secorvo
security consulting

Secorvo Security News

Oktober 2015

Datenschutzdomino

Elf Jahre lang, von 1998 bis 2009, fand jährlich der Domino-Day statt. Seine Spannung bezog er aus der Ungewissheit, wie viele Steine der erste Stein zum Fallen bringen würde.

Dieselbe Spannung befällt nun Unternehmen und Datenschützer angesichts des Realitäts-checks für Safe Harbor durch den EuGH. Allein bewirkt dieser erste gefallene Stein wenig, stehen doch u. a. mit Standardvertrags-klauseln und Corporate Binding Rules noch andere Wege für die rechtskonforme Übermittlung personen-bezogener Daten an US-Unternehmen bereit.

Doch die nächsten Steine wackeln. Die im Urteil festgestellten Schutzlücken gegenüber staatlicher Datenerhebung können auch Standardvertragsklauseln nicht beheben. Selbst die Einwilligung des Betroffenen wird, mangels Transparenz, als unwirksam angesehen. Solche Defizite sind nicht auf die USA beschränkt – die Urteilsfolgen werden es langfristig auch nicht sein. Andere Bausteine wie die Auf-tragsdatenverarbeitung bspw. im Konzern oder in der Cloud könnten bei konsequenter vergleichbarer Spruchpraxis wanken – hier hat der Auftraggeber häufig weder die Weisungshoheit noch effektive Kontrollmöglichkeiten.

Das Datenschutzrecht hat ein Problem mit der Schutzgewährleistung bei der kooperativen, vor allem internationalen Datenverarbeitung. Instrumente wie Safe Harbor versprachen Rechtssicherheit; die reale Umsetzung des europäischen Datenschutzes war jedoch schon lange und erkennbar reine Fiktion. Da kann auch ein auf die Schnelle verabschiedetes US-Gesetz nicht helfen.

Informationelle Selbstbestimmung durch Isolation der Daten in der EU ist unrealistisch. Laissez faire allerdings auch keine Lösung.

Beim Domino Day entstanden aus den umgefallenen Steinen neue Bilder. Genauso braucht das Datenschutzrecht neue Instrumente, die einen effektiven Schutz personenbezogener Daten nicht untergraben.

Inhalt

secorvo
security consulting

Security News

Chrome will weniger verwirren

Am 13.10.2015 hat Google in einem Blogpost angekündigt, mit Wechsel von der Version 45 auf 46 die Darstellung von HTTPS-Verbindungen in Chrome, die die Überprüfung nicht vollständig bestehen, zu vereinfachen. Das bisherige gelbe Symbol, mit dem auf kleinere Probleme bei einer HTTPS-Verbindung hingewiesen wurde, fällt weg. Dieser Status wird zukünftig mit dem Status „HTTP“ gleichgesetzt. Dadurch reduziert Google die Anzeige auf drei Status.

Das ist aus unserer Sicht ein begrüßenswerter Ansatz, denn bisher konnte die Vermutung aufkommen, dass HTTPS mit kleineren Problemen (gelb) unsicherer sei als reines HTTP (keine Farbe). Für Benutzer ist es schon schwierig genug, HTTPS zu verstehen – daher ist jeder Gewinn an Klarheit bei der Darstellung ein Gewinn für die Sicherheit.

Still und Heimlich

Mit dem eilig verabschiedeten neuen Gesetz zur Vorratsdatenspeicherung – offiziell Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten – ist, kaum wahrgenommen, auch ein neuer Straftatbestand der „Datenhehlerei“ im Strafrecht (§ 202d StGB) eingeführt worden.

Danach soll bestraft werden, wer sich oder Dritten Daten verschafft, verbreitet oder zugänglich macht, die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat. Ausgenommen sind lediglich Handlungen, die ausschließlich der Erfüllung beruflicher Pflichten dienen. Laut Entwurfsbegründung sollen so Lücken im Schutz vor dem Handel mit illegal erlangten Daten geschlossen werden.

Befürchtet wird jedoch, dass der Tatbestand auch Whistleblower oder Blogger erfasst, die Informationen veröffentlichen, ohne deren illegale Beschaffung ausschließen zu können. Die subjektiven Voraussetzungen schränken den Straftatbestand jedoch ein, denn es muss eine Bereicherungs- oder Schädigungsabsicht vorliegen. Journalisten sind nur dann ausgenommen, wenn ihr Status anerkannt wird – das dürfte mindestens zu Verunsicherung führen. Dabei drängt sich tatsächlich der Eindruck auf, dies könnte angesichts zahlreicher Leaks das primäre Ziel der Regelung sein.

DANE ist RFC 7672

Mit der Standardisierung von DANE for SMTP als RFC 7672 hat die Internet Engineering Task Force (IETF) im vergleichsweise kurzen Zeitraum von nur zwei Jahren einen neuen Standard für den sicheren E-Mail-Transport geschaffen. Auch das BSI fordert mittlerweile in seiner technischen Richtlinie Sicherer E-Mail-Transport den Einsatz von DANE.

