secorvo
security consulting

Secorvo Security News

März 2014

Im Netz der Spinne

Die Raumsonde Deep Space 1 wurde am 24.10.1998 zur Erforschung des Asteroiden (9969) Braille gestartet. Am 22.09.2001 nahm sie spektakuläre Bilder des Kometen 19P/Borrelly auf; am 18.12.2011 wurde sie schließlich deaktiviert.

Auch der israelische Gesichtserkennungsdienst face.com machte schon spektakulär auf sich aufmerksam. Im Juli 2011 gelang die Aufsehen erregende Erkennung von Emotionen, und im März 2012 die automatische Alterserkennung. Nach langer Freundschaft war die am 18.06.2012 von face.com bekannt gegebene Übernahme durch Facebook ein logischer Schritt. Euphorisch jubelte die Pressemitteilung: „By working with Facebook directly, and joining their team, we'll have more opportunities to build amazing products that will be employed by consumers – that's all we've ever wanted to do." Inzwischen erreicht die DeepFace getaufte Software mit Hilfe eines neuronalen Netzwerkes eine Treffergenauigkeit von 97,25 % bei der Identifikation von Personen auf einem Bild. Das menschliche Gehirn ist nur unwesentlich erfolgreicher – sofern es ebenso viele Personen kennt wie DeepFace...

Zwar wehrten sich die europäischen Datenschützer zuletzt erfolgreich gegen Facebooks Gesichtserkennung – frei nach Ovids Empfehlung in seiner Remedia amoris, die Liebe im Keim zu ersticken („Wehret den Anfängen"). Allerdings könnte es dafür bereits zu spät sein.

Denn anders als die Raumsonde Deep Space 1 macht DeepFace seine Analysen nicht im Orbit, sondern auf der Erde. Und es wäre sicherlich naiv zu hoffen, dass die Mission von DeepFace nach dreizehn Jahren durch Deaktivieren beendet wird. Denn DeepFace ist kein Forschungsprojekt, sondern eine Einnahmequelle, die perfekt in Mark Zuckerbergs selbst erklärter Mission passt, die Welt zu vernetzen.

Ein Schelm, wer dabei an eine Spinne denkt.

Inhalt

secorvo
security consulting

Security News

Das NIST und das Vertrauen

NSA-Enthüllungen und der Verdacht einer Backdoor im NIST-Standard SP 800-90A für Zufallszahlengeneratoren (siehe SSN 11/2013) haben die Integrität des NIST-Entwicklungsprozesses für kryptographische Standards in Frage gestellt.

In einem öffentlichen Schreiben vom 17.02.2014 betont das NIST nun die Bedeutung der Unterstützung durch die weltweite Krypto-Gemeinde für die Akzeptanz von kryptographischen Algorithmen und bittet im Rahmen der bereits im November 2013 initiierten Überprüfung des Standardentwicklungsprozesses um Kommentare.

Die Prinzipien und Prozeduren sind als Draft NIST Interagency Report 7977 öffentlich verfügbar. Dazu zählen insbesondere die Transparenz, die Offenheit und der Ausgleich der Interessen unterschiedlicher Gruppen. Als Prozeduren kommen beispielsweise internationale kryptographische Wettbewerbe und die Veröffentlichung von Standardentwürfen zum Einsatz.

Allerdings betont das NIST, auch weiterhin eng mit der NSA (einer der Interessensgruppen) zusammen zu arbeiten, da Mitarbeiter der NSA über immense Erfahrung in der Kryptographie verfügen und das NIST per Gesetz verpflichtet ist, bei der Standardentwicklung die NSA zu befragen.

Bis zum 18.04.2014 können Kommentare eingereicht werden. Eine 90 Seiten umfassende Kommentarsammlung zum NIST SP 800-90A ist bereits verfügbar.

Widerspruchsrecht bei Piwik

Auch wenn die IP-Adressen von Seitenbesuchern mit dem Webanalyse-Tool Piwik nur anonymisiert erfasst werden, muss der Seitenbesucher eine Möglichkeit zum Widerspruch haben. Das entschied das LG Frankfurt am 18.02.2014 (Az. 3-10 O 86-12). Ein entsprechender Hinweis ist in die Datenschutzerklärung der Webseite aufzunehmen.

Damit liegt ein weiteres Urteil vor, welches die Möglichkeit einer wettbewerbsrechtlichen Abmahnung für Verstöße gegen das Telemediengesetz bejaht. Bereits das OLG Hamburg hatte mit seinem Urteil vom 27.06.2013 einen Verstoß gegen datenschutzrechtliche Informationspflichten ähnlich bewertet.

Folgt man dem Frankfurter Urteil, so muss jeder Webseiten-Betreiber „zu Beginn des Nutzungsvorgangs“ auf den Einsatz eines Webanalyse-Tools hinweisen, was bei enger Auslegung wohl bedeutet, dass sich vor dem Öffnen einer Webseite ein Pop-up-Fenster öffnen muss, welches den Besucher informiert. So etwas sieht kaum eine Webseite vor.

