secorvo
security consulting

Secorvo Security News

Januar 2011

Hornberger Schießen

Die Reaktionen sind vorhersagbar: CEOs bekommen beim Thema „Cloud Computing“ glänzende Augen, Datenschützer Bauchgrimmen. Hier die erwarteten Einsparungen durch Bedarfsabrechnung statt pauschaler Lizenzkosten, günstige Thin Clients und vorkonfigurierte Software mit zentraler Pflege, dort die Ungewissheit, welche Daten eigentlich wo, wie und von wem verarbeitet werden – unvorstellbar, dass unter solchen Bedingungen eine rechtskonforme Auftragsdatenverarbeitung (schriftlicher Vertrag, Anweisung der Schutzmaßnahmen, Kontrolle des Auftragnehmers) möglich ist.

Tatsächlich sind die Auswirkungen des Cloud Computing-Konzepts schon heute sichtbar. Wer eine Suchmaschine für sich arbeiten lässt, einen Online-Routenplaner nutzt oder seine Kontakte in einem „Social Network“ pflegt, zahlt mit der Preisgabe personenbezogener Informationen. Auch Angreifer dürften sich nicht lumpen lassen und nutzen wahrscheinlich bereits verteilte Rechenpower, wie das Beispiel von Thomas Roth (siehe „Security News“) zeigt.

Bei genauerer Betrachtung werden die Fronten jedoch unscharf. So dürften viele Schutzmechanismen wie Virenschutz, Spam-Abwehr oder Patch-Services bei zentralen Diensten deutlich aktueller und wirksamer sein als in vielen heutigen IT-Infrastrukturen. Umgekehrt würden interne Informationen ungefiltert die Unternehmen verlassen – eine gruselige Vorstellung für die meisten Mittelständler. Dafür stiege der Schutz vor anderen Informationsabflüssen wie dem Verlust mobiler Geräte, wenn Unternehmensdaten nicht mehr lokal gespeichert sondern nur „in der Wolke“ zugänglich wären.

Voraussichtlich wird auch dieser Hype enden wie das Hornberger Schießen: Nach viel aufgewirbeltem Staub werden die Unternehmen versuchen, durch den Aufbau von Private Clouds die Vorteile zentraler Services mit einer kontrollierten Datenverarbeitung zu verknüpfen – nicht zur Freude der Service-Anbieter, die bereits neue Geschäfte wittern.

Inhalt

secorvo
security consulting

Security News

Sandkastenleck

Gleich am 04.01.1010 hat Billy Riot in seinem Blog zwei Schwachstellen in einer der Sandboxes von Adobes Flash-Player veröffentlicht. Wenngleich die Dokumentation anderes verspricht, ist damit ein Zugriff auf eine lokale URL und so die Übermittlung von Informationen möglich. Bei der Analyse der zweiten Schwachstelle zeigt sich, dass Adobe sich zur Filterung der Protokolle für eine Blacklist entschieden hat. Damit sind alle Protokolle, die für ungefährlich gehalten werden, auch für Zugriffe auf beliebige Systeme im Internet zugelassen. Auf diese Weise lassen sich aus der Flash-Sandbox heraus beliebige Daten an einen Server im Internet übermitteln.

Beunruhigend, dass Adobe auf die von Julia Wolf am 30.12. 2010 in Ihrem Vortrag auf dem Chaos Computer Congress 2010 (27C3) beschriebenen prinzipiellen Schwächen des Dateiformats PDF mit dem Hinweis auf ein Sicherheitsfeature in der aktuellen Version ihres PDF-Readers reagierte: einer Sandbox. Damit hat Adobe schon Erfahrung ...

Krypto-Umbruch vertagt

Der 2005 erschienenen und zuletzt 2007 überarbeiteten NIST SP 800-57 zufolge hätte der 31.12.2010 das Ende aller Kryptoalgorithmen und Schlüssellängen der „80-Bit-Äquivalent"-Klasse markieren sollen: 1024-Bit-RSA und SHA-1 für digitale Signaturen sowie 2-Key-Triple-DES für die Verschlüsselung.

Die damaligen Abschätzungen waren jedoch sehr konservativ - und seither waren keine spektakulären Erfolge bei der Kryptoanalyse zu verzeichnen. So erteilt die am 13.01.2011 erschienene NIST SP 800-131A diesen Algorithmen nochmals drei bzw. fünf Jahre Gnadenfrist. Dazu wurde zwischen „acceptable" und „disallowed" die Kategorie „deprecated" eingeführt – frei übersetzt: „eigentlich sollst Du nicht, aber wenn es partout nicht anders geht und Du Dir über die Risiken im klaren bist ...". Und bei Verwendung des 2-Key-Triple-DES muss nach maximal 8 MByte Daten der Schlüssel gewechselt werden - wie praktikabel das in der Praxis ist, wenn eine Dateilänge dieses Limit übersteigt, sei einmal dahin gestellt.

