secorvo
security consulting

Secorvo Security News

April 2023

Lernen durch Schmerzen

In jüngster Zeit mussten sich Gerichte vermehrt mit Schadensersatzklagen im Zusammenhang mit Datenschutzverstößen befassen. Immer wieder war dabei die Frage zu beantworten: Reicht es für einen Schmerzensgeldanspruch, dass sich ein Datenschutz-Risiko verwirklicht hat? Und falls ja, welches Schmerzensgeld ist angemessen?

Gemäß Art. 82 Abs. 1 DSGVO lässt sich die erste Frage schnell mit „Ja“ beantworten: Haftung und Verantwortung sind Wesenselemente des europäischen Datenschutzrechts. Allerdings messen die Gerichte mit zweierlei Maß: Bei Daten-Scraping (also dem Abgreifen personenbezogener Daten, die bspw. über ein Social-Media-Profil zugänglich sind) wird ein Schadensersatzanspruch in der Regel abgelehnt (so z.B. vom LG Gießen am 03.11.2022), selbst wenn die Betroffenen dabei ein „schlechtes Gefühl“ beschleicht. Anders sieht es bei einem „richtigen“ Datenschutzvorfall aus: Dann besteht ein Anspruch unabhängig davon, ob die Betroffenen durch das verwirklichte Risiko tatsächlich einen Schaden erlitten haben oder nicht – es reiche aus, dass die Betroffenen ein wenig Bauchgrummeln verspüren (so das OLG Hamm am 20.01.2023). Denn wenn nur genügend Betroffene ihre Ansprüche geltend machen würden, sei das in der Summe für den Verantwortlichen schmerzhaft, und Abschreckung müsse schließlich sein.

Übersehen wird dabei allerdings, dass für einen Schadensersatzanspruch auch ein materieller oder immaterieller Schaden entstanden sein muss – ein „Strafschmerzensgeld“ ist dem deutschen Recht nicht bekannt. Und das aus gutem Grund: Für die Sanktionierung von Datenschutzvorfällen und -verstößen sind die Datenschutz-Aufsichtsbehörden zuständig – und sollen das auch bleiben. Der Spagat zwischen einem wirksamen Grundrechtsschutz und der vorsätzlichen missbräuchlichen Ausnutzung lässt sich nur durch eine einheitliche Rechtsprechung bewältigen.

Inhalt

secorvo
security consulting

Security News

Grundschutz in der Cloud

Am 03.04.2023 hat Microsoft drei Leitfäden zur Umsetzung von IT-Grundschutz bei der Nutzung der Cloud-Lösungen Azure, Office 365 und Dynamics 365 veröffentlicht. In den Workbooks wird zu den Anforderungen aus dem Baustein OPS.2.2 des Grundschutz-Kompendiums zur Cloud-Nutzung erläutert, welche Microsoft-Funktionen und Konfigurationen deren Umsetzung unterstützen. Die Workbooks enthalten Referenzen auf weiterführende Microsoft-Informationen, und in einem weiteren Kapitel wird ausgeführt, was zur Erfüllung des „Mindeststandards des BSI zur Nutzung externer Cloud-Dienste“ (NCD.2) zu tun ist.

Angesichts der zahlreichen von Microsoft zur Verfügung gestellten Funktionen und Optionen sind die Leitfäden eine wertvolle Hilfestellung für alle am IT-Grundschutz ausgerichteten IT-Infrastrukturen, die die Microsoft-Cloud nutzen. Der Bericht der europäischen Datenschutz-Aufsichtsbehörde (edpb) vom 17.01.2023 über die Prüfung der Nutzung von Cloud-Diensten im öffentlichen Bereich dürfte Microsoft motiviert haben, die Nutzer bei der Umsetzung der technischen und organisatorischen Schutzmaßnahmen besser zu unterstützen.

Bauchschmerzen

Das OLG Hamm entschied am 20.01.2023, dass für einen Schadensersatzanspruch ein „schlechtes Gefühl“ der von einer Datenpanne betroffenen Person ausreicht. Nur wenn der Verantwortliche beweisen kann, dass er in keinerlei Hinsicht für die Panne verantwortlich ist, ist seine Haftung nach Art. 82 Abs. 3 DSGVO ausgeschlossen. Dafür müssen sämtliche notwendigen technischen und organisatorischen Maßnahmen ergriffen, umgesetzt und ausreichend dokumentiert sein.

Dies gilt übrigens auch für die Frage, ob eine nicht umfänglich erteilte Auskunft einen Schadensersatzanspruch auslösen kann (siehe Urteile des LAG Niedersachsen und des LArbG Nürnberg). Wer nicht zwischen den Mahlsteinen der Justiz zerrieben werden will, erteilt die Auskunft so, wie es Art. 12 DSGVO vorsieht. Dafür unerlässlich ist ein Datenschutzmanagement mit etablierten und dokumentierten Regelungen und Prozessen.

