secorvo
security consulting

Secorvo Security News

Oktober 2013

Die Waffen der Freunde

Die Enthüllungen Edward Snowdens über die nachrichtendienstliche Tätigkeit unserer Verbündeten lassen uns mit dem unguten Gefühl des Ausgeliefertseins zurück. Dabei gerät in der Diskussion um die Legitimität solchen Handelns leicht ein wichtiger Aspekt aus dem Blick, der eine nähere Betrachtung verdient.

Es steht außer Frage, dass ein Nachrichtendienst mit ausreichenden personellen, finanziellen und gesetzlichen Möglichkeiten fast jede Information gewinnen kann. IT-Sicherheitsmaßnahmen können das erschweren, aber nicht verhindern, denn es gibt wirksame klassische nachrichtendienstliche Mittel (Observation, Infiltration), die ohne Informationstechnik zum Ziel führen.

Bedeutsamer als die Frage des ‚Ob' ist hingegen die Frage des ‚Wie'. Denn die Wahl des nachrichtendienstlichen Mittels kann in einer Informationsgesellschaft weit reichende Konsequenzen haben. Entschlüsselt ein Nachrichtendienst eine kryptierte Nachricht mit Hilfe geballter Rechenleistung, ist das folgenlos für Dritte. Etwas gänzlich anderes ist es allerdings, wenn ein Nachrichtendienst von Herstellern Hintertüren in Soft- oder Hardware einbauen lässt, Einfluss auf die Standardisierung von Kryptosystemen nimmt (wie beispielsweise die Wahl Elliptischer Kurven) oder Zufallszahlengeneratoren manipuliert. In diese Kategorie gehören auch „TKÜ-Schnittstellen", die deutsche TK-Provider für das unbeobachtete Mitschneiden von Kommunikationsinhalten durch Bedarfsträger bereithalten müssen. Alle Maßnahmen dieser Art haben einen gefährlichen Seiteneffekt: Sie schaffen verborgene Angriffspunkte. Damit untergraben sie die Sicherheit der IT-Infrastruktur einer ganzen Gesellschaft.

Angesichts der wachsenden Bedeutung von IT-Infrastrukturen für moderne Gesellschaften gehören nachrichtendienstliche Mittel, die solche unverantwortlichen Kollateralschäden verursachen, völkerrechtlich geächtet. Neben dem Atomwaffensperrvertrag, der Biowaffen- und der Chemiewaffenkonvention benötigen wir daher eine UN-Cyberwaffenkonvention, die den Einbau von Backdoors in Standards, Algorithmen, Programme und Hardware unterbindet.

Inhalt

secorvo
security consulting

Security News

EU-Datenschutzreform

Mit einer beeindruckenden Zustimmung von fast 93 % hat der Innenausschuss des EU-Parlaments am 21.10.2013 den konsolidierten Entwurf der EU-Datenschutzgrundverordnung angenommen. Nun geht der Verordnungsentwurf in die Verhandlung mit EU-Rat und EU-Kommission.

Neben der Neuregelung der Bestellungspflicht eines Datenschutzbeauftragten, die für alle Firmen gelten soll, die Daten von mehr als 5.000 Betroffenen verarbeiten, ist vor allem die geplante Bußgeldhöhe beachtlich: Bis zu 100 Mio. Euro respektive 5 % des Jahresumsatzes sollen künftig als Bußgeld verhängt werden können.

Als Folge der NSA-Enthüllungen ist auch die so genannte Anti-FISA-Klausel (*Foreign Intelligence Surveillance Act*) wieder enthalten, die auf Druck der USA entfernt worden war. Sie regelt, dass europäische Unternehmen private Daten von EU-Bürgern nur dann an Drittstaaten (außerhalb der EU) weitergeben dürfen, wenn es hierfür eine eindeutige gesetzliche Grundlage in Europa gibt. Zudem soll Profiling ausdrücklich unter den Einwilligungsvorbehalt des Betroffenen gestellt werden. Schließlich ist die Einführung einer neuen EU-Datenschutzaufsicht vorgesehen.

Nicht alles aus dem Entwurf wird nach den Verhandlungen mit den Mitgliedstaaten und der EU-Kommission übrig bleiben. Der ehrgeizige Plan ist jedoch, die Verhandlungen bis Mai 2014 zum Abschluss zu bringen. Damit könnte die EU-Datenschutzreform noch vor der Europawahl Gesetzeskraft erlangen.

ISO 2700{1,2} runderneuert

Am 04.10.2013 hat die ISO nach acht Jahren eine runderneuerte Version des ISMS-Standards ISO 27001 veröffentlicht. Durch die Überarbeitung wurde der ISO/IEC 27001:2013 an andere Managementstandards angeglichen. Zudem wurden viele Anpassungswünsche aus den vergangenen Jahren berücksichtigt, so dass nun an vielen Stellen des Standards klarere Begrifflichkeiten verwendet werden als in der Vorgängerversion. Augenfällig ist der Verzicht auf den *Plan-Do-Check-Act*-Zyklus: Dabei ist das Prinzip nicht verschwunden, wird jedoch nicht mehr explizit erwähnt – die Grundidee liegt dem Standard weiterhin zu Grunde.

