secorvo
security consulting

Secorvo Security News

Januar 2023

Datenparadies Irland

Gegen die europäischen Niederlassungen mehrerer Meta-Unternehmen hatte Max Schrems' Initiative noyb wegen Umgehung der Einwilligungspflicht bei personalisierter Werbung sowie mangelnder Transparenz bei verschiedenen europäischen Aufsichtsbehörden mehrere Datenschutz-Beschwerden eingereicht – pünktlich zum Inkrafttreten der DSGVO am 25.05.2018.

Angelockt von niedrigen Steuern haben viele amerikanische „Big Tech"-Konzerne wie Microsoft, Meta, Google oder Apple ihre europäische Hauptniederlassung in Irland. In Datenschutzfragen ist damit die irische Datenschutzbehörde DPC zuständig.

Jahrelang verschleppte die DPC die Entscheidungen über die Beschwerden. Zunächst hatte die DPC sogar versucht, eine Leitlinie des Europäischen Datenschutzausschusses (EDSA) zu beeinflussen, um die Umgehung der Einwilligung durch Meta zu legitimieren. In einem ersten Entscheidungsentwurf vom 06.10.2021 ging die DPC nur auf die Transparenzverstöße ein, ließ das Vertragsmodell unberücksichtigt und empfahl ein Bußgeld von 28 bis 36 Mio. €. Nach Einsprüchen mehrerer europäischer Aufsichtsbehörden hob der EDSA am 05.12.2022 die vorläufigen Bußgeldbescheide der DPC gegen Facebook über 17 Mio. € (15.03.2022) und Instagram über 265 Mio. € (28.11.2022) auf und erhöhte die Bußgelder von Facebook, Instagram und WhatsApp auf insgesamt 390 Mio. € (SSN 12/2022).

Keine europäische Aufsichtsbehörde stellte sich dabei auf die Seite der DPC. Die Ankündigung der DPC, gegen den verbindlichen Beschluss des EDSA vorzugehen, spricht Bände. Dabei ist die DPC trotz eines Jahresbudgets von 19 Mio. € die Aufsichtsbehörde Europas mit den mit Abstand meisten unerledigten Fällen: Von 164 Beschwerden mit europaweiter Bedeutung wurden erst vier erledigt, wie ein Bericht des Irish Council for Civil Liberties vom 13.04.2022 aufzeigt. Die Geduld des EDSA ist nun hoffentlich zu Ende.

Inhalt

secorvo
security consulting

Security News

Detailfrage

Mit seinem Urteil vom 12.01.2023 hat der EuGH auf ein Vorabentscheidungsersuchen des Obersten Gerichtshofs Österreichs eine wichtige Auslegung des Art. 15 Abs. 1 lit. c DSGVO (Datenschutz-Auskunftsersuchen) geklärt: Danach muss der Verantwortliche (im vorliegenden Fall die Österreichische Post AG) die Identität der (Daten-) Empfänger so konkret wie möglich benennen, um dem Transparenzgrundsatz zu genügen und dem Betroffenen eine weitere Rechtsausübung überhaupt erst zu ermöglichen. Ist dem Verantwortlichen dies (noch) nicht möglich, darf er sich darauf beschränken die Kategorien der betreffenden Empfänger mitzuteilen.

Eine Auskunft kann verweigert werden, wenn ein Antrag offenkundig unbegründet oder exzessiv ist; das muss der Verantwortliche jedoch nachweisen.

iCloud-Verschlüsselung

Apple hat am 23.01.2023 auch in Deutschland die Möglichkeit freigeschaltet, unter iOS 16.2 und macOS 13.1 den erweiterten Datenschutz zu aktivieren. Damit lassen sich fast alle Daten in der iCloud Ende-zu-Ende verschlüsseln. Die Funktion muss vom Nutzer ausgewählt werden.

Die US-Bundespolizei FBI kritisiert die Ende-zu-Ende Verschlüsselung; im Rahmen von Ermittlungen bekommt sie nun nur noch eingeschränkten Zugriff auf die Daten in der iCloud. Gemäß Apples jüngstem Transparenzbericht von 2021 wurden in fast 4000 Fällen iCloud-Daten an Behörden herausgegeben – darunter auch iCloud Backups.

iCloud Mail, Kalender und Kontakte sowie zahlreiche Metadaten wie Dateinamen, Checksummen und Safari-Lesezeichen werden allerdings weiterhin nicht Ende-zu-Ende verschlüsselt. Die Lösung hat daher noch Luft nach oben.

