secorvo
security consulting

Secorvo Security News

April 2019

High Noon

Zweifellos eine Sternstunde der Filmgeschichte: das Duell zwischen Recht und Verbrechen, vertreten durch Marshal Will Kane (Gary Cooper) und den Banditen Frank Miller. Fred Zinnemanns Film erzählt auch eine Geschichte von Feigheit und Pflichtbewusstsein, Treue und Mut – aber darum geht es hier nicht. Es ist die Unausweichlichkeit, mit der sich die Handlung von der ersten Filmminute an auf das große Finale hinbewegt, die an amerikanische Cloud-Anbieter denken lässt. Denn ganz ähnlich spitzt sich seit Jahren die Spannung zwischen ihnen und dem europäischen Datenschutzrecht zu.

Es begann mit kleinen Scharmützeln wie der Auseinandersetzung um Google Analytics (wenig überzeugend gelöst durch den AV-Kompromiss des Hamburgischen Datenschutzbeauftragten) oder den gerade vor dem EuGH verhandelten Social Media Plug-ins. Dann kamen 2013 die Enthüllungen Edward Snowdens, die das EU-Parlament zur Verabschiedung der Datenschutz-Grundverordnung (DSGVO) motivierten und dazu beitrugen, das Safe Harbor-Abkommen zu kippen – mit einem EuGH-Urteil, dessen Begründung auch den Standardvertragsklauseln den Boden entzog.

Nun drohen die Cloud-Geschäftsmodelle von Microsoft und Amazon am europäischen Datenschutzrecht zu zerschellen. Zwar reagierte Microsoft schnell: mit einem irischen Rechenzentrum, ausgereiften Verträgen und der Weigerung, einer richterlichen Anordnung Folge zu leisten, die Zugriff auf in Irland gespeicherte Daten verlangte. Da fiel ihnen am 23.03.2018 der US CLOUD Act in den Rücken, der amerikanische Unternehmen verpflichtet, im Ausland gespeicherte Daten auch ohne Rechtshilfeabkommen an US-Behörden herauszugeben – ein Verstoß gegen Artikel 48 der DSGVO. Am 07.11.2018 stellte daher die Datenschutzfolgenabschätzung der niederländischen Aufsichtsbehörde die DSGVO-Konformität von Office 365 in Frage. Fehlt noch, dass der US-EU Privacy Shield (erwartungsgemäß) vor dem EuGH scheitert. Dann ist High Noon. Mit offenem Ausgang.

Inhalt

secorvo
security consulting

Security News

Firmenprofile in Social Networks

Die für den 11.04.2019 angekündigte Entscheidung des Bundesgerichtshofes (BGH) in der Sache I ZR 186/17 („Facebook“) mutierte zu einem Aussetzungsbeschluss: Der BGH will zunächst das in Kürze fällige Urteil des EuGH über Social Media Plug-ins (namentlich: Facebook Like Buttons) abwarten. Die bereits am 19.12.2018 veröffentlichten Schlussanträge des Generalanwalts Bobek lassen erwarten, dass der EuGH von einer gemeinsamen Verantwortung ausgehen wird – was dann analog auch für Firmenprofile in Social Networks zutrifft. Solche Profile müssen daher wie Webseiten mit einem Impressum und einer Datenschutzerklärung versehen sein – mindestens als Verlinkung der entsprechenden Erklärungen der Unternehmenswebseite.

Altlasten und Seitenkanäle I

Seit 2005 kann TLS nicht nur mit Zertifikaten, sondern auch mit einem vorab vereinbarten symmetrischen Pre-Shared-Key (PSK) genutzt werden. Israelische Sicherheitsforscher haben am 05.04.2019 einen *Selfie Attack* getauften Angriff auf TLS-PSK (1.3) veröffentlicht, bei dem ein Client durch einen aktiven MITM-Angriff zum „Selbstgespräch“ veranlasst wird – was zu erheblichen Problemen auf höheren Anwendungsschichten führen kann. Entwickler (und Nutzer) betroffener Anwendungen sollten die empfohlenen Schutzmaßnahmen ergreifen oder, besser noch, TLS ausschließlich mit Zertifikaten einsetzen.

Bereits am 06.02.2019 hat eine Forschergruppe um Adi Shamir einen Angriff auf den RSA-Schlüsselaustausch in TLS beschrieben, der Seitenkanäle wie das Cache-Timing nutzt, um trotz diverser Gegenmaßnahmen in neueren Browsern und TLS-Versionen das 1998 von Daniel Bleichenbacher publizierte adaptive Angriffsschema gegen das RSA-Padding nach dem veralteten PKCS#1 v1.5 umzusetzen. Zwar ist ein solcher RSA-Schlüsselaustausch in TLS 1.3 nicht mehr zulässig. Unterstützt ein Server aber auch ältere Protokollversionen mit RSA-Schlüsselaustausch, ist ein Downgrade-Angriff auch gegen TLS 1.3 möglich. Schutz bieten eine komplette Umstellung auf TLS 1.3 oder die Nutzung von Zertifikaten auf Basis von ECC-Verfahren.

