secorvo
security consulting

Secorvo Security News

März 2009

Editorial: Zwangsbeglückung

Vor 22 Jahren erblickte der erste E-Mail-Sicherheitsstandard das Licht der Welt: In RFC 989 spezifizierte John Linn im Februar 1987 „Privacy Enhancement for Internet Electronic Mail“, einen frühen Vorläufer von S/MIME. Obwohl zahlreiche E-Mail-Clients, darunter Thunderbird, Notes und Outlook, heute S/MIME-basierte E-Mail-Verschlüsselung standardmäßig unterstützen und OpenPGP-Verschlüsselung sogar über die freie GnuPG-Programmfamilie komfortabel genutzt werden kann, sind E-Mails nach wie vor zumeist elektronische Postkarten.

Eine willkommene Gelegenheit, behütend einzugreifen: „*Der moderne Staat steht deshalb vor der Aufgabe, im elektronischen Kommunikationsraum für eine Grundversorgung an Verbindlichkeit und Vertraulichkeit zu sorgen*“, so das BSI im BSI-Forum der Fachzeitschrift <KES> (1/2008). „De-Mail“ soll der Dienst heißen, der ab 2010 mit Hilfe privatwirtschaftlicher „Bürgerportale“ einen Schlussstrich unter die chaotische Internet-Kommunikation ziehen soll.

Bei genauer Betrachtung entpuppt sich De-Mail als missratener Versuch, der digitalen Signatur nach 12 Jahren Misserfolgsgeschichte doch noch in den Sattel zu helfen. Das Konzept krankt an denselben Designfehlern: Wer De-Mail nutzt, schickt eine nicht abstreitbare Nachricht. Der Empfänger wiederum ist verantwortlich für das fristgerechte Abholen elektronischer Zustellurkunden. Eine Verschlüsselung erfolgt hingegen nur zwischen Nutzern und Bürgerportalen.

Am 23.03.2009 erlitt der Gesetzentwurf zur Regelung der Bürgerportale vom 04.02.2009 eine empfindliche Schlappe: Die Empfehlung der Ausschüsse des Bundesrats ist ebenso klarsichtig wie vernichtend: So seien die „konkreten Sicherheitsanforderungen an mehreren Stellen unklar“ und die Pflicht des Empfängers zur regelmäßigen Leerung des Postfaches ein unzumutbarer Grundrechtseingriff. Offenbar gibt es noch Volksvertreter, die nicht vergessen haben, dass der Idealtypus des „modernen Staates“ kein Leviathan, sondern eine freiheitliche Ordnung ist.

Inhalt

secorvo
security consulting

Security News

Klare Absage

So deutlich hat das Bundesverfassungsgericht weder bei der Online-Durchsuchung noch bei der Vorratsdatenspeicherung geurteilt: Am 03.03.2009 erklärte es den Einsatz von Nedap-Wahlcomputern und die Bundeswahlgeräteverordnung (BWahlGV) vom 20.04.1999 für verfassungswidrig, da „sie keine dem verfassungsrechtlichen Grundsatz der Öffentlichkeit der Wahl entsprechende Kontrolle sicherstellt". Denn es gilt: „Beim Einsatz von elektronischen Wahlgeräten müssen die wesentlichen Schritte von Wahlhandlung und Ergebnisermittlung [vom Wähler] zuverlässig und ohne besondere Sachkenntnis überprüft werden können." Ein klares Votum für die Souveränität des Souveräns (siehe SSN 10/2008) – und das an der Universität Karlsruhe entwickelte und mit dem IT-Sicherheitspreis 2008 ausgezeichnete „Bingo Voting" (Kurzbeschreibung).

Keine drei Wochen nach dem Urteil berichtete Matt Blaze, Mitautor einer Studie über Sicherheitsmängel einer in den USA verbreiteten elektronischen Wahlmaschine, am 23.03.2009 über die Aufdeckung systematischer Wahlfälschungen in Kentucky: Sechs Wahlhelfer hatten eine Schwäche in der Benutzerschnittstelle der Wahlmaschine zur Veränderung von Stimmabgaben genutzt.

SSL-Authentifikation für alle

SSL – seit zehn Jahren unter dem Namen Transport Layer Security (TLS) genormt – ist ein bekanntes, bewährtes und deshalb von seinem ursprünglichen Zweck, der Absicherung von Webzugriffen, auch auf andere Bereiche wie z. B. VPN oder WLAN übertragenes Sicherheitsprotokoll. Sollte man meinen. Auch sollte sich im Jahr 20 nach der Erstveröffentlichung des X.509 Standards herumgesprochen haben, dass Zertifikate naturgemäß öffentliche Daten sind und für sicherheitsrelevante Operationen das private Gegenstück des per Zertifikat bestätigten öffentlichen Schlüssels benötigt wird.

