Secorvo Security News

Mai 2023

Tröpfchen

Ohne Einwilligung, gesetzliche Grundlage oder einen Vertrag ist die Verarbeitung personenbezogener Daten verboten. Das gilt auch für Daten, die nach Vertragsende oder Ablauf einer Aufbewahrungspflicht noch in Systemen schlummern.

Diese Daten sind der Kern des (Datenschutz-) Problems. Sie erlauben eine Rekonstruktion vieler unserer Lebensbereiche: Reisen (Flug- und Bahnkarten, GPS-Daten), Nutzung (Apps, Browser, Online-Shops) und Kommunikation (Telefonie, E-Mail, Messenger). Inzwischen protokollieren auch Geräte (Autos, Saugroboter, Sportuhren, ...) unser Leben. Wer diese Daten kennt, kennt die Menschen: ihre Kaufentscheidungen, ihr Sozialverhalten und ihre Freizeitbeschäftigungen, ihre Gesundheit, ihr Fahrverhalten und ihre Vorlieben. Und damit wachsen auch die Begehrlichkeiten – sowohl kommerzielle als auch staatliche.

Welche Größenordnungen letztere schon heute annehmen zeigt eine Antwort der Bundesregierung auf eine Anfrage im Bundestag vom 27.04.2023 zu Fluggastdatenabfragen: 424 Mio. Datensätze von 121 Mio. Passagieren wurden von den Fluggesellschaften 2022 an das Bundeskriminalamt (BKA) geliefert. Damit wurden rund 19.800 zur Fahndung ausgeschriebene Passagiere identifiziert und es kam zu knapp 1.400 Festnahmen – 0,001% der von den BKA-Abfragen betroffenen Personen. In 99,999% der Fälle wurden vom BKA also Daten von Unschuldigen erhoben und verarbeitet. Klammern wir die Kosten für den Aufbau (54 Mio. €) und den Betrieb (14,5 Mio. €, also 10.500 € je Festnahme) des Fluggastdatensystems einmal aus: Kann man das noch „verhältnismäßig" nennen?

Dabei hat das BKA die Auto- und Scooterverleiher noch gar nicht entdeckt. Viele speichern bislang praktisch unkontrolliert GPS-Daten – meist ohne Löschfristen. Erst am 28.03.2023 hatte die französische Aufsichtsbehörde CNIL ein Bußgeld gegen Cityscoot verhängt (125.000 €). Ein Tröpfchen auf einem glühenden Stein.

Security News

Eine Kopie ist (k)eine Kopie

Am 04.05.2023 stellte der EuGH zum datenschutzrechtlichen Auskunftsanspruch nach Art. 15 DSGVO klar, dass es nicht ausreicht, den Betroffenen Auskunft in Form allgemeiner Beschreibungen der Daten bzw. Datenkategorien zu geben. Das Recht auf Kopie bedeutet, dass „der betroffenen Person eine originalgetreue und verständliche Reproduktion aller dieser Daten" zu übermitteln ist. Ist dies nicht möglich, müssen die verarbeiteten Daten so zur Verfügung gestellt werden, dass „der betroffenen Person die wirksame Ausübung der ihr durch diese Verordnung verliehenen

Rechte“ ermöglicht, dabei aber auch die Rechte und Freiheiten anderer berücksichtigt werden. Damit werden insbesondere Geschäftsgeheimnisse und die Rechte Dritter geschützt. Dem Anspruch auf eine originalgetreue Kopie dürfen die Verantwortlichen also nicht uneingeschränkt nachkommen, sondern müssen eine Abwägung mit Rechten und berechtigten Interessen Dritter vornehmen.

Recovery Attack

Zusätzliche Sicherheitsmechanismen können auch zusätzliche Risiken bergen, wie Apples Recovery Key beweist. Der bereits 2014 eingeführte Mechanismus schützt die Apple-ID: Hat man das Kennwort zu seiner Apple-ID vergessen oder wurde es bei einem Angriffsversuch gesperrt, kann es mit einem vorher erzeugten, 28-stelligen zufälligen Recovery Key zurückgesetzt werden. Den Key sollte man außerhalb des Geräts speichern oder ausgedruckt in einen Tresor legen. Seit iOS 14 (2020) unterstützt Apple nach Aktivierung des Recovery Keys kein anderes Rücksetzungsverfahren mehr. Damit kann der Mechanismus nach hinten losgehen: Gewinnt ein Angreifer kurzzeitig physischen Zugriff auf das iPhone, kann er einen Recovery Key wählen oder einen bestehenden durch einen neuen ersetzen. Damit kann sich der Angreifer später jederzeit Zugriff auf die Apple-ID und damit das iCloud-Backup aller zugehörigen Geräte verschaffen – und den Geräteinhaber „aussperren“.