Im Gegensatz zur Ende-zu-Ende-Verschlüsselung (wie S/MIME oder PGP) zielt DANE darauf ab, einen sicheren Transport zwischen den Mailservern mittels SSL/TLS zu gewährleisten. Hierzu publizieren die E-Mail-Server einen über DNSSEC gesicherten Eintrag mit dem Fingerprint ihres X.509 Zertifikats. Der sendende E-Mail-Server kann diesen Fingerprint zum Schutz vor manipulierten Zertifikaten beim Verbindungsaufbau prüfen.

Der schnellen Verbreitung von DANE steht derzeit noch entgegen, dass alle beteiligten E-Mail-Server für DANE konfiguriert sein müssen und das noch nicht sehr weit verbreitete DNSSEC-Protokoll benötigen.

Audit Fails

Am 07.10.2015 veröffentlichte Guido Vranken gleich acht Schwachstellen, die er bei seiner Analyse des Quellcodes der freien SSL/TLS Bibliothek ARM mbed TLS / PolarSSL gefunden hatte. Damit lässt sich PolarSSL teilweise sogar über das Netzwerk angreifen. Die Ursache sind überwiegend Buffer-Overflows auf Stack und Heap – typische Fehler der 90er Jahre des vergangenen Jahrhunderts. Pikant wird diese Entdeckung vor dem Hintergrund, dass PolarSSL im Auftrag des niederländischen Geheimdienstes AIVD durch die Firma Fox-IT einem Code-Audit unterzogen wurde, bei dem diese Schwachstellen nicht gefunden wurden.

Der Fall weist eine gewisse Ähnlichkeit zu Truecrypt auf: Forscher des Google-Projekts Zero veröffentlichten am 18.09.2015 eine kritische Schwachstelle von Truecrypt (Incorrect Impersonation Token Handling EoP), die bei der Prüfung im Rahmen des Open Crypto Audit Project (siehe SSN 04/2015) offenbar nicht aufgefallen war. Ein Fehler im Truecrypt-Treiber ermöglicht den unberechtigten Zugriff auf Truecrypt-Container anderer Nutzer auf derselben Maschine. Auch wenn die Schwachstelle nur unter bestimmten Voraussetzungen ausgenutzt werden kann, ist ein Umstieg auf Alternativen wie den Truecrypt-Nachfolger Veracrypt (Fehler gefixt) oder Ciphershed zu empfehlen.

Auch ein Code-Audit ist keine Garantie für die Abwesenheit von Schwachstellen. Denn erstens kann aufgrund der Komplexität heutiger Anwendungen meistens nur ein Teil intensiv durchleuchtet werden; das sollte von den Auditoren sauber dokumentiert werden. Und zweitens ist trotz der

Unterstützung durch ausgefeilte Tools am Ende immer der Auditor gefragt. Dabei kann leicht der eine oder andere kleine Fehler übersehen werden – mit fatalen Folgen für die Sicherheit des Produkts.

Threat Modelling Tool 2016

Am 07.10.2015 hat Microsoft eine verbesserte Version des Microsoft Threat Modelling Tool angekündigt. Das Tool hat sich in der Praxis für die Erstellung von Bedrohungsmodellen bewährt, hatte aber bisher einige Schwächen bei der Anpassung der Vorlagen für Modelle. Wir begrüßen es sehr, dass Microsoft sich genau dieser Punkte angenommen hat und mit der neuen Version einen Template-Editor liefert, auf den wir sehr gespannt sind. Bedrohungsmodelle sind ein wichtiger Teil von Sicherheitsanalysen. Nach unserer Erfahrung lohnt es, das (kostenlose) Werkzeug für die Durchführung von Bedrohungsanalysen in Betracht zu ziehen.

Secorvo News

Ritterschlag

Mit der zunehmenden Sensibilität für IT-Sicherheit wachsen Penetrationstester wie Pilze aus dem Boden. Wenn ein Penetrationstest keine relevanten Schwachstellen findet, liegt das daher manchmal nicht nur an der Absicherung.

Mit dem Zertifikat „Offensive Security Certified Professional“ (OSCP) haben die Urheber von Kali-Linux und der Exploit-DB vor knapp fünf Jahren eine Qualifikation für Pentester geschaffen, die es in sich hat: Nach intensiven Live-Hacking-Lektionen über mehrere Monate (von der Informationssammlung über die Nutzung von Exploit-Code bis zur Übernahme von Windows-Domänen) folgt eine praktische Prüfung, in der die Kandidaten innerhalb von 24 Stunden in einer Laborumgebung ein vorgegebenes Hacking-Ziel erreichen und anschließend dokumentieren müssen.

Im Oktober haben **Dr. Safuat Hamdy** und **André Domnick** diese derzeit anerkannteste Pentester-Zertifizierung bestanden – ein Ritterschlag.

T.I.S.P., CPSSE und mehr...