Software Security Game

Am 21.03.2023 hat GitHub als Teil seiner Ausbildungsangebote ein Spiel veröffentlicht, mit dem sich die Kenntnisse zur Sicherheit von Software trainieren lassen. Dieses Secure Code Game richtet sich an Entwickler, die Schwachstellen in Software besser erkennen und vermeiden wollen. Der Fokus liegt auf der Programmiersprache Python, doch sind die vermittelten Konzepte größtenteils sprachunabhängig. Das Spiel kann lokal geclont oder in GitHub Codespaces genutzt werden.

Jahr des DSB

Der Europäische Datenschutzausschuss (EDSA) hat am 15.03.2023 für das Jahr 2023 eine koordinierte Prüfung der Situation der Datenschutzbeauftragten (DSB) angekündigt. Geprüft werden soll, ob die DSB gemäß den Vorgaben der Art. 37-39 DSGVO organisatorisch eingebunden und mit ausreichenden Ressourcen ausgestattet sind. Dazu werden zunächst Fragebögen an die DSB verschickt (deren Auswertung später zur Verfügung gestellt werden soll), ggf. gefolgt von förmlichen Untersuchungen der nationalen Aufsichtsbehörden.

Mut zum Besseren

„Das Bessere ist der Feind des Guten“ wusste schon Voltaire. Hätte es damals schon IT gegeben, wären ihm allerdings Zweifel gekommen – denn da hält man gerne an Bewährtem fest, solange z. B. Kryptoverfahren nicht komplett gebrochen sind. Das war schon bei der Hashfunktion SHA-1 so, bis das CA/Browser-Forum 15 Jahre später den Einsatz des Nachfolgers SHA-2 erzwang.

Für die Linux-Festplattenverschlüsselung LUKS hat der Linux-Entwickler Matthew Garrett am 17.04.2023 empfohlen, von älteren Versionen mit der Schlüsselableitung per PBKDF2 (Ursprung 1993) auf das vor 9 Jahren eingeführte LUKS2 mit Argon2id zu wechseln. Zwar muss man dem dieser Empfehlung zu Grunde liegenden Gerücht über einen erfolgreichen Angriff auf PBKDF2 mit Skepsis begegnen. Aber Argon2 wurde gegen Angriffstypen gehärtet, die beim Design von PBKDF2 noch gar nicht „auf dem Schirm“ waren. Daher sollte man den Mut zum Besseren haben – der Wechsel wird sicherlich weniger schmerzen als vielleicht befürchtet.

Der Preis ist heiß

Neben den klassischen Cookie-Bannern gibt es – insbesondere auf Webseiten mit „redaktionellen Inhalten“ – Cookie-Walls, bei denen die Nutzer entscheiden müssen, ob sie mit Daten (Zustimmung zu Tracking und Werbung) oder mit Geld bezahlen wollen (Pur-Abo). Die DSK hat am 22.03.2023 entschieden, dass solche Abo-Modelle zulässig sind, wenn beide Varianten (Tracking und Geldzahlung) gleichwertig sind. Dafür müssen „die Angebote zumindest dem Grunde nach die gleiche Leistung umfassen“. Leider klärt die DSK nicht, welches Entgelt angemessen ist und verweist nur auf die Marktüblichkeit. Das ist bedauerlich, da ein unan-

gemessenes Entgelt die Freiwilligkeit der Einwilligung in Frage stellen kann.

Patchpolizei Exchange

Im Exchange-Team-Blog kündigte Microsoft am 23.03.2023 an, dass Exchange-Server in der Cloud zukünftig sukzessive keine Nachrichten mehr von ungepatchten on-premise-Exchange-Servern annehmen werden. Betreiber verwundbarer Exchange-Server sollen erst informiert, dann der Empfang gedrosselt und, sofern innerhalb von 90 Tagen keine Abhilfe geschaffen wird, die Verbindung abgebrochen werden. Betroffene E-Mail-Absender werden darüber informiert.

Keine Frage: Für die „Internet-Hygiene“ und die Sicherheit der Allgemeinheit ist es eine gute Sache, wenn Patch-Muffel unter Druck gesetzt werden. Aber maßt sich Microsoft hier nicht eine bestenfalls hoheitliche Aufgabe an? Und was passiert mit nicht gepatchten Postfix-Mailservern? Oder veralteten Webservern? Sollte in solchen Fällen zukünftig auch ein E-Mail-Empfang als erzieherische Maßnahme verweigert werden? Aber bei wem liegt die Verantwortung, wenn einem Nutzer, der den Patch-Stand des Servers seines Providers nicht beeinflussen kann, durch die Nichtzustellung einer Nachricht ein Schaden entsteht? Zwar wird man Microsoft nicht vorwerfen können, dass dabei Nachrichten unterdrückt werden, um einem Dritten einen Nachteil zuzufügen (§ 274 Abs. 1 StGB). Allerdings könnten die verweigerten E-Mails einwandfrei sein, nur eben der versendende „Gammel“-Server nicht: In diesem Fall läge nicht zwingend eine Bedrohung für Exchange-Online vor. Daher empfehlen wir eine genauere Betrachtung der insbesondere rechtlichen Implikationen einer solchen Zwangsmaßnahme.