Vertrauenskett(ch)en

Wer eine Vertrauenskette aufbaut, steht vor dem gleichen Dilemma wie Baron Münchhausen, der sich samt Pferd am eigenen Zopf aus dem Sumpf zog – im echten Leben gelingt das nur mit einer standfesten Verankerung. In der angelsächsischen Version der Legende zieht der Protagonist sich an den eigenen Stiefelriemen heraus – er „boot strap“-t.

Ist im Betriebssystem Secure-Boot aktiviert, prüft es, ob die UEFI-Firmware des Computers korrekte Daten zur Integritätsprüfung übergibt. Wie UEFI die herleitet, ist eine andere Frage. Um den Vertrauensanker dazu möglichst stabil zu gestalten, bietet Intel (in teureren CPUs) das Boot-Guard Verfahren an, dessen Details leider nicht offengelegt sind. Die Grundzüge sind wie folgt: Ein Computerhersteller kann über „Fuses“ den Hashwert eines eigenen Public-Keys in die verbaute CPU brennen. Mit dessen Hilfe prüft der Microcode in der CPU die Integrität des ersten UEFI-Codeblocks, noch ehe ein Befehl aus der Firmware des Computers aufgerufen wird.

Dumm nur, wenn, wie Anfang Mai MSI und zuvor schon Lenovo passiert, der Private-Key dazu entschlüpft. Noch schlimmer, wenn der Mechanismus gar nicht aktiviert ist und eine UEFI-Malware den eigenen Key in die CPU-Fuses brennen könnte, um sich auch dort schon einzunisten – und somit Firmware-Updates zum Entfernen der UEFI-Malware selbst dem Hersteller nur noch durch Austausch der CPU möglich wären.

Insgesamt fehlt es der Secure-Boot-Vertrauenskette an Transparenz und Aufsicht. Im Web-PKI-Ökosystem ist – trotz Verbesserungspotenzials auch dort – die

Vertrauenskette um Größenordnungen besser etabliert. Das CA/Browser-Forum ist die Steuerungsinstanz, die Requirements transparent veröffentlicht und ein recht striktes Aufsichts-Regime mit jährlichen Audits, Certificate Transparency usw. etabliert hat. Secure-Boot sollte da bald nachziehen, damit dessen Vertrauenskette nicht dauerhaft auf tönernen Füßen steht – und dessen Nutzer sich in falscher Sicherheit wähnen, wenn Secure-Boot aktiviert ist.

Top Secret

Am 24.11.2022 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Stellungnahme zum datenschutzkonformen Einsatz von Microsoft 365 (SSN 11/2022) und stellte dabei Anforderungen an den Auftragsverarbeiter, die sich so nicht in der DSGVO wiederfinden. Daraufhin hat Microsoft zum 01.01.2023 das EU Data Boundary eingeführt (SSN 12/2022), wonach personenbezogene Daten im beschriebenen Rahmen innerhalb der EU gespeichert und verarbeitet werden sollen. An der Position der DSK hat sich jedoch nichts geändert.

Mittlerweile haben die Länder ein Rechtsgutachten zum Datenschutz konformen Einsatz von MS 365 anfertigen lassen. Ein Antrag von Frag den Staat auf Überlassung des Gutachtens wurde am 14.02. 2023 abgelehnt. Begründung: Die Herausgabe dürfe nicht dazu führen, dass sich Dritte durch darin enthaltene Informationen wirtschaftliche Vorteile zu Lasten öffentlicher Haushalte verschaffen (§ 14 Nr. 7 Landestransparenzgesetz Rheinland-Pfalz). Darüber hinaus würde eine Herausgabe das Verfahren zum Einkauf cloudbasierter Software und deren Vertragsmodalitäten – und damit die Verhandlungsposition gegenüber Microsoft – *„erheblich beeinträchtigen“* (§ 6 lit. b IFG NRW). Eine Anfrage von golem wurde ebenfalls abgelehnt.

Dabei liegt doch ein datenschutzkonformer Einsatz von Microsoft 365 mit geeigneten technischen und organisatorischen Mahnahmen im Interesse aller Beteiligten. Da fragt man sich doch, wie ein offenes und transparentes Vorgehen die Verhandlungsposition der Länder wohl schwächen könnte…

Kausalitätsprinzip

Am 04.05.2023 hat der EuGH die Voraussetzungen für das Vorliegen eines immateriellen Schadens nach Art. 82 DSGVO konkretisiert. Demnach setzt der Schadensersatzanspruch für immaterielle Schäden nicht voraus, dass der Schaden eine gewisse Erheblichkeit erreichen muss. Auch führt ein bloßer Verstoß gegen die Regelungen der DSGVO nicht automatisch zu einem Schadensersatzanspruch. Vielmehr bedarf es (1) eines Verstoßes gegen die DSGVO, (2) eines materiellen oder immateriellen Schadens, der aus diesem Verstoß resultiert, und (3) eines Kausalzusammenhangs zwischen Schaden und Verstoß. Dies entspricht dem deutschen Schuldrecht, welches ebenfalls einen kausalen Schaden als Voraussetzung für den Schadensersatz verlangt (§ 280 Abs. 1 BGB).

