Secorvo Security News

Januar 2022

Rechtsstaatsprinzip

Vor fünf Jahren hat das BVerfG in seinem Urteil zum NPD-Verbot die Prinzipien der freiheitlich-demokratischen Grundordnung präzisiert – die Wesenseigenschaften unserer politischen Ordnung, die uns von einer Diktatur unterscheiden. Darunter: die „Rechtsbindung der öffentlichen Gewalt" nach Art. 20 Abs. 3 GG. Polizei, Verwaltung und Regierung müssen sich an geltende Gesetze halten.

Zugegeben: Gesetze gibt es viele in Deutschland, und manche davon mögen mit heißer Nadel gestrickt sein. Doch das entbindet kein Organ der Exekutive von der im Grundgesetz verankerten Pflicht, sich daran zu halten. Damit ist es allerdings gelegentlich nicht weit her.

§ 28a Abs. 4 des Infektionsschutzgesetzes in der Fassung vom 18.11.2020 regelt den Umgang mit Coronabedingt erhobenen Kontaktdaten unmissverständlich: „Eine Weitergabe der übermittelten Daten durch die zuständigen Stellen nach Satz 3 oder eine Weiterverwendung durch diese zu anderen Zwecken als der Kontaktnachverfolgung ist ausgeschlossen."

Am 07.01.2022 meldete der SWR, dass die Mainzer Polizei für Ermittlungen in einem Unfall mit Todesfolge vom Gesundheitsamt die Kontaktdaten von 21 Gästen einer Mainzer Gaststätte angefordert und (unter Vortäuschung einer Infektion durch das Gesundheitsamt) erhalten hat – aufgrund einer „fehlerhaften Bewertung des Infektionsschutzgesetzes". Weitere Fälle seien nicht bekannt.

Inzwischen schon. In über 100 Fällen haben Staatsanwaltschaft und Polizei Kontaktlisten oder Kontaktdaten der Luca-App ausgewertet, wie das ZDF am 20.01.2022 berichtete. Soweit bekannt.

Offenbar gibt es Strafverfolger, die der Überzeugung sind, dass es in ihrer Entscheidungshoheit liegt, an welche Gesetze sie sich halten müssen – und an welche nicht. Genau diese Haltung ist es, die einen funktionierenden Rechtsstaat schleichend zu einem Unrechtsstaat mutieren lässt.

Security News

Videokonferenzen sind Telekommunikation

Mit Inkrafttreten der am 07.05.2021 verabschiedeten TKG-Novelle am 01.12.2021 fallen nun auch nummernunabhängige interpersonelle Telekommunikationsdienste (§ 3 Nr. 40 TKG) unter das TKG. Dahinter verbergen sich Messenger- und Videokonferenzdienste wie Teams oder Zoom. Statt der Datenschutzaufsichtsbehörden ist nun die Bundesnetzagentur zuständige Aufsichtsbehörde. Wichtige Folge: Für Telekommunikationsdienste müssen keine Auftragsverarbeitungsverträge nach Art. 28 DSGVO geschlossen

werden, denn die Kommunikation fällt unter das Telekommunikationsgeheimnis des Art. 10 GG. Die Grundsätze des Datenschutzes bleiben gültig und sind nach wie vor zu beachten; dennoch wird der Einsatz in Unternehmen dadurch wesentlich erleichtert.

Aus für Google Analytics?

Vor dem Hintergrund der Schrems II-Entscheidung des EuGH vom 16.07.2020 (C-311/18), nach der es für eine Übermittlung personenbezogener Daten in die USA entweder einer Einwilligung der Betroffenen oder eines Vertrags nach den aktuellen Standardvertragsklauseln der EU-Kommission sowie „zusätzlicher effektiver Maßnahmen" zur Herstellung eines gleichwertigen Schutzniveaus bedarf, entschied die österreichische Datenschutzbehörde (DSB) am 22.12.2021, dass die Datenübermittlung eines Webseitenbetreibers an Google mittels Google Analytics nicht mit der DSGVO vereinbar und somit illegal ist. Nach Ansicht der DSB verhindern die zusätzlichen Maßnahmen einen Zugriff der US-Behörden auf die übermittelten Daten nicht.

Zwar wurde weder entschieden, ob eine Anonymisierung der IP-Adressen eine Vereinbarung entbehrlich macht, noch, ob eine Übermittlung an Google Irland zulässig wäre. Die DSB weist jedoch darauf hin, dass eine IP-Adresse nur ein Teil des „digitalen Fußabdrucks" eines Nutzers sei.

