secorvo
security consulting

Secorvo Security News

Dezember 2022

Runder Kopf

Der Kopf ist rund, damit das Denken die Richtung wechseln kann.
Francis Picabia

Verfolgt man, welche Standpunkte in jüngster Zeit zum Thema Datenschutz eingenommen werden, lassen sich nur zwei Positionen finden: Die derjenigen, die jegliche Risiken für die Betroffenen vermeiden, und die derjenigen, die den Datenschutz am liebsten ganz abschaffen möchten.

So fordert Alena Buyx, Vorsitzende des deutschen Ethikrats, am 08.12.2022 im Interview mit der Süddeutschen Zeitung, nicht über Risiken von Daten zu sprechen, sondern über deren Nutzen. Zu viel Datenschutz gefährde Patienten. Liest man hingegen beispielsweise die FAQ zu MS365 des LfDI Rheinland-Pfalz, so scheint nach Auffassung der Aufsichtsbehörden eine Verarbeitung nur noch zulässig zu sein, wenn keinerlei Risiken für den Betroffenen verbleiben.

Beide Positionen gehen am Kern der DSGVO vorbei. Denn dort geht es in erster Linie um den Umgang mit möglichen Risiken: So dürfen personenbezogene Daten im lebenswichtigen Interesse der Betroffenen immer verarbeitet werden (Art. 6 Abs. 1 d)), während sich in anderen Fällen die Zulässigkeit einer Verarbeitung nach der Frage richtet, welche konkreten Risiken es gibt, wie wahrscheinlich deren Eintritt ist und welche Maßnahmen dagegen ergriffen werden (können). Schließlich soll nach dem Grundsatz „Privacy by Design" der Datenschutz schon bei der Konzeption und Entwicklung innovativer Lösungen mitberücksichtigt werden.

Auch die datenschutzrechtlich Verantwortlichen sind Grundrechtsträger und verfolgen berechtigte Interessen. Die sind abzuwägen gegen die schutzwürdigen Interessen der Betroffenen. Das gelingt nur mit einem unverstellten Blick auf die tatsächlichen Risiken und die Umstände des Einzelfalls. Das ist mühsamer als ein pauschales „so nicht" – wird aber zu besseren Entscheidungen führen.

Inhalt

secorvo
security consulting

Security News

Spy Kit

Die Firma Pushwoosh vertreibt Software Development Kits (SDK) zur Auswertung von Nutzeraktivitäten in Apps (Tracking, Profiling), die Entwickler in ihre Programme integrieren können. Nach der Webseite des Herstellers nutzen bereits über 80.000 Firmen ein Pushwoosh-SDK.

Am 14.11.2022 wurde das vorgeblich in den USA ansässige Unternehmen nach Reuters-Recherchen in Novosibirsk verortet: Es hat 40 Mitarbeiter und einen Jahresumsatz von (umgerechnet) 2,4 Mio. €. „Mailand oder Madrid, Hauptsache Italien!" möchte man da fast sagen… Am selben Tag veröffentlichte Internet Safety Labs eine Liste einiger tausend Apps, die vorgeblich Pushwoosh-Code verwenden – darunter auch Training-Apps der US Army. Offenbar hatte man angenommen, das Unternehmen käme aus Washington D.C.

Tatsächlich bietet die Webseite von Pushwoosh Anlass für Skepsis: Eine Firmenanschrift sucht man dort vergeblich. Wer fremde Software in seine „Supply Chain" integriert, sollte daher schon genau hinsehen – vor allem, wenn der Code Nutzerdaten auf externe Server überträgt.

Domain-Trickserei

Schon immer konnte man den Kartendienst Google Maps sowohl über maps.google.com als auch über google.com/maps erreichen. Wie Rutger Roffel am 02.12.2022 auffiel, ersetzt Google jedoch neuerdings die URL maps.google.com beim Aufruf durch google.com/maps. Kleiner Schritt – große Wirkung:

Bisher waren alle Dienste von Google (wie news.google.com oder mail.google.com) durch eine eigene Sub-Domain logisch von der Top-Level-Domain google.com getrennt – mit der Folge, dass Browser-Freigaben nur für den jeweils aktiven Dienst gelten. Diese Trennung hat Google nun bei Maps aufgehoben und den Kartendienst damit zu einem Teil der Top-Level-Domain google.com gemacht. Gibt ein Nutzer für den Kartendienst die Übermittlung seines Standorts durch den Browser frei, gilt diese Freigabe für die gesamte Domain google.com – der Standort wird also auch bei der Google-Suche übermittelt. Ein Schelm, wer…