Zwar steigt durch das Urteil des EuGH das Risiko für Unternehmen auf Schadensersatzansprüche durch

Betroffene, allerdings wird sich in der Praxis der Nachweis eines immateriellen Schaden schwierig gestalten.

Geburtstagswünsche

Mit Inkrafttreten der DSGVO am 25.05.2018 wurde innerhalb des Europäischen Wirtschaftsraums ein „einheitliches Datenschutzrecht" geschaffen und das Recht auf informationelle Selbstbestimmung der Betroffenen gestärkt.

Allerdings mangelt es noch immer an einer konsequenten Durchsetzung und Kontrolle durch die Aufsichtsbehörden. Zwar erhielten die deutschen Aufsichtsbehörden im letzten Jahr ein Gesamtbudget von ca. 114 Millionen Euro, das deutlich über dem Budget anderer Mitgliedstaaten liegt. Doch verursacht der Föderalismus unterschiedliche Interpretationen und Durchsetzungsansätze bei den 17 deutschen Aufsichtsbehörden (inklusive der Sonderzuständigkeiten für Medien und Kirchen). Beschwerden konnten im letzten Jahr nicht zufriedenstellend bearbeitet werden. So kam es entweder nur zu geringen oder gar keinen Bußgeldern. Viele Beschwerden wurden insbesondere durch die Schaffung einer „Erheblichkeitsschwelle" abgewiesen. Auch mangelt es an Transparenz, da – anders als in anderen Mitgliedstaaten – die Entscheidungen der Aufsichtsbehörden nicht konsequent veröffentlicht werden. Der Fokus liegt auf Informations- und Beratungstätigkeit und nicht auf konkreten Entscheidungen, wie sie beispielsweise zum Einsatz von Microsoft 365 überfällig wären.

Auch bei anderen europäischen Aufsichtsbehörden wird ein Großteil der Beschwerden nicht bearbeitet. Darüber hinaus zeigt der Bericht der ICCL deutlich, dass die irische Aufsichtsbehörde noch immer die Rolle eines Verhinderers bei der Durchsetzung des Datenschutzes gegen große IT-Unternehmen spielt. So wurden in der Vergangenheit rund 88 % der Entscheidungen der irischen Datenschutzbehörde durch den Europäischen Datenschutzausschuss außer Kraft gesetzt. Zum Geburtstag wünschen wir der DSGVO klarere Entscheidungen, einheitlichere Auslegungen des Datenschutzrechts und in der Höhe abgestimmte Bußgelder.

Secorvo News

Secorvo Seminare

Auf unserem Spätsommer-T.I.S.P.-Seminar vom **18. bis 22.09.2023** sind noch Plätze frei. Wir freuen uns auf Ihre Anmeldung.

Wo, bitte, ist meine schwache Stelle?

Schwachstellen sind die Kletterhaken der Angreifer – wer Software entwickelt, muss sie meiden wie der Teufel das Weihwasser. Wie man mit Hilfe von Vulnerability Management Systemen Schwachstellen sucht und bewertet, erfahren Sie am **22.06.2023** um **18 Uhr** auf dem kommenden Event der KA-IT-Si von den Experten der WIBU-Systems. Genießen Sie beim anschließenden „Buffet-Networking" den Sommer auf der Dachterrasse. Schnell anmelden – die Zahl der Plätze ist begrenzt.

Back to normal

Endlich wieder im bewährten Format: Der 13. Tag der IT-Sicherheit findet am **20.07.2023** ab **14 Uhr** im Saal Baden der IHK Karlsruhe statt.

Es erwarten Sie Fachvorträge u. a. zur Bedrohung durch Quantencomputer, den Herausforderungen durch KI und zum Patchmanagement – sowie ein intensives Buffet-Networking. Hier geht's zu Programm und Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2023	
12.-13.06.	DuD 2023 (COMPUTAS, Berlin)
14.-15.06.	Entwicklertag 2023 (VKSI, GI, ObjektForum, Karlsruhe)
19.-23.06.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
22.06.	Wo, bitte, ist meine schwache Stelle? (KA-IT-Si, Karlsruhe)
Juli 2023	
03.-07.07.	8th IEEE European Symposium on Security and Privacy (IEEE, Delft/NL)
09.-12.07.	DFRWS USA 2023 (DFRWS, hybrid)
10.-15.07.	PETS 2023 (Université de Lausanne, hybrid)>
20.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL Karlsruhe)

Fundsache

Die aktualisierte Handreichung zum "Stand der Technik" des TeleTrusT vom 09.05.2023 führt technische und organisatorische Maßnahmen auf, die gemäß definiertem Bewertungsschema von Unternehmen und Institutionen umgesetzt werden sollten. Die Handreichung wird kontinuierlich weiterentwickelt, ergänzt und stellt in kompakter Form die jeweilige Maßnahme vor und welche Schutzziele sie unterstützt. Aus unserer Sicht absolut lesenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, 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