Secorvo Security News

Juni 2022

Wer nicht hören will…

Dieser Grundsatz gilt fast überall, nur nicht für den Datenschutz im öffentlichen Bereich: Anlässlich des EuGH-Urteils vom 05.06.2018 hatte die Datenschutzkonferenz am 01.04.2019 Anforderungen an den rechtskonformen Betrieb von Facebook-Fanpages aufgestellt. Zuletzt veröffentlichten die Datenschutzaufsichtsbehörden hierzu am 18.03.2022 ein Kurzgutachten und forderten im selben Atemzug Ministerien und weitere öffentliche Stellen auf, für datenschutzkonforme Zustände zu sorgen, sprich: die Nutzung von Facebook-Fanpages einzustellen. Passiert ist seitdem: nichts. Und es ist fraglich, ob sich daran etwas ändert. Denn anders als Unternehmen und Bürger müssen Behörden Vorgaben der Aufsichtsbehörden faktisch nicht umsetzen. Juristisch ausgedrückt: § 20 Abs. 7 BDSG entzieht den Aufsichtsbehörden die Befugnis zur Anordnung der sofortigen Vollziehung nach § 80 Abs. 2 Nr. 4 VwGO ausdrücklich, und § 43 Abs. 3 BDSG schließt die Verhängung von Bußgeldern gegen öffentliche Stellen aus. Behörden sind, wie Meldungen aus den Aufsichtsbehörden zeigen, auch nicht gewillt, sich freiwillig zu unterwerfen.

Angesichts der Vorbildfunktion der öffentlichen Hand schwant einem nichts Gutes: Hier werden Ignoranz und Respektlosigkeit gegenüber hoheitlichem Handeln zum Schutz der Privatsphäre rechtlich gebilligt. Ein Staat, der seinen Behörden einen Freibrief bei datenschutzwidrigem Verhalten einräumt, verletzt nicht nur das Rechtsstaatsprinzip der Gesetzmäßigkeit der Verwaltung (Art. 20 GG), sondern setzt auch seine Autorität aufs Spiel, wenn er von Bürgern, Schulen und Unternehmen verlangt, wichtige Arbeitsmittel wie z. B. Teams oder Microsoft 365 durch Open-Source-Lösungen zu ersetzen und damit die eigene Arbeitsfähigkeit zu gefährden. Der Verweis auf den Klageweg ist da ein stumpfes Schwert – ein Griff in die Haushaltskasse der Behörde (auch mal in sechsstelliger Höhe, wie es in anderen EU-Ländern Gang und Gäbe ist) dürfte da schon wirkungsvoller sein, auch wenn das Bußgeld nur von der rechten in die linke Tasche wandert.

Security News

Don't Stop Top 10

Regelmäßig veröffentlichen Hersteller, Fachportale oder Behörden die fünf, sieben oder zehn häufigsten Risiken oder gefährlichsten Schwachstellen, wahlweise in IT-, Informations- oder Cybersicherheit. So auch am 17.05.2022 die CISA mit zehn Handlungsfeldern bezüglich schwacher Sicherheitsmaßnahmen und typischer Angriffswege auf IT-Systeme. Andere Zusammenstellungen wie die CWE Top 25 Most Dangerous Software

Weaknesses oder die OWASP Top 10 listen verbreitete Schwachstellen in der Software-Entwicklung.

Solche Rankings unterstützen eine schnelle Risiko-Priorisierung der jeweiligen Bedrohungen und nennen teilweise, wie die CISA-Liste, Maßnahmen zur Abschwächung oder Abhilfe. Sie richten den Blick allerdings nur auf ausgewählte verbreitete Risiken und ersetzen daher keine umfassende Risikoanalyse, wie sie ein Informationssicherheitsmanagementsystem (ISMS) fordert. Ihren vollen Nutzen entfalten sie auch erst im Kontext eines ISMS (bspw. nach ISO 27001 oder BSI IT-Grundschutz), das sicherstellt, dass die Umsetzung der Maßnahmen zur Reduktion der ermittelten Risiken regelmäßig und systematisch überprüft werden.

Cloud Computing Threats

Die Cloud Security Alliance (CSA) veröffentlichte am 06.06.2022 die elf Top Threats to Cloud Computing. Dazu waren zuvor über 700 Experten befragt worden. In der Auflistung finden sich zahlreiche Bekannte wie „Insufficient Identity" oder „Insecure Interfaces and APIs". Dennoch ist der Bericht lesenswert, denn er beschreibt die einzelnen Bedrohungen im Detail und vergleicht die Ergebnisse mit denen des Berichts aus dem Jahr 2019. So kann er helfen, die eigenen Risikoabschätzungen und Maßnahmenlisten für Cloud-Dienste zu überprüfen.