Datenschutzrechtlich ist das ein Verstoß gegen das Transparenzgebot (Art. 12 DSGVO), denn Google täuscht Nutzerinnen und Nutzern vor, dass sich die Standortfreigabe lediglich auf Maps bezieht. Da sich Google bei der Verarbeitung zudem auf „berechtigtes Interesse" beruft, wird der Standort auch dann verarbeitet, wenn im Consent-Banner „alles" abgelehnt wird. Die Zustimmung zur Standort-Übermittlung durch den Browser ist jedoch keine rechtskonforme Datenschutz-Einwilligung.

Immerhin: Firefox-User sind nicht betroffen, da Firefox ausschließlich temporäre Standortfreigaben erteilt.

Threema-Verschlüsselung

Am 09.01.2023 veröffentlichten Forscher der ETH Zürich eine kryptografische Analyse der Threema-Verschlüsselung. Darin beschreiben sie sieben Angriffsmöglichkeiten auf das Protokoll des verbreiteten Messengers. Laut Threema ist das im Dezember 2022 eingeführte neue Protokoll Ibex für die dargestellten Angriffe nicht anfällig; soweit bekannt wurde auch keiner der beschriebenen Angriffe in der Praxis eingesetzt.

Doch der Fall ist ein Paradebeispiel für mehrere Lektionen, die bei der Entwicklung kryptografischer Protokolle beachtet werden sollten. So war nicht eine fehlerhafte Implementierung kryptografischer Verfahren das Problem, sondern deren Zusammenstellung zu miteinander verwobenen Protokollen. Zusätzlich zum bekannten Mantra „don´t roll your own crypto" lautet die generelle Empfehlung der ETH-Forscher, wann immer möglich auf bekannte und bewährte Protokolle wie beispielsweise TLS zurückzugreifen – spätestens seit dem Desaster des WEP-Protokolls (SSN 3/2002) sollte das eigentlich das „übliche Vorgehen" sein.

Auch Schneier´s Law haben die Threema-Entwickler missachtet: Danach kann ein kryptografisches Protokoll (genau wie ein kryptografischer Algorithmus) nur durch unabhängige Analysen seine Sicherheit unter Beweis stellen. Für die Einordnung solcher Sicherheitsanalysen muss zudem definiert sein, gegen welche Angriffsmodelle das Protokoll schützen soll; erst daraus können Sicherheitsaussagen abgeleitet werden. Die Definition von Standard-Angriffsmodellen, gegen die ein kryptografisches Protokoll für einen Messenger schützen soll, wäre daher für Entwickler und Sicherheitsexperten hilfreich.

Um Protokoll-Analysen zu erleichtern ist der derzeitigen Darstellung des Threema-Protokolls eine höhere Detailtiefe zu wünschen – vergleichbar der der Dokumentation des Signal Protokolls.

Bußgeld-Krimi

Seit dem 20.08.2018 hatte sich die für ihre laxe Haltung in Datenschutzfragen bekannte irische Datenschutzaufsichtsbehörde (DPC) mit offensichtlichen Datenschutzverstößen von Meta beschäftigt – nicht auf eigene Initiative, sondern ausgelöst

durch eine Beschwerde der von Max Schrems gegründeten Non-Profit-Organisation NOYB bei der belgischen Datenschutzaufsicht vom 25.05.2018.

Um die strengen datenschutzrechtlichen Anforderungen an eine Einwilligung zu umgehen hat Meta die Verarbeitung von Nutzerdaten für personalisierte Werbung als Klausel in die AGB von Facebook und Instagram aufgenommen, da diese für die Bereitstellung der Dienste erforderlich sei. Ein Umgehen der Einwilligung durch die Aufnahme in einen Vertrag ist jedoch durch das Kopplungsverbot (Art. 6 Abs. 4 DSGVO) untersagt. Der Verstoß hat zusätzliches Gewicht durch die Monopolstellung von Meta.