Umso größer die Verwunderung, als Microsoft am 10.03.2009 im Security Bulletin MS09-007 einräumte, dass die SSL-Komponente in Windows – vom Veteranen Windows 2000 bis zum neuesten 64-Bit-System – bei der Client-Authentifikation jahrelang patzte: Zwar wurde die Gültigkeit des vorgelegten Zertifikats geprüft; der im Standard vorgeschriebene Schritt, per Signatur der ausgetauschten Protokollnachrichten zu verifizieren, dass der Client auch den passenden privaten Schlüssel verwendet, wurde jedoch eingespart. Tatsächlich akzeptierte der Server also jeden Client mit irgend einem gültigen Zertifikat - ob nun dem eigenen oder einem fremden.

Durch das weite Einsatzspektrum von SSL/TLS sind wahrscheinlich nicht nur IIS-basierte Webanwendungen von diesem Bug betroffen, sondern jede zertifikatsbasierte VPN-, WLAN- und NAC-Anmeldung, sofern dabei der Microsoft-eigene RADIUS-Dienst IAS zum Einsatz kommt.

Vielleicht haben sich die Microsoft-Entwickler bei der Implementierung auf das SSL-Diagramm in Wikipedia verlassen – das den wichtigen Verifikationsschritt ebenfalls fehlerhaft darstellt. Manchmal geht Studieren doch über Probieren.

„Man in the Middle" is back

Nachdem in der jüngeren Vergangenheit andere Themen öffentlich diskutiert wurden, ist kürzlich die Bedrohung durch "Man in the Middle"-Attacken wieder ins Zentrum der Aufmerksamkeit gerückt, insbesondere dank der Veröffentlichung des White Papers "Active Man in the Middle Attacks – A Security Advisory" von Roi Saltzman und Adi Sharabani aus der IBM Rational Application Security Group am 27.02.2009.

In der Präsentation und dem White Paper werden Szenarien vorgestellt, bei denen ein Angreifer als "Man in the Middle" nicht durch Mitlesen auf zufällig übertragene Credentials (Cookies) wartet, sondern Server-Antworten so manipuliert, dass der Client seine Credentials ohne Wissen des Benutzers an ausgesuchte Webseiten überträgt. Dabei wird kein Implementierungsfehler, sondern ein Design-Problem von HTTP ausgenutzt.

Erst wenige Tage zuvor war das Thema „Man in the Middle" (MitM) am 18.02.2009 auf der Blackhat 2009 von Moxie Marlinspike in seinem Vortrag "New Tricks For Defeating SSL In Practice" aus einem anderen Blickwinkel beleuchtet worden. Darin wurden MitM-Angriffe betrachtet, die mit Manipulationen an SSL-Zertifikaten arbeiten. Als „Proof of Concept" wurde das Tool sslstrip vorgestellt.

Die Präsentationen beider Autoren auf der OWASP AU 2009 wurden am 04.03.2009 von Robert Hansem („RSnake") auf ha.ckers.org kommentiert. Wir können uns seinem Fazit anschließen: Das Thema ist keineswegs neu, aber inzwischen stehen so mächtige Angriffswerkzeuge zur Verfügung, dass zu erwarten ist, dass diese in Zukunft verstärkt von Amateur-Hackern genutzt werden.

Aktuelle Fehlerübersicht

Am 10.03.2009 wurde Version 1.3 des von 50 führenden amerikanischen IT-Unternehmen und Organisationen getragenen Projekts Common Weakness Enumeration (CWE) vorgestellt. In dieser Liste

werden die aktuell wichtigsten und schwerwiegendsten Sicherheitsprobleme bei der Softwareentwicklung identifiziert. Dazu werden sicherheitsrelevante Fehlerquellen bei der Erstellung von Software systematisch erfasst und detailliert ausgewertet.

Entsprechend wurden die 2009 CWE/SANS Top 25 Most Dangerous Programming Errors an die Resultate der aktuellen Erhebung angepasst. Sie sollten an dem Arbeitsplatz eines jeden Softwareentwicklers hängen – gleich neben den OWASP Top 10.

Umstrittenes BDSG

In seiner Sitzung am 23.03.2009 befasste sich der Innenausschuss des Deutschen Bundestages mit den geplanten Änderungen im Bundesdatenschutzgesetz und dem Entwurf eines Datenschutzauditgesetzes (DSAG). Die Bundesregierung hatte hierzu im Dezember neue Texte vorgelegt, nachdem die Erstentwürfe vom Spätsommer in der Fachwelt insgesamt auf große Kritik gestoßen waren.

Leider folgt der aktuelle Entwurf des DSAG weiterhin einem einstufigen Verfahren, bei dem die Gutachter (Kontrollstellen) gleichzeitig die zertifizierende Stelle sein sollen. Es ist schlichtweg unerklärlich, warum die Bundesregierung hinter international übliche Standards zurückfallen will: Schließlich ist die Trennung von Begutachtung und Zertifizierung in einem zweistufigen Verfahren Voraussetzung für die Minimierung von Interessenskonflikten – und damit Garant für die Seriosität eines Zertifikats. Erwartungsgemäß erntete gerade diese Grundkonzeption allgemeines Kopfschütteln in der Expertenrunde.

Heftige Kontroversen wurden unter den Sachverständigen über die vorgesehenen Regelungen zum Listenprivileg ausgetragen. Sogar einige Abgeordnete ließen sich angesichts der teils recht emotional vorgetragenen Stellungnahmen zu flammenden Reden während der Anhörung hinreißen, die sonst der parlamentarischen Debatte vorbehalten sind.

