secorvo
security consulting

Secorvo Security News

März 2008

Editorial: Ach wie gut!

Heute back' ich, morgen brau' ich,
übermorgen hol' ich der Königin ihr Kind;
ach, wie gut dass niemand weiß,
dass ich Rumpelstilzchen heiß!

Das war es also. Dieses Märchen unserer Kindheit erklärt unser gespaltenes Verhältnis zum Datenschutz. Tief verinnerlicht haben wir, dass nur derjenige seinen richtigen Namen verheimlicht, der Böses im Schilde führt – wird er erkannt, reißt er sich selbst in Stücke. Und so glauben wir im Umkehrschluss, dass der Unbescholtene nichts zu verbergen habe. Streift man durch „soziale Netzwerke" wie myspace, facebook, Xing oder SchülerVZ, so drängt sich der Eindruck auf, als wollten Millionen aus dieser tief verankerten Überzeugung ihre Unbescholtenheit durch exzessives Nichtverbergen unter Beweis stellen.

Wehe aber, wenn die Erkenntnis dämmert, dass es vielleicht nicht immer gut ist, Dritten umfangreiche persönliche Informationen zur Verfügung zu stellen. So geschehen, als facebook ab 07.11.2007 zur Nutzung des verkaufsfördernden „me too"-Effekts die aktuellen Online-Einkäufe der registrierten Benutzer an deren Freundeslisten schickte. Aber auch unwissentlich geben viele Nutzer persönliche Informationen im Internet preis – so weiß beispielsweise nicht jeder, dass die private Wunschliste beim Online-Buchhändler Amazon von jedermann eingesehen werden kann, wenn die Voreinstellung nicht geändert wurde. Daher lohnt es, gelegentlich bei einer Personensuchmaschine wie Yasni das eigene „Bild im Netz" zu überprüfen.

Zugleich nimmt die Überwachung im Windschatten der Terrordrohung zu – ungeachtet der jüngsten Urteile des BVerfG zu Online-Durchsuchung und Vorratsdatenspeicherung, die dem behördlichen Zugriff auf persönliche Daten hohe Hürden auferlegen. Dabei gibt die älteste Demokratie Europas den Schritt vor: Nach der flächendeckenden Installation von Videokameras in britischen Großstädten soll zukünftig eine Bilddatenbank die automatische Identifikation Verdächtiger erlauben. Ein 18-monatiges Pilotprojekt mit 750.000 Fotos verlief offenbar vielversprechend. Ob es hilft, den Namen des Ideengebers herauszufinden – damit er sich selbst in Stücke reißt?

Inhalt

secorvo
security consulting

Security News

Mifare-Cloning

Auf dem Jahreskongress des Chaos Computer Clubs stellten Karsten Nohl und Henryk Plötz am 28.12.2007 einen Angriff auf das Authentifikationsverfahren kontaktloser Mifare-Chipkarten vor. Dem vom Hersteller geheimgehaltenen, etwa 15 Jahre alten "CRYPTO1"-Algorithmus waren sie mit einer Mikroskop-Analyse des Chip auf die Spur gekommen, um dann nach kryptographischen Schwächen (zu kleiner Zufallswert, lineares Schieberegister) darin zu suchen. Zu dieser Krypto-Schwachstelle gibt es nun den passenden „Mifare-Cloner“: Am 12.03. 2008 haben Forscher der Radboud Universiteit Nijmegen ein Video in YouTube veröffentlicht, auf dem sie zeigen, wie sie mit minimalem Aufwand Mifare-basierte Zugangskarten duplizieren.

Von der Attacke betroffen sind Tausende von Anwendungen mit einer Milliarde ausgegebenen Karten, vom Betriebsausweis über die Kantinenkarte bis zum bargeldlosen Bezahlsystem im öffentlichen Nahverkehr, sofern sie Mifare-Chips des Typs MF1 IC S50 oder S70 verwenden. Fein raus ist, wer seine Anwendung bereits auf den neueren Mifare DESFire (MF3 IC D40) migriert hat – statt einer etwas ältlichen Stromchiffre verwendet er bei der Authentifikation wahlweise DES oder TripleDES.

Fingerwischerei

In einem am 12.03.2008 online veröffentlichten Beitrag aus c't 05/08 beschreibt Daniel Bachfeld eine simple Methode, wie auf zahlreiche USB-Sticks unter Umgehung des Fingerprint-Schutz zugegriffen werden kann. Verwendet der Stick den Controller USBest UT176 oder UT 169 von Afa Technology, so erfolgt zwar die Fingerprint-Prüfung auf dem Chip – das Freigabe-Kommando für die „geschützte“ Partition sendet jedoch die Systemsoftware vom PC. Mit dem Open-Source-Tool PLscsi gelingt der Zugriff ohne Fingerkuppen-Imitat in nur drei Schritten.