Datenschutzmanagement

Ein Verarbeitungsverzeichnis muss regelmäßig gepflegt werden; darauf weist der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) in einer Kurzinformation vom 01.04.2023 hin.

Die Umsetzungstipps sind nicht nur für öffentliche Stellen wertvoll. Dennoch greift diese Sicht zu kurz: Nicht nur das Verzeichnis der Verarbeitungstätigkeiten, sondern alle wesentlichen Datenschutz-Dokumente sollten regelmäßig, mindestens jährlich auf Vollständigkeit, Aktualität, Eignung und Korrektheit überprüft werden. Dazu sind, wie beim Informationssicherheitsmanagement, die notwendigen Abläufe (Prozesse) festzulegen und umzusetzen. Genau das sind Wesenselemente eines Datenschutzmanagementsystems – es wird Zeit, dass die Aufsichtsbehörden diese Gesamtsicht in den Blick nehmen.

Gesetzgeber gefordert

Mit seinem Urteil vom 30.03.2023 hat der Europäische Gerichtshof (EuGH) festgestellt, dass die Regelung in § 2 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes den Anforderungen der DSGVO nicht genügt. Damit dürfen diese und gleichlautende Regelungen zum Beschäftigtendatenschutz (also auch § 26 BDSG) nicht mehr angewendet werden. Wer seine Datenverarbeitungen auf diese Rechtsgrundlage stützt, sollte schnellstmöglich nach einer Alternative suchen. Die Rechtmäßigkeit der Verarbeitung richtet sich nunmehr ganz allgemein nach Art. 6 Abs. 1 DSGVO, solange die Gesetzgeber des Bundes und der Länder nicht durch entsprechende (neue) Regelungen dafür sorgen, dass ein Beschäftigtendatenschutz in Deutschland endlich vernünftig eingeführt und umgesetzt wird (was die DSK schon seit Längerem fordert).

Secorvo News

Seminare

Bereiten Sie sich mit unserem T.I.S.P.-Seminar vom **19. bis 23.06.2023** auf Ihre Zertifizierung vor: In 18 Lernmodulen vertiefen Sie Ihr Wissen in Informationssicherheit und Datenschutz. Bei Buchung bis zum 14.05.2023 profitieren Sie von unserem Frühbucherrabatt. Wir empfehlen eine schnelle Anmeldung – es sind nicht mehr viele Plätze frei.

Wo 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, wird das Thema des nächsten KA-IT-Si-Events am **22.06.2023** um 18 Uhr in den wunderbaren Räumen der WIBU-Systems (IT Security Club) sein. Wir freuen uns auf Ihre Anmeldung!

Tag der IT-Sicherheit

Nach zwei ausgefallenen (2020, 2022) und einer reinen Online-Veranstaltung (2021) wird der 13. Tag der IT-Sicherheit in diesem Jahr endlich wieder im bewährten Format in der IHK Karlsruhe stattfinden. Zusammen mit KASTEL, dem CyberForum und der IHK laden wir sie herzlich ein, am **20.07.2023** ab 14 Uhr mit Experten, IT-Sicherheits- und Datenschutzbeauftragten über aktuelle Herausforderungen wie Quantencomputer, KI und Patch-Management zu diskutieren. Auch hier empfehlen wir eine frühe Anmeldung – die Zahl der Plätze ist begrenzt (und die Nachfrage groß).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2023	
04.05.	KA-IT-Si-Event: "AD = Anno Domini?" (KA-IT-Si, Karlsruhe)
09.-10.05.	BvD Verbandstag 2023 (BvD, Berlin)
09.-12.05.	Blackhat Asia 2023 (Blackhat, Singapur/ASE)
09.-12.05.	European Identity and Cloud Conference 2023 (KuppingerCole, hybrid)
10.-14.05.	ISSE 2023 (IEEE, Timisoara/ROU)
10.-11.05.	19. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-24.05.	Omnisecure 2023 (in TIME berlin, Berlin)
23.-24.05.	24. Datenschutzkongress (EUROFORUM, Berlin)
23.-24.05.	IMF 2023 (Fraunhofer-Institut IAO, München)
Juni 2023	
01.-02.06.	Annual Privacy Forum 2023 (ENISA et al., Lyon/FR)
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)
21.-22.06.	31. ID:SMART Workshop (Fraunhofer SIT, Darmstadt)
22.06.	Wo, bitte, ist meine schwache Stelle? (KA-IT-Si, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Stefan Gora, Kai Jendrian, Hans-Joachim Knobloch, Oliver Oettinger, 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