Die auf dem Datenschutzgipfel im Herbst beschlossene Abkehr vom Opt-Out-Verfahren im Bereich der Werbung, Markt- und Meinungsforschung und des Adresshandels steht wieder zur Debatte. So sehr fühlen sich Versandhandel, Adresshändler und Verlage durch die Pflicht zur Einwilligungserteilung eingeschränkt, dass sie das Schreckgespenst tausender bedrohter Arbeitsplätze an die Wand malen. In wirtschaftlich problematischen Zeiten offenbar ein wirksames Argument, um das informationelle Selbstbestimmungsrecht wieder einmal hintenan zu stellen. Nun wird die Stellungnahme des Innenausschusses gespannt erwartet.

AutoRun Revisited

Schon am 08.11.2007 hatte Scott Dunn darauf hingewiesen – und war am 20.03.2008 vom US-Cert bestätigt worden: Die von Microsoft beschriebenen Maßnahmen zur Deaktivierung der AutoRun-Funktion funktionierten nicht korrekt (SSN 12/2008). Der von Microsoft am 08.07.2008 veröffentlichte Patch zur Behebung dieser Schwachstellen war allerdings zunächst nur für Windows Vista und Windows Server 2008 verfügbar – nicht für die weit verbreiteten Systeme unter Windows XP.

Wohl angesichts der Conficker-Wurm-Infektionen über USB-Sticks und eines neuen US-CERT Advisorys vom 20.01.2009 hat Microsoft endlich reagiert und am 24.02.2009 ein Security Advisory sowie Patches für Windows 2000, XP und Server 2003 zur Verfügung gestellt, die diese Gefährdung beseitigen.

Unsere Empfehlung: Wer zur Deaktivierung von AutoRun den neuen Patch installiert, sollte sicherheitshalber auch die Wirksamkeit überprüfen.

Secorvo News

Secorvo College aktuell

Nach der Zertifizierung ist vor der Zertifizierung: Vom **22. bis 26.06.2009** findet das zweite diesjährige T.I.S.P.-Seminar mit anschließender Zertifikatsprüfung statt. Vorher bietet Secorvo College mit dem „aktuellen Klassiker“ IT-Sicherheit heute vom **21. bis 24.04.2009** einen Überblick der zentralen Themen der IT-Sicherheit und vom **05. bis 08.05.2009** einen umfassenden Einblick in die Welt der Public Key Infrastrukturen, praktische Übungen inklusive.

Programm und Online-Anmeldung unter
http://www.secorvo.de/college

Das Original ist die beste Kopie

Auf dem kommenden Event der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) am **07.05.2009** wird Rüdiger Kügler von WIBU SYSTEMS – einem der Pioniere auf dem Markt für Softwarelizenzmanagement – Hintergründe und aktuelle Herausforderungen des Schutzes digitaler Güter vor Plagiaten (vulgo Raubkopien) beleuchten und heutige "best practices" zur Realisierung des Lizenzhandlings vorstellen. Im Anschluss gibt es wie gewohnt Gelegenheit zum „Buffet-Networking“. Um Anmeldung wird gebeten.

Das darauffolgende KA-IT-Si-Event am **25.06.2009** – Vertrauen ist gut – Zertifizierung ist besser – ist einem Erfahrungsbereicht zur Zertifizierung nach dem Sicherheitsstandard ISO 27001 gewidmet.

Veranstaltungshinweise

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

April 2009	
21.04.	2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (Usenix, Boston/US)
21.-24.04.	IT-Sicherheit heute (Secorvo College)
26.-30.04.	Eurocrypt 2009 (IACR, Köln)
Mai 2009	
05.-07.05.	10. Datenschutzkongress 2009 (EUROFORUM, Berlin)
05.-08.05.	PKI (Secorvo College)
07.05.	Das Original ist die beste Kopie (KA-IT-Si, Karlsruhe)
18.-20.05.	IFIP SEC 2009 (IFIP, Zypern/CY)
20.-22.05.	2009 ADFSL Conference on Digital Forensics, Security and Law (ADFSL, Burlington/US)
Juni 2009	
08.-09.06.	DuD 2009 (Computas, Berlin)
22.-26.06.	T.I.S.P. Schulung (Secorvo College)

Fundsache

Am 25.03.2009 wurde Version 1.0 von OpenSAMM (Software Assurance Maturity Model) des Open Web Application Security Projects (OWASP) veröffentlicht. Das Modell beschäftigt sich mit der Bewertung der Sicherheit im Softwareentwicklungsprozesse. Dabei werden alle Aspekte von der Steuerung über die Entwicklung, die Tests bis hin zur Verteilung betrachtet. Auf 96 Seiten werden nicht nur abstrakte Anforderungen gestellt, sondern auch praktische Hinweise zum Einsatz verschiedener Maßnahmen zur Verbesserung der Softwareentwicklung gegeben.

Impressum

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

ISSN 1613-4311

Redaktion: Dirk Fox, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Karin Schuler

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