NIS2

Am 14.12.2022 wurde die so genannte NIS2-Richtlinie über „Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union“ (EU 2022/2555) im EU-Amtsblatt veröffentlicht. Ziel der Richtlinie ist ein einheitlicheres Niveau der IT-Sicherheit kritischer Infrastrukturen innerhalb der EU. Sie muss bis Oktober 2024 in nationales Recht umgesetzt werden. In Deutschland ist vieles bereits im IT-Sicherheitsgesetz 2.0 geregelt (siehe SSN 5/2021).

Die Richtlinie gilt für Unternehmen in kritischen Infrastrukturen mit mindestens 50 Mitarbeitern und 10 Mio. € Umsatz. Teile der digitalen Infrastruktur und der öffentlichen Verwaltung sollen unabhängig von der Größe reguliert werden. Die Unternehmen müssen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ nach dem „Stand der Technik“ ergreifen, die sie nach einer „systemischen Analyse“ festlegen. Zuständig für die Umsetzung der Maßnahmen ist die Geschäftsführung. Die getroffenen Maßnahmen sind systematisch mit Hilfe eines implementierten Risikomanagementsystems zu dokumentieren.

Bei Verstößen können Bußgelder verhängt werden, deren Höhe an die der DSGVO angelehnt wurde: bis zu 10 Mio. € oder 2 % des weltweiten Jahresumsatzes bei wesentlichen und 7 Mio. € bzw. 1,4 % des Jahresumsatzes bei wichtigen Einrichtungen. Das kann teuer werden, da im schlimmsten Fall auch noch ein Bußgeld wegen Verstoßes gegen die DSGVO hinzukommen kann.

Verbannt

Am 25.11.2022 machte die US-Regierung ernst: In einer aktualisierten Auslegung des Secure Equipment Act vom 11.11.2021 (H.R.3919) verbot sie die Zulassung von chinesischen Telekommunikations- und Videoüberwachungseinrichtungen, da sie eine Gefahr für die nationale Sicherheit darstellten. Damit dürfen Komponenten von Huawai, ZTE und anderen chinesischen Herstellern zukünftig nicht mehr in Mobilfunkeinrichtungen oder Routern verbaut werden; auch Smartphones könnten betroffen sein.

Zwar gilt auch diese Regelung nicht ohne Ausnahmen und spielten sicher auch wirtschaftliche Interessen bei der Entscheidung eine Rolle. Doch macht sie deutlich, dass die USA die Gefahr einer technischen „Unterwanderung“ der IT-Infrastrukturen ernst nimmt. Anders als die Bundesregierung, die von einer entsprechenden Regelung in § 9b IT-Sicherheitsgesetz bisher keinen Gebrauch macht.

Teure Wahlkampfhilfe

Am 22.12.2022 stimmte Meta einem Vergleich zu: Der Konzern zahlt 725 Mio. US$ an Betroffene für die rechtswidrige Weitergabe der Daten von 87 Mio. Facebook-Nutzern an Cambridge Analytica. Das Unternehmen hatte die Daten 2016 im Wahlkampf von Donald Trump und für die britische Brexit-Kampagne genutzt. Nach Bekanntwerden des Skandals musste Cambridge Analytica am 02.05.2018 Insolvenz anmelden (siehe SSN 4+5/2018). Im Juli 2019 hatte Facebook bereits ein Bußgeld der US-Verbraucherschutzbehörde in Höhe von 5 Mrd. US$ akzeptiert. 660 € pro Datensatz – ein teurer Spaß für die Aktionäre. Auch in diesem Sinne kann sich Datenschutz auszahlen.

IT-Grundschutz-Kompendium

Am 01.02.2023 hat das BSI die Edition 2023 des IT-Grundschutz-Kompendiums vorgestellt. In der aktuellen Version finden sich 10 neue Bausteine, darunter ein Baustein zum allgemeinen IT-Betrieb, dem nun versionsunabhängigen Baustein „Windows Server“ sowie die vollständige Überarbeitung der Bausteine zur Nutzung und dem Anbieten von Outsourcing. Bei 21 Bausteinen gab es Änderungen, die das BSI in einem eigenen Dokument zusammengefasst hat. Das Kompendium steht in den Formaten PDF und XML zur Verfügung.

Für alle Unternehmen und Einrichtungen, die sich nach IT-Grundschutz zertifizieren lassen, sind ab dem 01.02.2023 die Versionen 2022 und 2023 verbindlich. Aber auch für alle anderen Unternehmen bietet das Kompendium gute Anregungen für die Implementierung von Maßnahmen der Informationssicherheit.