Gleichzeitig mit dem ISO 27001 wurde ein deutlich veränderter ISO/IEC 27002:2013 veröffentlicht. Die neue Version des ISO 27002 empfiehlt einen Satz von 114 *Controls*, aufgeteilt auf 35 *Control Objectives*. An vielen Stellen wurde offensichtlich aufgeräumt, allerdings ist die neue Ordnung nicht immer intuitiv. So fragt man sich z. B., warum der Abschnitt ‚*Mobile devices and teleworking*' unter ‚*Organization of information security*' angesiedelt wurde. Eine Hilfestellung bei der Einarbeitung in die Neuauflage der beiden Standards bietet der „Transition Guide" des britischen BSI.

EU-Krypto-Empfehlungen

Am 29.10.2013 hat die Enisa eine Empfehlung zu Kryptoalgorithmen, Schlüssellängen und Krypto-Protokollen veröffentlicht. An dem 96seitigen Report wirkten namhafte europäische Kryptologen wie Vincent Rijmen (Autor des AES), Arjen Lenstra und Christoph Paar mit. Zwar hätte die 27seitige Literaturübersicht z. B. zu Gunsten eines Hinweises auf *Perfect Forward Secrecy* bei TLS etwas kürzer ausfallen dürfen. Aber in Verbindung mit der Übersicht von Damien Giry zu den gängigen Schlüssellängen-Empfehlungen und den in den SSN 9/2013 vorgestellten NIST-Empfehlungen zu TLS vom 24.09.2013 bietet das Dokument eine gute Übersicht über die derzeit als sicher geltenden Kryptoverfahren und die zu empfehlende Parametrisierung.

Web of the Living Dead

Am 14.10.2013 publizierte der Forscher Georg Lukas seine Hintergrund-Analyse der Default-Präferenz schwacher SSL/TLS-Cipher-Suites in neuen Android-Versionen. Die Tatsache an sich ist noch kein Beinbruch. Bei näherem Hinsehen zeigt sich aber exemplarisch, wie es durch (vorgeschobene?) Anforderungen nach (Rückwärts-)Kompatibilität und die nicht hinterfragte Übernahme veralteter Vorgaben dazu kommen kann, dass die Sicherheitskonfiguration aktueller Systeme einen seit zehn Jahren überholten Stand der Technik widerspiegelt.

Drei Lehren lassen sich daraus ziehen: Erstens dürfen Anwendungsentwickler in Sicherheitsbelangen nicht blind davon ausgehen, dass das genutzte System oder Framework „es schon richtig macht". Zweitens: Es gibt für Nachrichtendienste – gerade bei Open-Source-Software – subtilere Methoden als Hintertüren einzubauen: Sorge dafür, dass es neben dem richtigen noch einen „unverzichtbaren" alternativen Weg gibt, Sicherheit zu konfigurieren – und mache es Entwicklern und Anwendern möglichst einfach, letzteren zu wählen.

Und drittens: Manchmal muss man alte Zöpfe zügig abschneiden, um in Sachen Sicherheit voran zu kommen – auch wenn es weh tut. Zur Übung sei empfohlen, einmal im Browser (wie in SSN 9/2013 beschrieben) RC4 zu deaktivieren und dann die Webseiten von BSI, BNetzA und BND zu besuchen.

Nichtflüchtiger Speicher

Am 08.10.2013 wurde Release 2.3 des Open-Source-Tools für Speicher-Forensik Volatility für den letzten Feinschliff freigegeben. So umfasst Volatility nun Profile für die Hauptspeicheranalyse bis Windows 7 und Server 2012. Neue Window-Plugins erkennen und extrahieren Einträge des *Master File Table* von NTFS-Dateisystemen und des *Master Boot Records*; damit können auf der Festplatte gelöschte Indexeinträge rekonstruiert und der Nachweis erbracht werden, dass Daten im Dateisystem existierten, die mit klassischen ‚Post-Mortem'-Forensikwerkzeugen nicht mehr auffindbar sind. Mit dem Carving-Plugin filescan kann man aus dem Hauptspeicher einen großen Teil zuvor geladener Dateien zurückgewinnen – auch wenn die Quelle (SD-Karte, USB-Stick) nicht mehr verfügbar ist. Und mit etwas Aufwand lässt sich ein Plugin zur Extraktion von Bitlocker-Schlüsseln erstellen.

Ebenfalls neu ist die Unterstützung der Versionen 10.5 bis 10.8.3 von Mac OSX; eine iOS-Untertützung fehlt allerdings noch. Dafür kann die VMware-Hauptspeicheranalyse nun auch auf States (.vmss) und Snapshots (.vmsn) erfolgen.

Erneut hat Volatility die Meßlatte für kommerzielle Forensik-Werkzeuge deutlich höher gelegt. Der Einstieg in die Nutzung des freien Tools wird unterstützt von Cheat-Sheets, die auch einem Forensik-Laien erste Analysen erlauben.