Die Entscheidung kann als Indiz für die künftige Position der deutschen Aufsichtsbehörden gelten, zumal die europäischen Datenschutzbehörden bei diesem Thema offenbar in einer Task-Force zusammenarbeiten. Solange Google keine tiefgreifenden Änderungen an Google Analytics vornimmt, ist Betreibern von Webseiten ein Wechsel zu europäischen Anbietern zu empfehlen.

Ransomware-Prävention

Am 30.11.2021 hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) ein anlassloses Prüfverfahren zur Ransomware-Prävention gestartet. Die Fragen der Aufsichtsbehörde zielen auf die in den geprüften Einrichtungen getroffenen Schutzmaßnahmen vor Ransomware-Angriffen. Der Fragebogen, die Handreichung und ein Informationsblatt des BayLDA ist auch für nicht betroffene Unternehmen eine gute Orientierung hinsichtlich der zu treffenden Mindestschutzmaßnahmen.

MFA wird Standard

Für Kunden von Salesforce wird ab dem 01.02.2022 die Multi-Faktor-Authentifizierung (MFA) zum Standard. Eine begrüßenswerte Maßnahme, gilt doch eine Kennwort-Authentifikation bei Cloud-Diensten als Schwachstelle. Zwar schützt eine MFA nicht vor allen Angriffen, aber eine solche Vorgabe (vgl. SSN 09+10/2021) verbessert die Sicherheit signifikant.

Bei der Wahl der Authenticator App sollte der Fokus auf Benutzerfreundlichkeit, Sicherheit und Datenschutzaspekten liegen. So sollte die App für mehrere Dienste nutzbar sein und die Authentifizierungsdaten ausreichend geschützt speichern.

Koalitionsvorhaben

Informationssicherheit und Datenschutz misst die neue Bundesregierung nach dem am 07.12.2021 unterzeichneten Koalitionsvertrag erhebliches Gewicht bei: Im Abschnitt „Digitale Bürgerrechte und IT-Sicherheit“ werden ein „Recht auf Verschlüsselung“ und ein „wirksames Schwachstellenmanagement“ gefordert. Außerdem sollen Hersteller für Schäden durch fahrlässige IT-Sicherheitslücken in ihren Produkten haften. Staatliche Stellen sollen verpflichtet werden, „ihnen bekannte Sicherheitslücken beim BSI zu melden“ und ihre IT-Systeme regelmäßig einer externen Prüfung zu unterziehen. Dem staatlichen Ankauf von Sicherheitslücken erteilt die Koalition eine klare Absage, und im Bundespolizeigesetz soll es keine Ermächtigung mehr zu Quellen-TKÜ und Onlinedurchsuchung geben.

Zum Datenschutz plant die Regierung einen weiteren Anlauf für ein Beschäftigtendatenschutzgesetz (inzwischen ein „running gag“), will in einem „ambitionierten Abkommen“ mit den USA wieder datenschutzkonforme Datenübermittlungen auf europäischem Schutzniveau ermöglichen und die schon totgesagte E-Privacy-Verordnung wiederbeleben.

Orientierung im Einwilligungs-Dschungel

§ 25 des kürzlich in Kraft getretenen Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) regelt die Anforderungen an Einwilligungen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) hat daraufhin am 20.12.2021 eine neue Version ihrer Orientierungshilfe für Anbieter:innen von Telemedien veröffentlicht. Darin weist sie ausdrücklich darauf hin, dass nicht nur Cookies, sondern alle Tracking-Technologien einwilligungsbedürftig sind. Wichtig ist auch die Unterscheidung zwischen der Einwilligung nach DSGVO und TTDSG, da es für letztere eben nicht auf den Personenbezug ankommt.

Hinsichtlich der Einwilligungsverwaltung für Cookies zeigt der aktuelle Beschluss des VG Wiesbaden vom 01.12.2021, dass die Aufklärung bei Aufruf einer Webseite transparent erfolgen und zu dem passen muss, was im Hintergrund abläuft. Werden Funktionen bspw. zur Anzeige von Informationen verwendet, die eine Verbindung mit Servern im Nicht-EU-Ausland herstellen, muss die Einwilligung hierfür vor deren Ausführung eingeholt werden.

Datenschutz-Zertifizierungen

Bis zum Inkrafttreten der DSGVO waren das Gütesiegel und das Audit des Unabhängigen Landeszentrums für Datenschutz in Schleswig Holstein (ULD) die bekanntesten Datenschutzzertifizierungen. Mit Art. 42 und 43 DSGVO wurden datenschutzspezifische Zertifizierungsverfahren und Datenschutzprüfzeichen zum Nachweis der DSGVO-Konformität bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingeführt.