Cookie-Chaos

Cookie-Banner sind ein Ärgernis für Webseitenbesucher, Datenschützer und Webseitenbetreiber – wenn auch aus jeweils anderen Gründen. Zwar sind die gesetzlichen Anforderungen klar: Wer personenbezogene Daten ohne Vertrag oder andere gesetzliche Grundlage verarbeiten möchte (hier: Tracking von Webseitenbesuchern) benötigt eine Einwilligung der Betroffenen.

Wie aber ist eine solche Einwilligung auf einer Webseite rechtskonform zu gestalten? Da gehen die Auffassungen schon seit vielen Jahren (siehe z. B. SSN 2/2015) erheblich auseinander. Am 14.03.2022 hatte sich das European Data Protection Board (EDPB) auf eine Richtlinie zu „Dark Patterns“ geeinigt (SSN 4/2022), mit denen Seitenanbieter versuchen, Besucher zur Zustimmung zu verleiten.

Das ist aber nur ein Teil des Problems. Angesichts der Schwemme der Beschwerden über vorgeblich rechtswidrige Cookie-Banner haben die Datenschutz-Aufsichtsbehörden daher eine „Taskforce Cookie Banner“ eingerichtet, die am 17.01.2022 ihren Bericht vorgelegt hat. Er enthält zahlreiche bereits durch einschlägige Urteile bestätigte Klarstellungen (wie die Forderung, dass ein Tracking erst nach der expliziten Zustimmung erfolgen, die Zustimmung nicht vorausgewählt sein und optionale Cookies nicht als „erforderlich“ deklariert werden dürfen), bleibt aber beispielsweise hinsichtlich der Gestaltung eines „alles Ablehnen“-Knopfs unscharf. Wer Cookies und Tracking wirksam verhindern möchte, bleibt daher bis auf weiteres auf Browser-Plugins wie Privacy Badger der EFF (SSN 12/2017) oder uBlock Origin angewiesen (SSN 10/2022).

Secorvo News

Secorvo auf der DFN-Konferenz

Auf der diesjährigen 30. DFN-Konferenz Sicherheit in vernetzten Systemen (08.-10.02.2023) referierten unsere Datenschutzexperten Friederike Schellhas-Mende und Christian Blaicher zu „E-Mail-Tracking und -Profiling“, und der Krypto-Experte Hans-Joachim Knobloch beschrieb den „Kampf gegen Goldene Zertifikate“ und wie man sich vor Angriffen über die ‚Certifried'-Schwachstelle schützen kann. Die Beiträge erschienen im Konferenzband.

Seminare

Das Seminar BSI Vorfall-Experte vom **07.03.** bis **09.03.2023** bietet Ihnen eine Vorbereitung nach dem Curriculum des Bundesamts für Sicherheit in der Informationstechnik (BSI) auf die Zertifizierung zum BSI-Experten.

Das Seminar IT Security Insights – T.I.S.P. Update vom **21.03.** bis **22.03.2023** frischt Ihren Wissensstand rund um die Themen Informationssicherheit und Datenschutz auf. Und 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.

Phish me, if you can

Ein weltweit agierendes Kollektiv anarchischer Hacker hat sich, getrieben von anarchistischen Freiheitsidealen zum Ziel gesetzt, die vorherrschenden Gesellschaftsstrukturen zu destabilisieren und in totales Chaos zu stürzen. Ihr erstes Ziel ist die Energiewirtschaft.

Beim Jahreseröffnungsevent der KA-IT-Si am **16.03.2023** berichtet Jan Tomasch, Information Security Awareness Manager der EnBW, in seinem Vortrag „Security Awareness Kampagne mit Gamification“, wie die Mitarbeitenden der EnBW als Cyber-Interventionsteam ihre Verteidigungslinie aufbauen, um den Hackern das Handwerk zu legen.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2023	
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)
16.03.	Phish me, if you can (KA-IT-Si, Karlsruhe)
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)
25.-26.04.	Security Forum 2023 (Hagenberger Kreis, Hagenberg/AT)

Fundsache

Die DSK hat am 24.11.2022 Version 3.0 des Standard-Datenschutzmodells beschlossen. Diese Methode zur Datenschutzberatung und -prüfung erleichtert die Umsetzung der rechtlichen Anforderungen der DSGVO in konkrete technische und organisatorische Maßnahmen.

Impressum

Secorvo Security News – ISSN 1613-4311

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