secorvo
security consulting

Secorvo Security News

Juli 2020

Menschenrecht Anonymität

Menschen urteilen täglich. Vieltausendfach. Über Menschen. Wir müssen das tun, um angemessen auf unser Umfeld zu reagieren. Aber diese Urteile sind nie zutreffend und nur selten gerecht, denn es sind verkürzende, vereinfachende Bewertungen, die wir auf der Grundlage sehr begrenzter Detailkenntnis vornehmen. Das ist jedoch unvermeidlich – schließlich sind wir begrenzte Wesen: Kein Mensch, kein Richter könnte von sich behaupten, alle für ein Urteil relevanten Fakten und Hintergründe zu kennen. Doch da wir handeln müssen, müssen wir auch mit Halbwissen urteilen.

Und genau hier beginnt das Dilemma. Je mehr wir wissen, desto schwerer fällt es uns, ein Urteil zu fällen. Entgegenstehende Fakten trüben den Blick, lassen die Konturen von schwarz und weiß, von richtig und falsch unscharf werden. Das mag einer der Gründe sein, warum Vorurteile und generalisierte Bewertungen etwas bestechend Verlockendes an sich haben: Sie sind klar, rein, einfach – leider aber (fast) immer falsch. Denn sie zeichnen ein überscharfes (Zerr-) Bild der Wirklichkeit, das die komplexe, vielschichtige „Wahrheit" bestenfalls in einer ganz bestimmten Perspektive widerspiegelt.

Können wir einen Menschen mit irgendeiner Information in Verbindung bringen, fällen wir also unvermeidlich ein (wahrscheinlich ungerechtes) Urteil – sogar dann, wenn die Information unzuverlässig, sachfremd oder in diesem Kontext irrelevant ist. Genau deshalb brauchen wir Anonymität: Sie allein schafft einen urteilsarmen Raum, in dem neutraler Respekt und unvoreingenommener Umgang zwischen Menschen möglich wird. Und damit freie Entfaltung.

Am 10.07.2020 machte ein Beitrag auf netzpolitik.org das polnische Startup PimEyes bekannt, das aus im Internet verfügbaren Bildern biometrische Daten von mehr als 900 Mio. Gesichtern gewonnen haben will. Es bietet Gesichtsidentifikation für jedermann – der Anfang vom Ende der Anonymität. Wer aber anonyme Räume zerstört, schafft freie Entfaltung ab.

Inhalt

secorvo
security consulting

Security News

Ende des Privacy Shields

Der Europäische Gerichtshof hat am 16.07.2020 – wie von europäischen Datenschutzexperten erwartet – den Kommissionsbeschluss zum EU-US-Privacy Shield für ungültig erklärt. Auch die Standardvertragsklauseln werden im Urteil sehr kritisch beurteilt und dürften als Rechtsgrundlage für viele der bisher über das Privacy Shield legitimierten Verarbeitungen in den USA ausscheiden: Mit Rechtsvorschriften wie dem CLOUD Act (SSN 3/2019) garantiere das amerikanische Recht nach Auffassung des EuGH keinen dem EU-Recht äquivalenten Schutz personenbezogener Daten.

Damit hat der EuGH der Verarbeitung europäischer personenbezogener Daten in den USA, aber auch durch Töchter amerikanischer Unternehmen in Europa eine deutliche Absage erteilt – wer es dennoch tut, ist in der Nachweispflicht. Das wird auch aus den FAQ des europäischen Datenschutzausschusses zum Urteil deutlich, die dieser am 23.07.2020 veröffentlichte. Sollten die Aufsichtsbehörden nun gezielt Verarbeitungen personenbezogener Daten europäischer Bürger durch amerikanische Unternehmen mit Bußgeldern ahnden, dürfte eine Schockwelle durch Online-Marketing-Abteilungen schwappen.

Bußgeld für die AOK

Am 30.06.2020 teilte der Baden-Württembergische Beauftragte für Datenschutz und Informationssicherheit mit, dass seine Behörde gegen die AOK Baden-Württemberg ein Bußgeld in Höhe von 1,24 Mio. € verhängt hat. Im Zusammenhang mit Gewinnspielen hatte die AOK personenbezogene Daten erhoben und zu Werbezwecken verwendet; in mehr als 500 Fällen lag die dafür notwendige Einwilligung jedoch nicht vor. Bei der Bußgeldbemessung (SSN 10/2019) wurden das kooperative Verhalten der Krankenkasse, ihre Bedeutung für das Gesundheitssystem sowie die Belastung durch die Corona-Pandemie berücksichtigt. Wie hoch wäre es wohl ausgefallen, wenn diese begünstigenden Faktoren nicht vorgelegen hätten?