Zwar richten sich die NIST-Empfehlungen formal nur an US-Bundesbehörden; sie gelten aber gemeinsam mit dem am 22.12.2010 in der Fassung für 2011 erschienenen SigG-Algorithmenkatalog der BNetzA als Referenz für den Stand der Technik bei Kryptoalgorithmen und Schlüssellängen.

Simples Foto-Tagging

... ist das Thema eines auf den ersten Blick unscheinbaren Eintrags vom 16.12.2010 im Facebook-Blog. Als erstes „Soziales Netzwerk" beginnt Facebook damit, im großen Stil biometrische Informationen über seine Mitglieder (und darüber hinaus) zu sammeln: Die Kombination von automatischer Gesichtserkennung und vereinfachter Markierung von Personen in Fotos wird Facebook dank der Beliebtheit des Fotodienstes absehbar mit einer der größten personenbezogenen Bilddatenbanken ausstatten.

Die Datenbank wird allen europäischen Datenschutzbestimmungen zum Trotz auch Aufnahmen von Personen enthalten, die weder der Bereitstellung eines Bildes in Facebook noch der Markierung zugestimmt haben – möglicherweise nicht einmal Nutzer des „Sozialen Netzwerks" sind. Das wird zweifellos Begehrlichkeiten wecken – sofern diese Begehrlichkeiten nicht bereits eins der Motive für diesen Datenbankaufbau darstellen.

Für die Facebook-Nutzer ist dies ein Danaergeschenk, das Erziehungsberechtigte an die Warnung Laokoons in Vergils Aeneis erinnern sollte: „Quidquid id est, timeo Danaos et dona ferentes."[1] Die Geschichte hat ihm Recht (und Schadsoftware einen illustren Namen) gegeben.

Im Glashaus

... sitzend warf der Hamburger Datenschutzbeauftragte Prof. Johannes Caspar am 10.01.2011 mutig mit Steinen: Bei seiner für Google Deutschland zuständigen Datenschutzaufsichtsbehörde stand nach einer Reihe von Beschränkungsforderungen an Street View und dem Entwurf eines auf Google zugeschnittenen neuen BDSG-Paragrafen 4a (SSN 5/2010) nun Google Analytics auf der Agenda.

Bereits am 26./27.11.2009 hatte der Düsseldorfer Kreis einen Entschluss über Zulässigkeitsbedingungen für Trackingdienste (SSN 8/2010) gefasst. Im Wesentlichen wurden darin die verkürzte, anonyme Verarbeitung von IP-Adressen beim Tracking, die Möglichkeit zum Widerspruch und eine ausreichende Information in den Datenschutzerklärungen gefordert.

Da Google dem eher verhalten nachgekommen war, hatte Caspar angekündigt, nun mit Bußgeldern gegen Nutzer von Google Analytics vorgehen zu wollen. Entgangen war ihm jedoch, dass seine eigene Website sowie die der Stadt Hamburg gleich

[1] *Was auch immer es ist, ich fürchte die Danaer und ihre überbrachten Geschenke.*

mehrere nicht gesetzeskonforme Trackingdienste – darunter Google Analytics – verwendete. Nach seiner eher unglücklichen Verteidigung auf der Blogseite des Rechtsanwaltes Stadler ging die Webseite der Aufsichtsbehörde dann „trackerfrei“ offline.

Dem Datenschutz wird diese Komödie nicht gedient haben. Obwohl die Nutzung von Google Analytics weiterhin gegen geltendes Datenschutzrecht verstößt, dürfte glaubwürdigen Maßnahmen der Aufsichtsbehörden damit bis auf weiteres der Boden entzogen sein.

Undurchsichtige Wolke

Das Verlagern von Rechenaufgaben in die Cloud ist nicht nur für Unternehmen ein Thema. Am 10.01.2011 beschrieb Thomas Roth, wie diese „Demokratisierung von Rechenleistung“ genutzt werden kann, um für wenige Euro per Wörterbuchangriff in der Cloud das WLAN-Passwort (WPA-PSK) des Nachbarn zu knacken, und präsentierte auf der Black Hat DC am 19.01.2011 seine „Cloud Cracking Suite“, mit der die Wolke zum Hacker-Tool mutiert.

Zwar verdankte er den schnellen Erfolg beim Nachbarn einem schlecht gewählten Passwort – dennoch wirft der Fall eine wichtige Frage auf: Muss ein Cloud-Anbieter prüfen, zu welchem Zweck sein Kunde die Rechenleistung nutzt? Und falls ja: Wie kann er das beurteilen? Eine ähnliche Frage stellte sich beim SETI@Home und dem inzwischen eingestellten RC5-Wettbewerb. Zwar dürfte jede „missbräuchliche“ Verwendung der Ressourcen in den AGB der meisten Cloud-Anbieter untersagt sein – in der Praxis ist jedoch eine tatsächliche Bewertung der Nutzung unmöglich.