Dies ist eine ähnliche Forderung, wie sie die in Deutschland noch nicht umgesetzte „Cookie-Richtlinie“ (2009/136/EG) der EU enthält, die eine Einwilligung (Opt-in) für Cookies verlangt. Webseitenbetreiber sollten diese Entwicklungen im Auge behalten und in jedem Fall ihre Datenschutzerklärung aktuell und gut erreichbar halten.

Full Disclosure ist tot – es lebe...

Am 19.03.2014 hat John Cartwright, Gründer der im Jahr 2002 ins Leben gerufenen Mailing-Liste Full Disclosure, per E-Mail an die Mailing-Liste bekannt gegeben, dass er den Dienst einstellen wird. In der Liste wurden in den letzten zwölf Jahren viele wichtige Hinweise auf Sicherheitsschwachstellen anonym veröffentlicht. Die Security-Community wird diese wichtige Informationsquelle vermissen.

Das dachte sich auch Gordon Lyon – und kündigte am 25.03.2014 an, die Liste fortzuführen. Allerdings ist dafür eine Neuanmeldung erforderlich.

Datenschutzaufsicht zu BYOD

Bereits am 06.02.2014 hat der Hamburgische Landesdatenschutzbeauftragte seinen Jahresbericht für die Amtsjahre 2012/2013 vorgelegt und anhand der berichteten Vorkommnisse zu einer Vielzahl praktischer Datenschutzfragen Stellung genommen. Ein längerer Abschnitt ist dem Thema „Bring your own device“ (BYOD) gewidmet.

Die warnende Analyse des Berichts basiert auf der Prüfung der Container-Lösung DME-Extractor für iPhone und Android-Geräte in der hamburgischen Verwaltung. Grundsätzlich wird BYOD danach als sehr risikoreich eingeschätzt; der Bericht warnt vor einer Unterschätzung des Schutzbedarfs. Gefordert wird als Stand der Technik wenigstens ein Mobile Device Management, eine Container-Lösung, eine umfassende Nutzungsregelung für den Geräteeinsatz, vor allem bezüglich der Container-Löschung im Falle einer Wartung durch Dritte.

Vor einer Freigabe des Verfahrens wird ein umfassender Penetrationstest empfohlen. Die zum Bezug der verfahrensnotwendigen App (unter Android) erforderliche Registrierung des Nutzers bei Google wird wegen der verbundenen Datenübertragung von Beschäftigtendaten an Google als inakzeptabel angesehen. Allgemein seien die für die private Freizeitnutzung ausgelegten Geräte für die geschäftliche Verarbeitung von Daten mit möglicherweise hohem Schutzbedarf ungeeignet.

Vor dem Hintergrund der aufgezeigten Bedenken mutet das Résumé, der Einsatz sei sehr ‚risikoreich', inkonsequent an. Wünschenswert wäre eine klare Feststellung gewesen, dass der Einsatz bei Nichterfüllung der aufgestellten Anforderungen schlicht als rechtswidrig angesehen werden muss.

Die Stellungnahme kündigt eine abgestimmte Wertung der Datenschutzbeauftragten des Bundes und der Länder an. Diese wird sich hoffentlich in der Frage der Zulässigkeit eindeutiger festlegen, um Unternehmen eine rechtssichere Orientierung für den Datenschutz konformen Umgang mit BYOD-Bestrebungen zu geben.

Nachweis des Nicht-Ereignisses

Der BGH hat in einem Urteil vom 19.02.2014 seine Rechtsprechung zur Beweisführung bei streitigen Faxzugängen präzisiert. Die Vorinstanz hatte den Zugang – trotz vorgelegter Sendeberichte – ohne weitere Beweisaufnahme verneint, da der OK-Vermerk des Sendeprotokolls lediglich ein Indiz darstelle, aber keinen Anscheinsbeweis begründe.

Der BGH führt nun aus, dass bei vorliegendem Sendeprotokoll ein einfaches Bestreiten des Zugangs nicht ausreicht. Der Empfänger hat im Rahmen der so genannten sekundären Darlegungslast wenigstens darzustellen, welches Gerät er nutzt, ob dieses eine Verbindung verzeichnet hat, und – soweit vorhanden – sein Empfangsjournal vorzulegen. Anhand dieser Angaben hat das Gericht dann eine Beweiswürdigung vorzunehmen.

Einen Zuwachs an Rechtssicherheit bringt das Urteil jedoch weder für den Empfänger noch für den Sender. Sowohl Sendeprotokolle als auch Empfangsjournale sind regelmäßig nicht gegen Manipulationen geschützt, so dass sie nur schwache Anhaltspunkte darstellen. Das Versenden im Beisein eines Zeugen ist ein wirksamerer Beweis – umgekehrt lässt sich aber ein Nicht-Empfang schlechthin nicht bezeugen.