Zweifel an Office 365

Bereits am 07.11.2018 hat die niederländische Datenschutzaufsichtsbehörde eine umfangreiche Datenschutz-Folgenabschätzung zu Microsoft Office 365 veröffentlicht. Darin wurden zahlreiche Punkte beanstandet und Microsoft aufgefordert, diese bis April 2019 zu beheben. Die Probleme umfassen nicht nur technische Aspekte wie z. B. die Beobachtung, dass umfangreiche Telemetriedaten „nach Hause gefunkt“ werden, ohne dass die Nutzer dies wissen. Problematisch ist auch, dass Unternehmen mit Sitz in den USA den US-Behörden im Falle von Ermittlungsverfahren aufgrund des CLOUD Act Zugriff auch auf (Cloud-) Server in Europa gewähren müssen, selbst wenn die Voraussetzungen des Art. 48 DSGVO nicht vorliegen.

Nach einer Pressemitteilung des europäischen Datenschutzbeauftragten werden nun auch die vertraglichen Beziehungen zwischen Microsoft und den EU-Behörden überprüft. Ziel ist es herauszufinden, ob hier – wie in den Niederlanden – Datenschutzverstöße festzustellen sind und ob die Datenübermittlungen im Einklang mit Art. 48 DSGVO stehen.

Unternehmen aus Drittstaaten, die Cloud-Dienste in Europa DSGVO-konform anbieten wollen, könnten diese von einem europäischen Anbieter als Treuhänder erbringen lassen, ohne selbst Zugriff auf die Daten zu haben. Aber auch hier steckt der Teufel im Detail: Betreibt der europäische Partner eine Niederlassung in den USA, könnten die US-Behörden durch diese Hintertür zugreifen.

Altlasten und Seitenkanäle II

Auch im neuen WLAN-Sicherheitsstandard WPA3-Personal (SSN 01/2018) haben Sicherheitsforscher mehrere Mängel entdeckt und am 10.04.2019 unter dem Namen *Dragonblood* veröffentlicht, die eine Rekonstruktion des WLAN-Pre-Shared-Key ermöglichen.

WPA3-Personal ersetzt den gegen Offline-Wörterbuchangriffe anfälligen Vier-Wege-Handshake von WPA2-Personal durch SAE – auch als Dragonfly bekannt –, das derartige Angriffe verhindern soll. Um den Übergang zum neuen Protokoll zu erleichtern, definiert WPA3 einen „Transition Mode“, in dem sowohl WPA3- als auch WPA2-Clients unterstützt werden. In diesem Mischbetrieb lässt sich jedoch ein Downgrade auf WPA2 provozieren, wodurch der Angriff wieder möglich wird. Zwei weitere Dragonblood-Angriffe bedienen sich eines Timing- bzw. Cache-Seitenkanals, um den PSK über einen Wörterbuchangriff zu ermitteln. Schließlich wurde ein Downgrade-Angriff entdeckt, der das Sicherheitsniveau auf die schwächste von Client und Access Point unterstützte Diffie-Hellman-Gruppe absenkt.

Einige der Schwächen lassen sich per Software entschärfen; entsprechende Sicherheitsupdates sollten zügig installiert werden. Ein Mischbetrieb von WPA3/WPA2 sollte unbedingt vermieden werden.

secorvo
security consulting

Europäische Hilfestellung

Der Europäische Datenschutzausschuss hat am 09.04.2019 Richtlinien zur Datenverarbeitung bei Diensten der Informationsgesellschaft verabschiedet und zur öffentlichen Konsultation gestellt. In dem 14-seitigen Papier erläutert der Ausschuss seine enge Auslegung des Art. 6 Abs. 1 b) DSGVO: Mit der Erforderlichkeit zur Vertragsdurchführung sollen nur solche Verarbeitungen personenbezogener Daten legalisiert werden, ohne die der Vertrag nicht erfüllt werden kann. Dabei seien auch die Erwartungen der Betroffenen zu berücksichtigen.

Analysen des Nutzerverhaltens, Sicherheitslogs, Speicherungen zu Gewährleistungszwecken oder aufgrund von Aufbewahrungspflichten seien nicht von Abs. 1 b) umfasst, sondern erforderten andere Rechtsgrundlagen. Zweifellos eine zutreffende Klarstellung. Daraus folgt jedoch, dass die Betroffenen gemäß Art. 12 ff DSGVO über diese zu informieren sind. Exzessive Verarbeitungen werden sich so kaum verhindern lassen – die Laienverständlichkeit der Datenschutzerklärung dürfte jedoch leiden.

