontinuierliches Aktualisieren der Maßnahmen sei allerdings nicht zumutbar.

In dem aus dem Jahr 2006 datierenden Fall erwartete der BGH eine aktivierte WPA-Verschlüsselung. Jedoch habe der Beklagte seine Sorgfaltspflicht verletzt, indem er für den Routerzugang kein eigenes, ausreichend langes Passwort vergeben, sondern es bei dem voreingestellten Passwort belassen habe – eine merkwürdige Einschätzung, sofern das Herstellerpasswort individuell und zufällig gewählt war.

Zur Klärung der bestehenden Rechtsunsicherheit wird diese Entscheidung wenig beitragen. Zu lückenhaft waren die weitgehend auf Annahmen und Unterstellungen beruhenden Sachverhaltsfeststellungen der Instanzgerichte; zu viele Fragen waren nicht Gegenstand der Revision. Offen bleibt bspw. die Anwendbarkeit der Deckelung der Abmahnkosten aus § 97a UrhG. Auch hätten dem Urteil Ausführungen zur Handhabung der Beweislastverteilung gut getan. Sowohl unschuldig Abgemahnte als auch Opfer einer Urheberrechtsverletzung werden es weiterhin schwer haben, ihre jeweiligen Rechtsansprüche durchzusetzen.

„Grundschutzscanner“

Seit dem Linuxtag (09.-12.06.2010) ist Version 3.0 der BOSS-Scanner-Live CD des BSI verfügbar. Sie basiert nun auf einer komfortabel startbaren Version des Scannerframeworks OpenVAS 3.0. Damit bleibt das BSI seiner Open-Source-Philosophie treu. Mit der Förderung der Entwicklung von Plugins (ca. 17.000) wurden auch die Anwender in Unternehmen und Behörden nicht vergessen: Aktuelle Plugins sind über den kommerziellen Greenbone Security Feed (GSF) beziehbar.

Der GSF in BOSS 3.0 liefert bei einigen Plugin-Ergebnissen genauere und weiter gehendere Ergebnisse als Nessus. Der GSF wurde im Kontext der als Open Source verfügbaren Security Management Suite OSSIM sogar mit Scan-Konfigurationen für die 10. und 11. Ergänzungslieferung der IT-Grundschutz-Kataloge ausgestattet. Aber Achtung: Ein „fehlerfreier“ Scan bedeutet nicht, dass ein IT-Verbund IT-Grundschutz-konform ist – naturgemäß werden z. B. organisatorische Maßnahmen nicht geprüft.

Erfreulich ist, dass mit BOSS 3.0 bewährte und neue Werkzeuge nun wieder „amtlich“ für Auditoren verfügbar sind, darunter amap, nmap, ldapsearch, snmpwalk, strobe, portbunny und w3af – ein wichtiges Signal zur Klärung der immer noch verbreiteten Unsicherheiten im Umgang mit dem „Hackerparagrafen“ § 202c StGB.

Sammelwütig

Nach Mahnungen diverser Gerichte und des Bundesdatenschutzbeauftragten (22. Tb., S. 58) hat das Bundesinnenministerium mit Zustimmung des Bundesrats am 04.06.2010 im Schatten der WM die konstituierende Verordnung zur „Verbunddatei Gewalttäter Sport“ und zahlreichen weiteren zentralen Dateien des Bundeskriminalamts erlassen.

Die Verordnung legt die Art der zu speichernden Daten für ca. 80 präventive Verbunddateien fest, die zwischen 100 und 6 Millionen Datensätze über verdächtige Bürger enthalten.