Da Empfangsprotokolle oft nur eine begrenzte Zeit zurückreichen und nicht wirksam gegen Manipulation geschützt werden können, und Faxgeräte zudem meist nicht nur einer Person zugänglich sind, dürfte ein wirksames Abstreiten des Empfangs in der Regel schwierig sein. Vor einer ungerechtfertigten Zurechnung schützt danach wohl nur ein vollständig digitaler Empfang mit ausführlichen und weit zurück reichenden Log-Protokollen – eine datenschutzrechtlich unschöne Lösung.

Geldfund

Die insolvente Bitcoin-Börse Mt. Gox hat am 20.03.2014 bekannt gegeben, ein Wallet mit 200.000 der vermissten 850.000 Bitcoins ‚gefunden' zu haben. Das entspricht – nach dem aktuellen Kurs – immerhin beachtlichen 90 Mio. US$. Offenbar kommen Bitcoins leicht unter die Räder: Zuletzt hatte am 27.11.2013 der britische Guardian über James Howells berichtet, der Bitcoins im Wert von 4,5 Mio. Pfund zusammen mit seiner Festplatte entsorgt hatte. Da war das Leben früher doch viel sicherer: 90 Mio. US$ in Scheinen verliert man nicht – in 50-Dollar-Bündeln wiegen diese 1,8 Tonnen.

Secorvo News

Zertifikat mit Erkenntnisgewinn

Auf rund 190 Jahre summiert sich die Berufserfahrung aus unterschiedlichen Tätigkeitsfeldern der Informationssicherheit der elf Secorvo-Referenten in der fünftägigen T.I.S.P.-Schulung. Die nächste Gelegenheit, von diesem Erfahrungsschatz als Teilnehmer eines Secorvo-T.I.S.P.-Seminars unmittelbar zu profitieren, bietet sich Ihnen **vom 19. bis 23.05.2014**.

Sicherheit ist programmierbar

Wenn grundsätzlich im Software-Entwicklungsprozess Sicherheit als wesentliches Entwurfskriterium von Anfang an berücksichtigt werden würde, dann gäbe es viele heutige Sicherheitsprobleme definitiv nicht. Doch was noch nicht ist, kann ja noch werden: Als Certified Professional for Secure Software Engineering (CPSSE) kennen Sie – oder Ihre Kollegen – die Techniken und Vorgehensweise von „Security by Design". Das nächste Seminar mit noch freien Plätzen findet statt **vom 05. bis 08.05. 2014**. (Online-Anmeldung).

Herkunft verpflichtet

"Data Provenance. Auch Daten haben ihre Geschichte." ist das Thema des nächsten KA-IT-Si-Events am **03.04.2014** um 18 Uhr im Max-Syrbe-Saal des Fraunhofer IOSB in Karlsruhe. Christoph Bier (Fraunhofer IOSB) wird in seinem Vortrag zeigen, wie die Datenschutzauskunft der Zukunft aussehen könnte. Anschließend gibt es – wie gewohnt – Gelegenheit zum „Buffet-Networking". Wir freuen uns auf Ihre Anmeldung.

Teamverstärkung

Wieder konnten wir eine Verstärkung für das Consulting-Team gewinnen: Am 01.03.2014 ist André Domnick zu uns gestoßen. Er bringt viel Erfahrung in den Bereichen sichere Softwareentwicklung und Web Application Security mit – und einen Bachelor in Information Security.

Veranstaltungshinweise

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

April 2014	
03.04.	Herkunft verpflichtet. (Karlsruher IT-Sicherheitsinitiative, Karlsruhe)
08.-09.04.	Datenschutztage 2014 (FFD Forum für Datenschutz, Wiesbaden)
09.-10.04.	Security Forum 2014 (Hagenberger Kreis, Hagenberg/AT)
Mai 2014	
05.-09.05.	CPSSE (Certified Professional for Secure Software Engineering) – Schulung und Prüfung (Secorvo College, Karlsruhe)
07.-09.05.	1st DFRWS EU Conference (DFRWS, Amsterdam/NL)
11.-15.05.	Eurocrypt 2014 (IACR, Kopenhagen/DK)
12.-14.05.	IMF 2014 (Fraunhofer IAO, Münster)
12.-16.05.	Security Engineering – Schulung & T.E.S.S.-Prüfung (Secorvo College, Karlsruhe)
14.-16.05.	15. Datenschutzkongress (Euroforum, Berlin)
19.-24.05.	T.I.S.P. - Schulung und Prüfung (Secorvo College, Karlsruhe)
21.-23.05.	Entwicklertag 2014 (VKSI, Karlsruhe)

Fundsache

Apple hat am 20.02.2014 eine aktualisierte Version der Dokumentation zur iOS Security veröffentlicht. Darin erläutert Apple viele Sicherheitsfeatures, über die bisher lediglich spekuliert werden konnte. Lesenswert.

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, Dr. Yun Ding, Dr. Safuat Hamdy, Kai Jendrian, Michael Knopp, Christoph Schäfer (Editorial), 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