Drittstaatenübermittlung

Anlässlich des Beginns des fünften Geltungsjahrs der Datenschutzgrundverordnung (DSGVO) forderte der IT-Verband Bitkom am 25.05.2022, dass sich der „Datenschutz an realen Gefahren orientieren" müsse, nicht an „theoretischen Risiken", wie beispielsweise bei der Frage der Zulässigkeit des Einsatzes von Videokonferenzsystemen von US-Unternehmen in deutschen Schulen.

Dabei kommt es bei der Feststellung der Zulässigkeit einer Übermittlung von personenbezogenen Daten in Drittstaaten (Art. 44 ff. DSGVO) auf das Risiko gar nicht an. Entscheidend ist einzig, ob „das betreffende Drittland [...] ein angemessenes Schutzniveau" für die personenbezogenen Daten bietet. Dies hat Auswirkungen auf die Bewertung von Rechtsakten der Drittstaaten, die die Rechte (insbesondere ausländischer) Betroffener beschränken, wie der CLOUD-Act der USA. Und der EuGH stellte 2020 im Schrems II-Urteil klar, dass personenbezogene Daten nur dann in ein Drittland übermittelt werden dürfen, wenn das vom Anbieter garantierte Schutzniveau dem in der Union garantierten gleichwertig ist.

Das stellt viele Unternehmen bei der Nutzung von Cloud-Diensten vor Herausforderungen, denn die Verantwortung für die in ihrem Auftrag durch Dritte verarbeiteten Daten und die Pflicht zur Einholung von Einwilligungen liegt bei ihnen – auch dann, wenn ein Unter-Unter-Unterauftragnehmer eines Dienstleisters die Daten in ein Drittland übermittelt.

Schmerzensgeld für Google Fonts

Am 20.01.2022 sprach das Landgericht München I einem Kläger 100 € Schmerzensgeld zu, da auf einer von diesem besuchten Webseite Google Fonts eingebunden waren und damit seine IP-Adresse ohne Einwilligung an Google-Server übermittelt worden war. Da half auch nicht, dass Google (nach eigenen Angaben) die IP-Adresse nicht speichert.

Mit Verweis auf dieses Urteil wird derzeit versucht, Schadensersatzansprüche in Höhe von 100 € bei Webseitenbetreibern geltend zu machen, die Google Fonts in ähnlicher Weise nutzen – leicht feststellbar mit einem Browser-Plugin zur Tracking-Analyse. Das kann lukrativ sein, denn Google Fonts wurden bereits mehr als 63 Billionen Mal abgerufen.

Wir empfehlen, die Einbindung von Google Fonts zu überprüfen und gegebenenfalls zu korrigieren. Gleiches gilt für die Einbindung anderer Dienste von Anbietern in Drittstaaten wie Karten, Videos oder Social Media Share Buttons: Auch hier wird die IP-Adresse an den Anbieter übermittelt, was nur mit expliziter Einwilligung des Besuchers in die Übermittlung an und die Datenverarbeitung in dem jeweiligen Drittstaat zulässig ist.

Zoom in der Schule

Der hessische Beauftragte für Datenschutz und Informationsfreiheit teilte am 21.06.2022 mit, dass nun der Einsatz von Zoom für Lehrveranstaltungen nach dem „Hessischen Modell“ erlaubt sei. Das setzt voraus, dass ein von Zoom unabhängiger Auftragsverarbeiter mit Servern und Sitz in der EU beauftragt wird und die Inhalte Ende-zu-Ende verschlüsselt werden. Ein Abfluss von personenbezogenen Daten in die USA wird durch diese Maßnahmen verhindert.

Tracking durch ID-Provider

Am 14.01.2020 hatte Google angekündigt, die Unterstützung von Third-Party-Cookies im Chrome-Browser im Jahr 2022 auslaufen zu lassen, und Apple hatte bereits am 26.04.2021 mit iOS 14.5 das Tracking durch Apps als Voreinstellung deaktiviert. Diese Entwicklung bedeutet keineswegs das Ende des Tracking (da Google und Apple über ausreichend selbst erhobene Verhaltensdaten verfügen) – wohl aber das Ende der Datenbasis heutiger Werbenetzwerke (siehe Editorial SSN 5/2022).

Die suchen bereits fieberhaft nach Alternativen, um auch zukünftig Verhaltensdaten zu gewinnen – idealerweise mit Bezug zu möglichst invarianten IDs wie der Mobilfunknummer oder der E-Mail-Adresse von Seitenbesuchern und App-Nutzern. Was liegt da näher, als die Nutzer-Identifikation gleich mit dem Login zu koppeln? Google, Apple und Facebook machen es seit Jahren vor: Sie bieten Login-Schnittstellen an, die Webseitenanbieter einbinden können, um sich damit die Implementierung einer eigenen Nutzerverwaltung zu sparen. Zahlreiche weiterer Identitätsanbieter erblicken gerade das Licht der Welt: Sie verschenken den Dienst und verdienen an den gehashten ID-Daten (wie bspw. Zoetap), die sie an zahlende Werbeanbieter und -broker weiterleiten.