Fingerabdrücke auf Reisen

Bereits vor der Einführung waren der elektronische Reisepass (ePass) und die zugrunde liegende EU-Verordnung umstritten. Im Kern der Kritik stand die Zwangserhebung von Fingerabdrücken als biometrisches Sicherheitsmerkmal, das vor Betrug schützen soll. Ein Bochumer bestritt die Zulässigkeit dieses Vorgehens und klagte gegen die Stadt und die Erfassung seiner Fingerabdrücke. Das Verwaltungsgericht Gelsenkirchen hatte Zweifel an der Rechtmäßigkeit der EU-Verordnung und legte den Fall dem Europäischen Gerichtshof (EuGH) zur Vorabentscheidung vor.

Am 17.10.2013 fällte der EuGH das Urteil. Nach Ansicht der Richter ist die Speicherung von Fingerabdrücken zwar ein Eingriff in die Privatsphäre, im Kampf gegen Betrug sei dieser aber gerechtfertigt. Damit wurde auch die Rechtmäßigkeit der EU-Verordnung bestätigt.

Heimlich, still und leise …

… ist auf der Webseite des BSI die 13. Ergänzungslieferung der IT-Grundschutzkataloge als Online-Version erschienen. Damit stehen einige lang ersehnte Bausteine wie Windows 7-Client, Windows Server 2008 und Webanwendungen bereit. Eine weitere wesentliche Neuerung ist die durchgängige Einführung von Prüffragen, die auch als Basis für Zertifizierungsaudits dienen können. Eine Zusammenfassung der Neuerungen gibt einen guten Überblick über alle Änderungen.

Secorvo News

Auf dem Laufenden

Es gibt verschiedene Möglichkeiten, sich hinsichtlich der aktuellen Entwicklungen der Informationssicherheit auf dem Laufenden zu halten. Als Leser der Secorvo Security News kennen Sie schon eine sehr effiziente Möglichkeit. Eine weitere ist der Besuch des Seminars „IT-Sicherheit heute", welches Secorvo College vom **12.–14.11.2013** in Karlsruhe anbietet. Aktuelle Bedrohungen, konkrete Risiken und Best Practice-Lösungswege stehen in diesem Kompaktseminar im Vordergrund. Noch wenige Plätze sind frei.

Unseren geballten Erfahrungsschatz aus 15 Jahren erfolgreichen PKI-Projekten, von Konzeption über Aufbau bis zum Betrieb, haben wir im Seminar PKI (**19.–22.11.2013**) gebündelt – ein Leckerbissen für alle, die sich mit Public Key-Infrastrukturen beschäftigen. Auch hier sind nur noch wenige Plätze verfügbar. Unser Seminarangebot, alle Termine des Jahres 2014 und eine Online-Anmeldung finden Sie unter http://www.secorvo.de/college.

Wer hat, der hat.

„Software Asset Management für Kenner" ist das Thema des nächsten KA-IT-Si-Events am **07.11.2013** um 18 Uhr im Raum TelemaxX des CyberForum e.V. in Karlsruhe. Marcel Lepkojis (CONNECT Karlsruhe GmbH) wird in seinem Vortrag Sicherheitsaspekte des *Software Asset Managements* vorstellen und Schutzmaßnahmen empfehlen. Anschließend gibt es – wie gewohnt –Gelegenheit zum „Buffet-Net(t)working". Wir freuen uns auf Ihre Anmeldung!

Die Zukunft ist mobil

Im Zentrum des diesjährigen Future IT-Kongresses am **14.11.2013** im Tagungszentrum der Buhlschen Mühle in Ettlingen, der sich mit allen Facetten des mobilen IT-gestützten Arbeitens befasst, stehen Datenschutz- und Sicherheitsaspekte des Mobile-, Cloud- und Social-Computing. Die begleitende Fachausstellung lädt zum Gespräch und Erfahrungsaustausch mit den Anbietern und Kongressteilnehmern (Anmeldung).

Veranstaltungshinweise

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

November 2013	
04.-08.11.	CCS 2013 (ACM SIGSAG, Berlin)
07.11.	Wer hat, der hat. (KA-IT-Si, Karlsruhe)
08.11.	Sicherheitsmanagement für mobile Geräte (GI/SECMGT, Frankfurt)
12.-14.11.	IT-Sicherheit heute (Secorvo College, Karlsruhe)
13.-15.11.	37. DAFTA (GDD, Köln)
14.11.	Future IT-Kongress 2013 (AppSphere AG, Ettlingen)
18.-21.11.	OWASP AppSec USA 2013 (OWASP Foundation, New York)
19.-22.11.	PKI (Secorvo College, Karlsruhe)
21.-22.11.	DeepSec ISDC 2013 (DeepSec GmbH, Wien)
Dezember 2013	
02.-03.12.	IsSec/ZertiFA 2013 (COMPUTAS Gisela Geuhs GmbH, Berlin)
10.-11.12.	2. DFN Workshop Datenschutz (DFN-CERT Services GmbH, Hamburg)
27.-30.12.	30th Chaos Communication Congress (30C3) (Chaos Computer Club, Hamburg)
Januar 2014	
21.-23.01.	Omnicard 2014 (in TIME berlin, Berlin)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Hans-Joachim Knobloch, Christoph Schäfer, 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