Für die „Hooligan-Datenbank“ mit 11.245 gespeicherten Personen (Stand 2009) dürfen neben Adress- und Identifizierungsdaten etwa Schulabschluss, frühere Staatsangehörigkeit, Volkszugehörigkeit, Angaben zu Personalausweis oder Reisepass, Angaben zu Kommunikationsmitteln, Konten- und Vermögensinformationen, Beziehungen zu Orten, Gruppen, Ereignissen oder Einzelpersonen sowie Referenzen auf weitere gespeicherte Vorgänge gesammelt und gespeichert werden. Zur Aufnahme in die Datei genügen eingeleitete Ermittlungen; beschränkt auf umfassende Kontaktdaten sogar die bloße Begleitung von Verdächtigen. Gelöscht werden müssen die Daten dagegen nur, wenn bei einer Einstellung des Verfahrens ausdrücklich das Fehlgehen des Verdachts festgestellt wurde.

Mit rekordverdächtiger Reaktionszeit hat das Bundesverwaltungsgericht am folgenden Tag einen anhängigen Löschantrag mit Verweis auf die Verordnung zurückgewiesen.

Ein Lerneffekt aus der gerade erst drei Monate alten Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung ist nicht feststellbar – das betrifft bereits die Rechtsgrundlagen im BKA-Gesetz: Es fehlen konkrete Vorgaben zur Datensicherheit, die Transparenz der Erhebung und Speicherung ist ebenso wie die diesbezüglichen Kriterien zur Zulässigkeit ungenügend – ein weiterer Fall für das Bundesverfassungsgericht?

Mythen sterben langsam

Am 28.06.2010 publizierte der Branchenverband BITKOM die Ergebnisse einer Forsa-Studie – mit vermeintlich erschütternden Ergebnissen: 41 % der Befragten ändern ihre Passworte nie. „Die wichtigsten Passwörter sollten alle drei Monate geändert werden“, fordert Prof. Dieter Kempf vom Präsidium des BITKOM.

Dabei sind erzwungene Passwortwechsel in der Praxis meist nutzlos: Sie verleiten Benutzer dazu, sich „Bildungsregeln“ zu überlegen – und damit den Sinn von Passwortwechseln zu konterkarieren. Denn Wechsel sollen im Falle einer Kompromittierung den Schaden begrenzen – erkennt der Angreifer aber die Bildungsregel, kann er aus jedem geknackten Passwort das nächste ableiten.

Zielführender als die Verbreitung von Passwort-Mythen (siehe SSN 6/2009) wäre die Forderung nach längeren Passwörtern. Das Projekt RainbowCrack publizierte am 17.06.2010 Version 1.41 des Software-Crackers, der mit einer schnellen Grafikkarte als Co-Prozessor und einer 576 GB großen Rainbow-Tabelle acht Zeichen lange Passwörter in 30 Minuten (!) findet. Kürzer als 10 Zeichen dürfen Passwörter (zumindest unter Windows) heute nicht mehr sein, wenn sie einem solchen Cracker wenigstens 90 Tage standhalten sollen – zum Schutz vor einer parallelisierten Berechnung sind 12 Zeichen das Minimum.

Nur ein Zeichen mehr, und der Aufwand, ein gutes Passwort zu Cracken, steigt um den Faktor 84 – das sollte für ein halbes Berufsleben reichen.

Schauen, was läuft

Am 15.06.2010 wurde Version 10 von Autoruns veröffentlicht. Ursprünglich von Sysinternals entwickelt und später von Microsoft übernommen zeigt es unter anderem an, welche Programme und Dienste unter Windows gestartet werden. Damit lassen sich nicht nur unnötig gestartete Programme, Dienste und Prozesse erkennen und deaktivieren, sondern auch eingenistete Schadsoftware und Spyware identifizieren.

Ähnliches leistet das Programm Starter; es bietet sogar die Möglichkeit, Dienste direkt zu konfigurieren oder eine Recherche zu den „Fundsachen“ in verschiedenen Internet-Suchmaschinen zu starten.

Allerdings sollten derartige Tools generell vor der produktiven Nutzung in einer Testumgebung überprüft werden – nicht selten wird beliebte Freeware in mit Schadcode infizierten Varianten verbreitet.

Löchrige Pen-Tests

Unter dem Titel “Why Johnny Can’t Pentest” veröffentlichten drei Forscher von der University of California am 27.04.2010 einen ausführlichen Vergleich aktueller Schwachstellenscanner für Web-Anwendungen. Dafür analysierten sie die Ergebnisse der Pen-Tests eigens entwickelter Web-Anwendungen mit bekannten Schwachstellen.