Angesichts unzureichender, aber immerhin vorhandener Maßnahmen und eines vergleichsweise geringen Anteils an rechtswidriger Werbeverwendung erscheint die Bußgeldhöhe kaum verhältnismäßig. Doch steigt damit der Druck auf Unternehmen, ihre Datenschutzumsetzung in der Praxis wirksamer zu überwachen.

Lunchgate

Die Sicherheitsfirma modzero veröffentlichte am 07.07.2020 eine Schwachstelle in der um eine Kontaktdatenfunktion erweiterte Tisch-Reservierungs-App des Schweizer Startups Lunchgate. Dem Bericht „Mit Webapps gegen COVID-19“ zufolge handelt es sich dabei um eine sogenannte Insecure Direct Object Reference, durch die alle erfassten Daten öffentlich einsehbar waren. Dabei fiel auf, dass Lunchgate die Kontaktdaten mindestens 21 statt der maximal zulässigen 14 Tage speichert. Lesen bildet: Ein Blick in die OWASP Cheat Sheets, hier konkret in das Insecure Direct Object Reference Prevention Cheat Sheet, hätte den Entwicklern geholfen, diese Lunchgate-Affäre zu vermeiden.

DSFA für CWA

Als die Corona-Warn-App (CWA) am 16.06.2020 zur Nutzung bereitgestellt wurde, hatte das Robert-Koch-Institut (RKI) erst vier Tage zuvor die zugehörige Datenschutz-Folgenabschätzung (DSFA) abgeschlossen. Der 117 Seiten lange Bericht dürfte eine der bislang meistdiskutierten und am besten durchleuchteten DSFA seit dem Inkrafttreten von Art. 35 DSGVO sein. Er orientiert sich am Standard-Datenschutzmodell (SDM) und berücksichtigt sämtliche in Art. 35 Abs. 7 DSGVO vorgegebenen Inhaltsbestandteile. So sind der Ablauf aus Nutzersicht, die Systemarchitektur, die Funktionsweise, die rechtliche Bewertung, die Analyse der Risiken für die Betroffenen und die getroffenen Maßnahmen ausführlich dokumentiert.

Dennoch werden dem Bericht datenschutzrechtliche Unerfahrenheit, Zielverfehlung (Legitimation statt Risikominimierung) und erhebliche Lücken attestiert, bspw. bei der Betrachtung der verwendeten Serverkomponenten und der möglichen Verknüpfung der Positivschlüssel mit den IP-Adressen bei der Übermittlung. Weitere Kritikpunkte sind das Ausklammern der Risiken durch das nicht kontrollierbare *Exposure Notifikation Framework* (ENF) von Apple und Google, durch das bestimmte Verarbeitungsschritte fremddiktiert werden, oder die Methodik der Risikobetrachtung. Die teilweise berechtigten Kritikpunkte erscheinen jedoch angesichts der Umstände (politischer Druck, Zeitdruck, vermeintliche Bedeutung der App) entschuldbar – zumal die öffentliche Diskussion über die Datenschutzkonformität der CWA zweifelsfrei dem Datenschutz gedient hat.

Bundesgenossen

Das Bundeskartellamt hat am 01.07.2020 den Abschlussbericht zur bereits im Dezember 2017 begonnenen Sektoruntersuchung zu Smart-TVs vorgelegt. Anlass der Untersuchung war der Verdacht auf erhebliche, dauerhafte Verstöße gegen verbrau-

cherrechtliche Vorschriften - mit einem Schwerpunkt beim Datenschutz.

Der Bericht dokumentiert erhebliche Datenschutzmängel wie zu pauschal bezeichnete Rechtsgrundlagen und Zwecke (bspw. „Verbesserung der angebotenen Dienste“), zu komplexe, unverständliche und zugleich undifferenzierte Datenschutzerklärungen, fehlende Angaben zu den verarbeiteten Daten, mangelnde Datensicherheit oder unerlaubte Werbung.

Dank des 9. Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) hat das Kartellamt seit dem 08.07.2017 mit § 32e Abs. 5 GWB die Befugnis zur Prüfung von Wirtschaftszweigen auf die Einhaltung von Verbraucherschutzrecht. Zuletzt hatte sich das Bundeskartellamt im Februar 2019 bereits mit dem Datenschutz bei Facebook beschäftigt (SSN 2/2019). Sollten weitere derartige Berichte folgen, könnte das Bundeskartellamt zu einem relevanten Player im Datenschutz werden.