Das Beispiel zeigt (leider) wieder einmal, dass es meist wenig hilft, einen Sicherheitsmechanismus nachträglich an eine bestehende Lösung „anzuflanschen“ – ist er nicht geeignet im System verankert, lässt sich das Verfahren an der Nahtstelle oft allzu leicht wieder auftrennen.

Einsatz von WAFs

Das OWASP German Chapter veröffentlichte am 18.03.2008 den deutschsprachigen Guide „Best Practices: Einsatz von Web Appliction Firewalls“. Das lesenswerte 25-seitige Dokument wendet sich an technische Entscheider im Bereich der Sicherheit von Web-Applikationen. Nach einer Einordnung von Web Application Firewalls (WAF) wird deren Haupteinsatzzweck erläutert – die nachträgliche Absicherung des externen Verhaltens von produktiven Web-Anwendungen, mit vertretbarem Aufwand und ohne Änderung der Applikation.

Die Betrachtung der Schutzmechanismen fokussiert auf den Schutz gegen die OWASP Top 10 (siehe SSN 06/2007). Abschließend werden Kriterien zur Einsatz-Entscheidung, Checklisten und Rollenmodelle für die Einführung sowie Best Practices für den Betrieb vorgestellt. Positiv fällt auf, dass in dem Dokument in allen Phasen Wert auf die Berücksichtigung von Aufwandsschätzungen gelegt wird.

Citrix-Ausbruch

Nicht nur bei einer Betriebssystemvirtualisierung sondern auch bei der Desktopvirtualisierung ist der Ausbruch aus einem beschränkten Kontext ein Risiko. So deckte Stefan Gora am 07.03.2008 auf, dass in Citrix-Umgebungen über den Microsoft-Taschenrechner auf weitere Applikationen zugegriffen werden kann, für die keine Berechtigung besteht. Denn unter Windows 2003 Server werden die Lizenzbedingungen des Taschenrechners mit dem Editor angezeigt, der über die Funktion „Datei öffnen“ das Starten weiterer Anwendungen ermöglicht.

Die Sicherheitslücke ist ein schönes Beispiel dafür, dass Hintertüren in komplexen Umgebungen manchmal ganz harmlos daherkommen. Zwar erlaubt der Taschenrechner unter den aktuelleren Microsoft-Server-Versionen diesen „Ausbruch“ nicht; dennoch empfehlen wir die Nutzung verschiedener Terminal-Server-Plattformen für Benutzergruppen mit unterschiedlichen Berechtigungen.

Rechenfehlerangriff

Zwei japanische Wissenschaftler veröffentlichten am 27.12.2007 einen Angriff auf den Advanced Encryption Standard (AES), der unter bestimmten Voraussetzungen 88 Bit eines 128-Bit-AES-Schlüssels rekonstruiert. Sie verwendeten dazu die auf den ersten Blick befremdlich anmutende Methode der „Differentiellen Fehleranalyse“ (DFA). In diesem speziellen Fall muss dazu ein bekannter Klartext mehrfach mit demselben Schlüssel verschlüsselt werden: Einmal ungestört, ein anderes Mal mit einem gezielt induzierten Fehler. Dabei muss der Angreifer erreichen, dass bei der neunten von zehn Runden eine bestimmte 32-Bit-Variable einen fehlerhaften Wert annimmt.

In der Praxis dürfte ein derartiger Angriff bei den meisten Anwendungen des AES nur äußerst schwer erfolgreich durchzuführen sein. Wer dennoch auf

Nummer sicher gehen will und die vierzigprozentige Leistungseinbuße nicht scheut, sollte den AES mit der maximalen 256 Bit Schlüssellänge verwenden – mit weiteren 128 Schlüsselbits und vier zusätzlichen Runden.

VMware-Hacks

Die am 25.02.2008 von Coresecurity veröffentlichte und vom Hersteller bestätigte Schwachstelle in VMware-Workstation und dem VMware-Player sollte nicht unterschätzt werden: Durch den Bug im Mechanismus der „Shared Folder" ist es möglich, von Wirtsbetriebssystemen aus auf das Hostsystem – und damit auf weitere Wirtssysteme – zuzugreifen. Die Abschottung der Systeme kann so vollständig ausgehebelt werden.

Unverständlich ist, dass bisher seitens VMware nur ein primitiver Workaround für die schon am 16.10. 2007 an den Hersteller gemeldete Schwachstelle vorliegt: die Empfehlung, „Shared Folder" zu deaktivieren.

Druckfrischer Entwurf

Auf den Webseiten des Bundesamt für Sicherheit in der Informationstechnik (BSI) steht der druckfrische Entwurf des „BSI Standards 100-4: Notfall-Management" in der Version 0.7 vom 19.03.2008 zum Download bereit. Die Veröffentlichung dieses schon lange erwarteten BSI-Standards zum Thema Business Continuity (BCM) und Notfall-Management verzögerte sich durch die Abstimmung mit den britischen Standards BS 25999-1:2006 und BS 25999-2:2007.