Die 21seitige Studie liefert nicht nur ein “Ranking” der getesteten Produkte – besonders interessant sind die Dokumentation der Vorgehensweise und die Erkenntnis, dass sich mit heutiger Technik einige Schwachstellen, wie beispielsweise Fehler in der Anwendungslogik, gar nicht und andere nur sehr schwer automatisiert erkennen lassen.

Das Fazit ist wenig überraschend: Der Einsatz von automatisierten Scannern sollte grundsätzlich durch händische Prüfungen ergänzt werden. Ausführlich werden die Ergebnisse der Studie auf der DIMVA 2010 in Bonn am 08.-09.07.2010 vorgestellt.

Secorvo News

iPhone Security

In nicht wenigen Unternehmen hält derzeit Apples iPhone Einzug. Trotz seiner nach wie vor deutlichen Nachteile bei Business-Anwendungen gegenüber RIMs BlackBerry wiegen „Sex-Appeal“ und Nimbus des Geräts auch bei Führungskräften oft schwerer.

Wie sicher aber sind Unternehmensdaten auf einem iPhone aufgehoben? Was ist von der Hardware-Verschlüsselung und anderen Schutzmechanismen zu halten? Lassen sich iPhones ohne Inkaufnahme zusätzlicher Risiken in die IT-Infrastruktur integrieren? Diesen und weiteren Fragen ist Jörg Völker auf den Grund gegangen – und hat die Ergebnisse seiner Untersuchungen nun in der Fachzeitschrift „Datenschutz und Datensicherheit“ (DuD) veröffentlicht.

„Tag der IT-Sicherheit"

Zum zweiten Mal findet am **15.07.2010** der Karlsruher „Tag der IT-Sicherheit“ statt – eine Kooperationsveranstaltung der IHK Karlsruhe, des Cyber-Forum e. V. und der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si). Die Vorträge behandeln aktuelle Themen der IT-Sicherheit und Best-Practice-Beispiele, darunter ein Lagebericht des Landesamts für Verfassungsschutz Baden-Württemberg zur Wirtschaftsspionage in deutschen Unternehmen, eine kritische Analyse der Sicherheit von iPhones und die erfolgreiche Awareness-Kampagne der EnBW AG.

Die Veranstaltung beginnt um 14 Uhr und richtet sich an Geschäftsführer und IT-Leiter unabhängig von Branche und Unternehmensgröße. Hier finden Sie das vollständige Programm und die Möglichkeit zur Anmeldung.

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Juli 2010	
08.-09.07.	DIMVA 2010 (Bonn)
15.07.	2. Karlsruher „Tag der IT-Sicherheit“ (KA-IT-Si/IHK/Cyberforum, IHK Karlsruhe)
24.-29.07.	Black Hat (Las Vegas/US)
29.07.-01.08.	DEFCON 18 (DEFCON, Las Vegas/US)
August 2010	
02.-04.08.	DFRWS 2010: Digital Forensic Research Workshop (DFRWS, Portland/US)
09.-13.08.	19th USENIX Security Symposium (Washington/US)
15.-09.08.	Crypto 2010 (IACR, Santa Barbara/US)
September 2010	
20.-23.09.	SEC 2010 (IFIP, Brisbande/AUS)
20.-24.09.	TISP-Schulung (Secorvo College)
28.-30.09.	Forensik – Verfahren, Tools, Praxiserfahrung (Secorvo College)
28.-29.09.	7. Security Awareness Symposium (Secorvo, Ettlingen)

Fundsache

Die Skulptur „Kryptos“ des Künstlers James Sandborn vor dem Hauptsitz der CIA von 1991 enthält vier Kryptogramme, von denen drei 1998 von einem Mitarbeiter der CIA dechiffriert wurden. Das vierte, 97 Zeichen lange Kryptogramm ist bis heute ungelöst.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Jochen Schlichting

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

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