Ohne Einwilligung der Betroffenen ist die Nutzung von ID-Anbietern, die (pseudonymisierte) Daten an Dritte weitergeben, allerdings genauso rechtswidrig wie die Nutzung der ID-Services von Google & Co.

Erhalte das freie Internet

Mit diesem Claim begrüßt TrustPid – ein von Vodafone und der Deutschen Telekom entwickelter ID-Service, der als deutsche Alternative zum Cookie-Tracking gedacht ist – seine Seitenbesucher. Willigt der Nutzer ein, wird aus der Mobilfunknummer und der IP-Adresse des Besuchers eine TrustPid-ID abgeleitet. Alle auf diese bezogenen Tracking-Informationen einer Seite, die TrustPid nutzt, werden dann an den TrustPid-Server übermittelt.

Die vom Nutzer erteilte Einwilligung lässt sich (anders als bei Cookies, die man beim Schließen des Browsers löschen lassen kann) allerdings nicht so leicht widerrufen. Der Weg ist umständlich und intransparent: Ein Widerruf ist nur aus dem Mobilfunknetz im Datenschutzportal von TrustPid oder (gegebenenfalls) auf der die Daten erhebenden Webseite möglich.

TrustPid befindet sich derzeit im Technik-Test beim Axel-Springer-Verlag und kommt beispielsweise auf bild.de zum Einsatz. Dort erfolgt der Widerruf über separate Einwilligungsverwaltungen: „Widerruf Nutzerkennungen“ (TrustPid) und „Widerruf Tracking“ (Cookies). Die Provider behalten sich vor, dass die Löschung der TrustPid-Daten bis zu 90 Tage dauern kann. Ein Widerruf ist damit deutlich umständlicher als die Einwilligung und zudem sowohl in TrustPid als auch auf bild.de für Nutzer kaum erkennbar, da er lediglich in der Datenschutzerklärung, nicht aber auf der „Cookie-Wall“ Erwähnung findet (obwohl in letzterer die Einwilligung eingeholt wird).

Die deutschen Aufsichtsbehörden haben noch keine abschließende Bewertung zu TrustPid abgegeben. Für die Verwendung einer ähnlichen Technik hatte Verizon in den USA am 07.03.2016 einen Bußgeldbescheid der Federal Communication Commission über 1,35 Millionen US-Dollar erhalten.

Secorvo News

Spätsommerbildung

Wer schon vor dem Sommerurlaub wissen möchte, was sie oder er anschließend lernen wird, sollte sich unseren Frühbucherrabatt sichern: z. B. für das T.I.S.P.-Seminar (19.-23.09.2022) mit anschließender Möglichkeit zur Zertifizierung oder das Seminar IT Security Insights (27.-29.09.2022). Wir freuen uns auf Ihre Anmeldung und Ihren Besuch in Karlsruhe!

13. Tag der IT-Sicherheit

Wir freuen uns sehr, Sie zum diesjährigen Karlsruher Tag der IT-Sicherheit am **14.07.2022** in den Saal Baden der IHK Karlsruhe einladen zu können. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, dem Kompetenzzentrum für angewandte Sicherheitstechnologie am KIT (KASTEL) und dem CyberForum e.V. will den Er-

fahrungsaustausch unter IT-Sicherheitsverantwortlichen (nicht nur) in der TechnologieRegion Karlsruhe fördern.

Es erwarten Sie spannende Fachvorträge zu den Themen Digitale Souveränität, Sicherheit und Erklärbarkeit von KI, Quantencomputer und Cybersicherheit sowie sicheres Betriebssystem durch Asset-, Lifecycle- und Patch-Management – und ein intensives Buffet-Networking.

Das Programm und die Möglichkeit zur Anmeldung finden Sie hier.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2022	
11.-15.07.	PETS 2022 (University of Minnesota, Sydney/AUS)
11.-14.07.	DFRWS USA 2022 (DFRWS, virtuell)
14.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
August 2022	
06.-11.08.	Blackhat USA 2022 (Blackhat, Las Vegas/US)
07.-09.08.	SOUPS 2022 (usenix, Boston/US)
10.-12.08.	31st USENIX Security Symposium (usenix, Boston/US)
11.-14.08.	DEF CON 30 (DEFCON, Las Vegas/US)
13.-18.08.	Crypto 2022 (IACR, Santa Barbara/US)
September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)

Fundsache

Der beste Schutz gegen Cyberattacken sind sensibilisierte Mitarbeitende. Das ist das Zwischenergebnis einer Datenschutzprüfung zur Ransomware-Prävention des Bayerischen Landesamts für Datenschutz (BayLDA). Für Unternehmen werden Ransomware-Angriffe und wirksame Gegenmaßnahmen in einem Infoblatt und einer Handreichung checklistenartig erklärt.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, 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