Zwei Gelegenheiten zur Zertifizierung Ihrer Qualifikation bietet Secorvo College noch in diesem Jahr: Ein CPSSE- (**16.–19.11.2015**) und ein T.I.S.P.-Seminar (**23.–27.11.2015**) mit anschließender Zertifikatsprüfung.

Im kommenden Jahr bieten wir wieder zahlreiche interessante und lehrreiche Schulungen an. Neu im Programm ist der D'Day – Datenschutz Deep Impact, der sich an Datenschutzbeauftrage richtet: Ausgewähltes aktuelles Erfahrungswissen, konzentriert an einem Tag. Die erste Gelegenheit für eine Teilnahme bietet sich am **25.02.2016**.

Den Schwerpunkt Sichere Software- und Systementwicklung haben wir ausgebaut. Mit den Seminaren Java Security und Secure Coding C/C++ vertiefen wir die Sicherheitsaspekte von der Projektierung bis zum Coding. Das Seminar spricht nicht nur Entwickler, sondern alle Beteiligte im Lifecycle der Softwareentwicklung an.

Auch die Zertifikatsseminare T.I.S.P., T.E.S.S. und CPSSE bieten wir im kommenden Jahr zu mehreren Gelegenheiten an, ebenso das Seminar IT-Sicherheit heute – praxisnah, zielsicher, kompakt mit den neuesten Entwicklungen in Informationssicherheit und Datenschutz. Am **26.–28.01.2016** können Sie sich auf den neusten Stand bringen lassen.

Globale Überwachung

Beim KA-IT-Si-Event „Eine kurze Geschichte der Überwachung“ am 08.10.2015 füllten knapp 200 Teilnehmer das Medientheater des ZKM | Karlsruhe. Den ersten 80 angemeldeten Teilnehmern konnten wir eine Sonderführung durch die sehr empfehlenswerte Ausstellung "GLOBALE: GLOBAL CONTROL AND CENSORSHIP. Weltweite Überwachung und Zensur" anbieten. Zahlreiche Exponate bieten einen interessanten Einblick in digitale Überwachung und Zensur, wie beispielsweise ein Live-Ticker der aktuell in China gesperrten Websites, eine Visualisierung aller gerade eingeschalteten Smartphones im ZKM (und der von diesen gesuchten WLANs) und eine Wand voller „Überwachungsmonitore“, die Live-Bilder von im Internet frei erreichbaren Webcams zeigen. Die Ausstellung kann noch **bis zum 01.05.2016** besucht werden. (Museums-) Eintritt: 10 €; freitags von 14-18 Uhr ist der Eintritt frei.

Eat, Sleep, Pwn, Repeat

Sicherheitslücken in Protokollen, Systemen und Anwendungen sind die zentrale Ursache erfolgreicher Angriffe auf moderne IT-Systeme. Dennoch gibt es nur wenige Möglichkeiten, tiefergehendes Wissen in diesem Bereich zu erlernen. Capture-The-Flag-Wettbewerbe (CTF) bieten dafür einen spielerischen Rahmen. Dabei treten über den Zeitraum eines Wochenendes mehrere Teams gegeneinander an und lösen anspruchsvolle Aufgaben aus den Bereichen Binary Exploitation, Kryptologie, Reverse Engineering, Web-Sicherheit und Forensik.

Beim nächsten KA-IT-Si-Event am **03.12.2015, 18 Uhr** berichten **Samuel Groß** und **Niklas Baumstark** (KITCTF Team) von ihren Erfahrungen und stellen ausgewählte Beispiele von Aufgaben aus CTFs vor (zur Anmeldung).

Veranstaltungshinweise

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

November 2015	
02.-03.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)
10.-13.11.	T.E.S.S. – Sichere Systeme dank System Security Engineering (Secorvo, Karlsruhe)
10.-11.11.	ISSE 2015 (TeleTrust e.V./eema, Berlin)
10.-13.11.	Blackhat Europe 2015 (Blackhat, Amsterdam/NL)
12.-13.11.	Smart Energy 2015 (Fachhochschule Dortmund)
16.-19.11.	CPSSE (Certified Professional for Secure Software Engineering) (Secorvo, Karlsruhe)
17.-20.11.	DeepSec ISDC 2015 (DeepSec GmbH, Wien/AT)
19.-20.11.	39. Datenschutzfachtagung (DAFTA) (GDD, Köln)
23.-27.11.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
24.-25.11.	3. DFN-Konferenz "Datenschutz" (DFN-Cert Services GmbH, Hamburg)
25.-26.11.	Die Zukunft der IT im Digital Business (Management Circle AG, München)
30.11.-01.12.	IsSec/ZertiFA 2015 (COMPUTAS Gisela Geuhs GmbH, Berlin)
Dezember 2015	
03.12.	Eat, Sleep, Pwn, Repeat, (KA-IT-Si, Karlsruhe)

Impressum

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

ISSN 1613-4311

Autoren: Dirk Fox, André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp (Editorial).

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