Nun sind die Datenschutzaufsichtsbehörden aufgerufen, die im Bericht festgestellten Mängel aufzugreifen, dessen Untersuchungstiefe über viele Betrachtungen der Aufsichtsbehörden deutlich hinausgeht.

Videokonferenzsysteme – revisited

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat am 03.07.2020 vier einander ergänzende Dokumente zu Videokonferenzsystemen, darunter eine ausführliche Bewertung führender Angebote (u. a. GoToMeeting, Jitsi, Google Meet, Teams, Skype, WebEx und Zoom) samt Handlungsempfehlungen für Unternehmen und Behörden vorgelegt und damit ihre erste Stellungnahme vom 08.04.2020 (SSN 5/2020) ergänzt.

Der Checkliste zufolge soll vor jeder Videokonferenz geprüft werden, ob nicht eine Telefonkonferenz ausreicht. Weiter sollen selbst betriebene Dienste vorgezogen werden, da die vorhandenen Angebote überwiegend als „nicht rechtskonform einsetzbar“ eingestuft werden. Dabei wird zum einen auf das (derzeit für solche Telemediendienste noch nicht anwendbare) Telekommunikationsgeheimnis verwiesen; zum anderen geht die Prüfung davon aus, dass das organisierende Unternehmen grundsätzlich Auftragsverarbeitungsverträge schließen müsse – und diese würden für Teams, Google Meet und Co. nicht ausreichend angeboten.

Nicht näher analysiert wird allerdings, ob die Voraussetzungen für eine Auftragsverarbeitung überhaupt regelmäßig vorliegen. Hieran bestehen Zweifel, denn nicht jedes der Angebote muss als Dienst mit fester Nutzeranmeldung betrieben werden. Und selbst dann ist fraglich, warum die damit verbundene Übermittlung dienstnotwendiger Daten nicht zu rechtfertigen sein soll. Die Untersuchung reiht sich damit leider in eine Reihe durch die Corona-Krise ausgelöster, überhasteter Stellungnahmen zu Videokonferenzsystemen ein, auch wenn die mit deren Einsatz verbundene grundsätzliche Problematik nicht in Abrede zu stellen ist.

Wieder einmal Störerhaftung

Seit dem 3. Gesetz zur Änderung des Telemediengesetzes (TMG), das die Störerhaftung von WLAN-Betreibern durch die Neufassung von § 8 TMG begrenzen sollte, ist es um Filesharing-Urteile ruhig geworden. Daher sorgte die (noch nicht rechtskräftige) Verurteilung einer älteren Dame, die nach eigenen Angaben einen offenen WLAN-Knoten betrieben aber selbst nicht genutzt hatte, durch das Amtsgericht Köln vom 08.06.2020 für Aufsehen. Um den Erstattungsanspruch abzuwehren hätte sie nach Auffassung des Gerichts konkrete Nutzer im fraglichen Zeitpunkt benennen müssen.

Eine Rückkehr zur Störerhaftung ist trotz dieses Urteils zum Glück nicht zu fürchten. Allerdings ist es keine gute Entwicklung, dass durch subtile Differenzierungen des Klägers unkundige WLAN-Betreiber ohne anwaltliche Vertretung – wie in diesem Fall – Gefahr laufen, verurteilt zu werden.

Secorvo News

Endlich wieder... Seminare

Nach langer Pause können wir Ihnen im September wieder die Möglichkeit bieten, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren: für das Teilgebiet des sicheren Software-Engineerings (T.P.S.S.E., **14.–17.09.2020**) und das Zertifikat als TeleTrust Information Security Professional (T.I.S.P., **21.–25. 09.2020**).

Zur Vorbereitung auf das Seminar und die T.I.S.P.-Prüfung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“, das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist – und sich inzwischen zahlreicher positiver bis begeisterter Kritiken erfreut. Wer also noch eine Sommerlektüre sucht...

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2020	
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
07.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
17.-21.08.	Crypto 2020 (IACR, Santa Barbara/US)
September 2020	
07.-11.09.	IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/IT)
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-22.09.	Security of Things World (we.CONECT Global Leaders GmbH, Berlin)
21.-25.09.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)
24.09.	IT-Sicherheitsrechtstag (TeleTrusT e.V., Berlin)
29.09.-01.10.	IT-Sicherheit - praxisnah und aktuell (Secorvo, Karlsruhe)
29.09.-02.10.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)

Fundsache

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe hat am 16.06.2020 den Umsetzungsbericht 10 Jahre „KRITIS-Strategie“ veröffentlicht. Der bietet vertiefte Einblicke in die Risikobewertung und den Schutz der verschiedenen Sektoren kritischer Infrastrukturen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

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