Mit Cloud-unterstützten Angriffen muss daher zukünftig verstärkt gerechnet werden. Das könnte die eine oder andere Annahme über die einem Angreifer typischerweise zur Verfügung stehende Rechenleistung Makulatur werden lassen.

Secorvo News

Smart, smarter, am smartesten

Das „intelligente Stromnetz“ (vulgo: „Smart Grid“) verspricht in vielerlei Hinsicht Vorteile: So sollen sich Spitzen in Stromerzeugung und -abnahme verringern lassen, wodurch wiederum eine gleichmäßigere Bereitstellung von Energie und der Verzicht auf Kraftwerke ermöglicht werden soll.

Doch eine Beeinflussung von Geräten birgt auch enormes Missbrauchspotenzial, wie die Analyse von Lastprofilen, die detaillierte Einblicke in die Vorgänge in einem Haushalt erlauben, bis zur unautorisierten Fernsteuerung elektrischer Geräte.

In seinem Vortrag über Sicherheits- und Datenschutzaspekte des Smart Grid auf dem nächsten KA-IT-Si-Event am 24.02.2011 im Schlosshotel Karlsruhe beleuchtet Klaus J. Müller beide Seiten. Um Anmeldung wird gebeten.

Lesestoff

Nicht nur in den Security News, sondern auch in einschlägigen Fachzeitschriften meldet sich Secorvo regelmäßig zu Wort. So hat sich in den vergangenen Monaten Michael Knopp zu WLAN-Haftung (DuD 9/2010) und der Datenschutzherausforderung Webtracking (DuD 11/2010) geäußert, Dirk Fox zur betriebswirtschaftlichen Bewertung von Security Investments in der Praxis (DuD 1/2011) Stellung genommen und Kai Jendrian und Klaus J. Müller Features und Maßnahmen gegen Browser-Angriffe beleuchtet (iX 2/2011).

In Kürze wird ein Beitrag zu Herausforderungen bei IPv6 von Dr. Safuat Hamdy und Hans-Joachim Knobloch in der <kes> (Ausgabe 1/2011) erscheinen.

Eine Übersicht der mehr als 350 Publikationen von Secorvo finden Sie auf unserer Webseite.

Neue Seminare

Mit dem Thema Web-Anwendungs-Sicherheit erweitern wir ab Frühjahr 2011 unser Seminarangebot. Jedem, der Web-Anwendungen entwirft, entwickelt, spezifiziert, oder prüft bietet das Seminar alles Wichtige über die Bedrohungen, denen Web-Awendungen ausgeliefert sind, sowie Lösungen, die einen verlässlichen Schutz bieten.

Zudem werden relevante rechtliche Rahmenbedingungen und insbesondere Datenschutzaspekte beleuchtet. Am 12. und 13.04.2011 startet das Seminar „Verlässliche Web-Anwendungs-Sicherheit“.

Ab diesem Jahr werden die unabhängige Prüfung und Zertifizierung zum T.I.S.P. (TeleTrusT Information Security Professional) vom TÜV PersCert durchgeführt, einem Tochterunternehmen des TÜV Rheinland. Die nächste T.I.S.P.-Schulung und -Prüfung bieten wir vom 23.03. bis 02.04.2011 an.

Programme und Online-Anmeldung aller Seminare unter http://www.secorvo.de/college.

Veranstaltungshinweise

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

Februar 2011	
01.-02.02.	Smart Grid Symposium (Secorvo, Ettlingen/KA)
02.-03.02.	21. SIT-SmartCard Workshop (SIT, Darmstadt)
08.-10.02.	CPSSE-Schulung (Secorvo College)
15.-16.02.	18. DFN-Workshop Sicherheit in vernetzten Systemen (DFN-CERT, Hamburg)
März 2011	
01.-05.03.	CeBIT (Deutsche Messe, Hannover)
22.-24.03.	Sicherheitsmanagement heute (Secorvo College)
28.03.-01.04.	T.I.S.P.-Schulung (Secorvo College)
April 2011	
04.-06.04.	IT-Sicherheitsaudits in der Praxis (Secorvo College)
07.-08.04.	Datenschutzaudit: Best Practice (Secorvo College)
12.-13.04.	Datenschutztage 2011 (FFD Forum für Datenschutz, Frankfurt)
Mai 2011	
10.-13.05.	Public Key Infrastrukturen (PKI) (Secorvo College)

Fundsache

Das US-amerikanische NIST hat dem Thema Datenschutz und Datensicherheit beim Cloud Computing ein 60seitiges Dokument gewidment: „Guidelines on Security and Privacy in Public Cloud Computing“, erschienen am 28.01.2011 als SP 800-144 (Draft) zur Kommentierung.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Kai Jendrian, Hans-Joachim Knobloch, Michael Knopp, Klaus J. Müller

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