Das BSI bittet um kritische Prüfung und Kommentierung des aktuellen 82-seitigen Entwurfs bis Ende April 2008.

Krypto-Historie

Auf der Tagung „Día Internacional de la Seguridad de la Información" (DISI) gab Martin E. Hellman am 03.12.2007 an der Universidad Politécnica de Madrid einen spannenden Einblick in die Geburtsstunden der modernen Kryptographie („A Fool's Errand"). Sowohl seine Vortragsfolien als auch ein Video der Keynote sind inzwischen online verfügbar – die Dokumentation einer der Sternstunden der IT-Sicherheit.

Überraschend sein wenig technischer Ausblick: „What is the most important unsolved problem in cryptography? Lack of user awareness."

Secorvo News

Secorvo College aktuell

Eine Einführung in das Information Security Management von A(udit) bis Z(ertifizierung) inklusive Umsetzungsworkshop bietet Secorvo College vom **15.–18.04.2008.** Ein guter Einstieg für alle, die ihr Sicherheitsmanagement auf Standard-Konformität „abklopfen" möchten.

Das tatsächlich erreichte Sicherheitsniveau lässt sich auch durch ein Audit prüfen. Dazu bietet das Seminar IT-Sicherheitsaudits in der Praxis am **06.–08.05.2008** zahlreiche Hilfestellungen.

Am **27.–30.05.2008** wird der Klassiker IT-Sicherheit heute wieder aufgelegt – und deckt nach einer gründlichen Überarbeitung und Aktualisierung in vier Tagen die wichtigsten aktuellen Themen der IT-Sicherheit ab.

Und im Juni bietet sich Ihnen die nächste Gelegenheit, Ihre Fachkunde zu zertifizieren: auf dem T.I.S.P.-Seminar am **02.–06.06.2008**, mit anschließender Prüfung (Achtung: frühzeitige Anmeldung empfohlen).

Detaillierte Programme, vollständige Jahresübersicht und Online-Anmeldung unter http://www.secorvo.de/college

Aktualisierte White Paper

Eine aktualisierte Fassung des Secorvo White Papers „Das Policy-Rahmenwerk einer PKI" (Petra Barzin, Stefan Kelm) ist seit dem 27.03.2008 verfügbar.

Ebenfalls aktualisiert wurde die Forensik-Checkliste von Stefan Kelm (Version 1.2 vom 05.03.2008).

Identity Management Symposium

Gemeinsam mit der vps ID Systeme GmbH veranstaltet Secorvo am **22.–23.04.2008** das erste „Identity Management Symposium" in Ettlingen (bei Karlsruhe). Im Stil der bewährten Secorvo-Symposien wird es einen intensiven Erfahrungsaustausch mit und zwischen Unternehmen und Behörden bieten, die ein integriertes Identity Management vorbereiten oder bereits eingeführt haben. Unter anderem werden die Lösungen von BASF, BMW, ESG, Evonik, Fraunhofer und Swisscom vorgestellt (vollständiges Programm und Online-Anmeldung).

ITSF 2008

Das von GAI Netconsult und der ComConsult Akademie veranstaltete IT-Sicherheits-Forum 2008 findet in diesem Jahr vom 26.-29.05.2008 in Frankfurt statt. Auch diesmal wirkt Secorvo am Programm der etablierten Veranstaltung mit einem Tutorium zu „Security Awareness" und einer Keynote mit. Die Frühbucherphase endet am 31.03.2008.

Veranstaltungshinweise

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

April 2008	
02.-04.04.	Sicherheit 2008 (GI, Saarbrücken)
14.-17.04.	Eurocrypt 2008 (IACR, Istanbul/TR)
15.-18.04.	Information Security Management - von A(udit) bis Z(ertifizierung) (Secorvo College)
15.04.	First USENIX Workshop on Large-scale Exploits and Emergent Threats (Usenix, San Francisco/US)
22.-23.04.	1. Identity Management Symposium 2008 (Secorvo & vps, Karlsruhe-Ettlingen)
Mai 2008	
06.-07.05.	9. Datenschutzkongress 2008 (Euroforum, Berlin)
06.-08.05.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
26.-29.05.	IT Sicherheitsforum 2008 (GAI Netconsult, Frankfurt)
27.-30.05.	IT-Sicherheit heute (Secorvo College)
Juni 2008	
02.-06.06.	T.I.S.P.-Schulung (Secorvo College)
09.-10.06.	DuD 2008 (Computas, Berlin)
17.-18.06.	6. Security Awareness Symposium (Secorvo, Karlsruhe-Ettlingen)
24.-25.06.	D-A-CH Security 2008 (GI/OCG/Bitkom/TTT, Berlin)
24.-26.06.	Sichere Softwareentwicklung (Secorvo College)
Juli 2008	
01.-03.07.	Forensik (Secorvo College)

Impressum

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

ISSN 1613-4311

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

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