Hambacher Manifest

Die 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat am 03.04.2019 unter anderem Anforderungen an die datenschutzgerechte Entwicklung von KI-Anwendungen unter dem Titel „Hambacher Erklärung zur Künstlichen Intelligenz“ verabschiedet. Die Anforderungen starten mit dem Grundsatz aus Art. 22 DSGVO, rechtlich relevante Entscheidungen nicht ausschließlich auf automatisierte Prozesse zu stützen sowie auch für Trainingsdaten das Zweckbindungsgebot zu beachten. Datenminimierung, die Entwicklung technischer und organisatorischer Standards, die klare Festlegung von Verantwortlichkeiten sowie der Anspruch, die Entwicklung auch politisch zu steuern und die regelmäßige Durchführung von Datenschutz-Folgenabschätzungen sind weitere Anforderungen.

Kein revolutionärer Wurf – zumal das Mantra der Transparenz nicht kritisch hinterfragt wird. Gerade bei KI-Anwendungen sind Zweifel angebracht, ob diese tatsächlich kurz, verständlich und für den Betroffenen nachvollziehbar dargestellt werden können – und ob dies der richtige Ansatz zum Schutz der Betroffenenrechte ist.

Secorvo News

200 Security News

Sie lesen gerade die 200. Ausgabe der Secorvo Security News. 800 Seiten mit rund 1.500 Nachrichten, die wir für Sie recherchiert, ausgewählt und formuliert haben, ungezählte fachliche Diskussionen und Tassen Kaffee liegen hinter uns. Die Security News haben mehr Leser als die meisten deutschen Fachzeitschriften im Gebiet Informationssicherheit und Datenschutz – und darauf sind wir auch ein kleines bisschen stolz.

Wir würden uns freuen, wenn Sie die Jubiläumsausgabe zum Anlass nähmen, uns in einem kurzen Kommentar zu verraten, was Sie uns schon immer einmal sagen wollten… Unter allen Einsendern verlosen wir die ersten zehn Exemplare der in Kürze erscheinenden dritten Auflage unseres Fachbuchs „Datenschutz und Informationssicherheit“.

T.I.S.P.-Zertifizierung

Kurzentschlossene können sich noch einen Platz auf dem T.I.S.P.-Seminar am **13.–17.05.2019** sichern. Die (über)nächste Gelegenheit zur Zertifizierung Ihrer Kenntnisse in der Informationssicherheit bieten wir am **14.–18.10.2019** (Achtung: nur noch vier freie Plätze, baldige Anmeldung empfohlen).

Wie souverän ist der Souverän?

Angesichts der wachsenden Komplexität von IT-Systemen, dem Eindringen der IT in immer mehr Lebensbereiche und der Zunahme der Verarbeitung personenbezogener Daten ist "digitale Souveränität" nicht mehr lediglich von mangelnder Medienkompetenz bedroht. Beim kommenden KA-IT-Si-Event am **06.06.2019** in Kooperation mit der Initiative Smart Ettlingen zeichnet Dirk Fox die Entwicklung des Internet vom "Schaufenster" zu einer Überwachungsinfrastruktur nach und zeigt auf, welche Verantwortung für die Erhaltung (oder womöglich die Wiederherstellung) von digitaler Souveränität auf die Softwareentwickler von heute und morgen zukommt – und welche Schritte dafür erforderlich sind. Im Anschluss folgt eine Diskussion zum Thema "Digitale Souveränität im internationalen Kontext". Danach haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim "Buffet-Networking" (Anmeldung).

11. Tag der IT-Sicherheit

Für die Keynote des bereits elften Karlsruher „Tag der IT-Sicherheit“ konnten wir die polnische IT-Security-Expertin Paula Januszkiewicz („*Think and Act Like a Hacker to Protect Your Company's Assets*“) gewinnen. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, KASTEL und dem CyberForum e.V. findet am **11.07.2019** im Saal Baden der IHK Karlsruhe statt. Das vollständige Programm sowie die Möglichkeit zur Anmeldung finden Sie auf unserer Webseite www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

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

Mai 2019	
06.-09.05.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
13.-17.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
14.-17.05.	European Identity & Cloud Conference 2019 (KuppingerCole Ltd., München)
19.-23.05.	Eurocrypt 2019 (IACR, Darmstadt)
21.-23.05.	16. Deutscher IT-Sicherheitskongress (BSI, Bonn)
22.-23.05.	20. Datenschutzkongress (EUROFORUM Deutschland SE, Berlin)
26.-30.05.	OWASP AppSec Tel Aviv 2019 (OWASP Foundation, Tel Aviv/ISR)
Juni 2019	
03.-05.06.	Entwicklertag 2019 (VKSI, GI, ObjektForum, Karlsruhe)
03.-04.06.	DuD 2019 (COMPUTAS Gisela Geuhs GmbH, Berlin)
05.-06.06.	BvD-Verbandstage 2019 (BvD e.V., Berlin)
13.-14.06.	Annual Privacy Forum 2019 (ENISA, EC DG Connect, Universität Wien, Rom/I)
17.-19.06.	4rd IEEE European Symposium on Security and Privacy (IEEE Computer Society, Stockholm/SWE)
24.-25.06.	T.I.S.P. Update Schulung (isits AG, Bochum)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Hans-Joachim Knobloch, Michael Knopp, Jannis Pinter, Friederike Schellhas-Mende.

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