Nach der in der DSGVO gewählten Formulierung können Datenschutz-Produkte, -Prozesse oder -Dienstleistungen zertifiziert werden, nicht jedoch Datenschutz-Managementsysteme, obwohl diese Systeme oft Grundlage für datenschutzgerechte Produkte sind.

Der größte Bedarf an Zertifizierungen liegt sicherlich in der Zertifizierung von Auftragsverarbeitungen.

Als europaweit gemeinsame Grundlage für die Akkreditierung von Zertifizierungsstellen nach Art. 43 DSGVO hatte der Europäische Datenschutzausschuss im Dezember 2018 Leitlinien veröffentlicht. Daran anknüpfend haben die deutschen Datenschutzaufsichtsbehörden und die Deutsche Akkreditierungsstelle (DAkkS) einen Akkreditierungsprozess erarbeitet, der der DIN EN ISO/IEC 17065 und den ergänzenden Anforderungen der Datenschutzkonferenz folgt. Für in Deutschland tätige Zertifizierungsstellen wird die Akkreditierung durch die DAkkS zusammen mit der zuständigen Datenschutzaufsichtsbehörde erteilt.

Das von der DAkkS in einem Merkblatt veröffentlichte Musterzertifikat und die Ankündigungen verschiedener Datenschutzaufsichtsbehörden wie dem ULD lassen erwarten, dass es im Laufe des Jahres erste Datenschutz-Zertifizierungen geben wird.

Gefragter Staat

Beim Onlinekongress 2021 des Chaos Computer Club (CCC) stellte ReclaimYourFace das Ergebnis von 195 Anfragen zu Videoüberwachung im öffentlichen Raum vor, die sie über Fragdenstaat.de (auf Grundlage des Informationsfreiheitsgesetzes des Bundes und mehrerer Länder) an Polizeibehörden, Innenministerien und Datenschutzbehörden gesendet hatten. Nur auf 70 Anfragen erfolgte überhaupt eine Reaktion. 13 Angefragte lehnten eine Auskunft ab, 31 Anfragen wurden weiterverwiesen oder waren ergebnislos. Nur auf 26 Anfragen (13%) wurden Informationen herausgegeben, teilweise sehr ausführlich. In einigen Bundesländern wurden jedoch hohe Gebühren verlangt, zog sich der Vorgang über mehrere Monate hin oder kam erst auf Intervention von Datenschutzbeauftragten ins Rollen.

Kein besonders rühmliches Bild.

Secorvo News

T.I.S.P. und IT Security Insights

Wir hoffen, die nächsten Seminare wieder wie geplant in unseren Räumen in Karlsruhe durchführen zu können – das Zertifizierungsseminar T.I.S.P. (**07.–11.03.2022**) und das T.I.S.P.-Update-Seminar IT Security Insights (**15.–17.03.2022**) – und freuen uns auf Ihre Anmeldung.

Willkommen bei den Quanten

Der amerikanische Forscher Peter Shor schockte 1997 die Welt mit der Publikation eines Algorithmus', mit dem die Zerlegung sehr großer Zahlen in ihre Primfaktoren auf Quantencomputern in polynomieller Zeit gelingt – damit könnte man die wichtigsten der heute verwendeten asymmetrischen Kryptoverfahren brechen. Wie aber funktionieren Quantencomputer eigentlich? Warum lässt sich mit ihnen das „Faktorisierungsproblem" lösen? Sind auch symmetrische Verfahren wie der AES gefährdet? Bis wann müssen wir Ersatzverfahren verfügbar haben? Worauf sollten wir schon heute achten?

Um diese und weitere Fragen rund um Quantencomputer dreht sich das Expertengespräch von Professor Dr. Müller-Quade (KASTEL), Oliver Winzenried (WIBU-SYSTEMS) und Dirk Fox (Secorvo Security Consulting) auf dem Jahresstartevent der KA-IT-Si am **03.02.2022**. Die limitierten Präsenzplätze im jüngst eröffneten IT Security Club des „House of IT Security" der Karlsruher WIBU Systems sind bereits ausgebucht, aber Sie können das Expertengespräch per Livestream miterleben (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2022	
01.-02.02.	18. Deutscher IT-Sicherheitskongress (BSI, virtuell)
03.02.	KA-IT-Si-Event „Willkommen bei den Quanten" (KA-IT-Si, hybrid)
02.-04.02.	29. DFN-Konferenz „Sicherheit in vernetzten Systemen" (DFN-CERT, virtuell)
März 2022	
07.-11.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.-17.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, virtuell)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)
April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, 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