Gegen den vorläufigen Entscheidungsentwurf der DPC legten neun europäische Aufsichtsbehörden Beschwerde ein, sodass eine Streitbeilegung nach Art. 65 durch die europäische Datenschutzaufsicht (EDPB) erforderlich wurde. Derweil verhängte die DPC am 15.03.2022 ein 17 Mio. €-Bußgeld gegen Facebook und am 28.11.2022 ein 265 Mio. €-Bußgeld gegen Instragram. Wenige Tage später veröffentlichte der EDPB am 05.12.2022 die verbindlichen Anordnungen zu Facebook und zu Instagram, in denen Meta die Praxis untersagt und von der DPC die Verhängung eines höheren Bußgelds verlangt wird. Die reagierte am 31.12.2022 mit einem weiteren Bußgeldbescheid über 390 Mio. €. Darin ist allerdings die Abschöpfung der von Meta mit den unrechtmäßig verarbeiteten Daten erwirtschafteten (Milliarden-) Gewinne nicht enthalten – das letzte Wort ist also wohl noch nicht gesprochen.

Vor diesem Hintergrund wirkt die Stellungnahme von Meta gegenüber der DPA geradezu hämisch: „Wir glauben zutiefst, dass unser Ansatz die EU-Datenschutzverordnung respektiert […].“

Garantien von Microsoft

Am 15.12.2022 hat Microsoft bekannt gegeben, dass das lange angekündigte EU Data Boundary für Microsoft 365 (SSN 11/2022) zum 01.01.2023 in Betrieb geht. Automatisch kommt man aber nicht in den Genuss der Vorteile dieser Regelung: Nur wer das Data Protection Addendum auf die Fassung vom 01.01.2023 aktualisiert, kann sicher sein, dass seine Daten in dem von Microsoft beschriebenen Rahmen innerhalb der EU gespeichert und verarbeitet werden. Die Verantwortung dafür liegt beim Kunden. Das Angebot richtet sich nicht nur an Kunden mit Volumenlizenzvertrag, sondern an alle, die mit Microsoft Vereinbarungen im Zusammenhang mit deren Cloud-Produkten und –Dienstleistungen abgeschlossen haben.

Mit Daten bezahlen

Am 29.11.2022 hat die Datenschutzkonferenz (DSK) einen Beschluss zu den „Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht“ veröffentlicht – dem „Bezahlen mit Daten“, das durch die Änderung des § 312 BGB zur Umsetzung der EU-Richtlinie zu digitalen Inhalten und Dienstleistungen nun zulässig ist. Die DSK beschränkt sich allerdings darauf festzustellen, dass die neuen Regelungen nur auf Verträge über digitale Produkte anwendbar sind, und nicht, wenn Betroffene lediglich ihre Einwilligung bei Consent Bannern erteilen. Bei Consent Walls wird man hingegen davon ausgehen dürfen, dass es zu einem Vertragsabschluss kommt.

Die Frage nach dem angemessenen Preis, wenn sich Betroffene dafür entscheiden, statt mit Geld mit ihren Daten zu bezahlen, wird auch von der DSK nicht beantwortet.

Secorvo News

Seminare

Ins Jahr 2023 startet unser Seminarbereich mit dem Seminar BSI Vorfall-Experte. Vom **07.03.** bis **09.03.2023** haben Sie die Möglichkeit, sich bei uns auf die Zertifizierung zum BSI-Experten nach dem Curriculum des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorzubereiten.

Im Seminar IT Security Insights – T.I.S.P. Update vom **21.03.** bis **22.03.2023** können Sie Ihren Wissenstand rund um die Themen Informationssicherheit und Datenschutz auffrischen. Kurz vor Ostern (**27.03.–31.03.2023**) bieten wir Ihnen mit dem T.I.S.P.-Seminar die Möglichkeit, Ihre IT-Security-Kenntnisse nicht nur zu vertiefen, sondern auch zertifizieren zu lassen – zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser T.I.S.P.-Buch „Informationssicherheit und Datenschutz“ (erschienen im dpunkt-Verlag).

Die Seminarprogramme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2023	
20.-22.01.	ShmooCon 2023 (The Shmoo Group, Washington/US)
Februar 2023	
08.-10.02.	30. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
07.-09.03.	BSI Vorfall-Experte (Secorvo, Karlsruhe)
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
21.-22.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende (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