Secorvo Security News

Februar 2022

Zutatenverzeichnis

Ende des kommenden Jahres feiert die Regelung ihren 40. Geburtstag: Seit dem 26.12.1983 kennt das deutsche Lebensmittelrecht die Pflicht, jedem Produkt auf der Verpackung eine Zutatenliste in absteigender Reihenfolge der Zugabemenge beizufügen. Dank dieser Transparenz kennen Verbraucher seitdem die Bestandteile ihrer Nahrungsmittel und können somit Unverträglichkeiten vermeiden und die Qualität angebotener Lebensmittel einschätzen. Das ist sicherlich eine der wichtigsten Regelungen des Lebensmittelrechts, die zweifellos bereits viele Menschen mit schweren Allergien das Leben gerettet hat.

Leider sind wir in der Informationstechnik von einer solchen Offenheit weit entfernt. Dabei mixt inzwischen jeder Softwareentwickler unzählige Bibliotheken und Codefragmente beliebiger Provenienz in „seine" Programme – dank Cloud-Services, Open Source und offenen APIs mit steigender Tendenz. Kaum eine Entwicklungsumgebung, die ohne eigene Bibliotheksfunktionen daherkommt, kaum ein Softwareprodukt, das keinen Open Source-Code unter seiner Haube verbirgt. Letzteres unterliegt zwar klaren Offenlegungsregeln, die aber bei weitem nicht von jedem Hersteller beachtet werden.

Das Ergebnis dieser wachsenden Code-Mehrfachnutzung kann ein erheblicher Risikoanstieg sein: Wird ein Sicherheits-Bug in einer der verwendeten Bibliotheken oder Open-Source-Code-Basen bekannt, erfahren Nutzer davon nur, wenn der Hersteller sie warnt und Patches liefert. Das setzt allerdings voraus, dass der Hersteller die verwendeten Code-Teile sauber dokumentiert – und auch seine „Code-Zulieferer" dasselbe bei ihrem Programmcode tun.

Verlass ist darauf keineswegs: Wird ein Bug bekannt, geht die Suche los – und die Schwachstelle wird in einigen Anwendungen erst nach Wochen gefixt. Wäre der Hersteller zur Dokumentation seiner Code-Zutaten verpflichtet, könnte der Käufer das diesbezügliche Risiko schon vor dem Erwerb einschätzen.

Security News

TCF nicht DSGVO-konform

Die belgische Datenschutzbehörde (APD) hat am 02.02.2022 entschieden, dass das Transparency and Consent Framework (TCF) der IAB Europe gegen die DSGVO verstößt. Das TCF ordnet mittels eines sogenannten TC-Strings und eines Consent-Cookies das Verhalten des Nutzers dessen IP-Adresse zu und ermöglicht die Versteigerung zielgruppenspezifischer Werbeplätze. Nach Ansicht der ADP mangelt es dabei an einer Rechtsgrundlage, transparenten Informationen sowie ausreichenden technischen und organisatorischen Maßnahmen. IAB Europe sei zudem ihren

Pflichten als Verantwortliche nicht nachgekommen. IAB will die Entscheidung rechtlich prüfen, zeigt sich aber optimistisch, dass die Verstöße behoben werden können. Sollte IAB nicht nachbessern, bleibt möglicherweise das RTB-Protokoll von Google als einzige technische Alternative.

Die Entscheidung gilt nach dem „one-stop-shop"-Prinzip für die gesamte Europäische Union und dürfte sich erheblich auf die digitale Werbewirtschaft auswirken.

Nun auch Frankreich „ohne"

Nach der österreichischen Datenschutzbehörde (siehe SSN 01/2022) untersagte am 10.02.2022 auch die französische Datenschutzbehörde CNIL Webseiten-Betreibern die Nutzung von Google Analytics. Zur Begründung führt die CNIL aus, dass die von Google getroffenen Maßnahmen nicht ausreichten, um das fehlende Schutzniveau in den USA auszugleichen und daher Art. 44 DSGVO verletzt sei. Betreibern empfiehlt sie, Dienste zu verwenden, die nur anonyme statistische Daten produzieren, um die sonst notwendige Einwilligung zu vermeiden. Zudem kündigte sie ein Evaluierungsprogramm an, mit dem festgestellt werden soll, welche Lösungen von der Einwilligungspflicht ausgenommen sind.

Da die für Google Europa zuständige Datenschutz-Aufsichtsbehörde in Irland nicht aktiv wird, treibt derzeit die Schrems-Initiative noyb mit Beschwerden alle anderen europäischen Aufsichtsbehörden in Sachen Google Analytics vor sich her. Eine Entscheidung der deutschen Datenschutzaufsicht ist wohl nur noch eine Frage der Zeit. Daher empfehlen wir dringend einen Wechsel zu europäischen Anbietern – oder eine effektive Anonymisierung.

IT-GSK 2022 in XML

Am 08.02.2022 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das IT-Grundschutzkompendium in der Version 2022 veröffentlicht. Wie jedes Jahr finden sich im neuen Kompendium redaktionelle und inhaltliche Änderungen sowie Ergänzungen, darunter vor allem neue Bausteine zur „Containerisierung" und Fernwartung. Eine wichtige Neuerung ist, dass das BSI das Kompendium nun nicht mehr nur in traditionellen „Lese-Formaten" wie PDF bereitstellt, sondern mit der Veröffentlichung als DocBook-XML-Version Anwendern die Möglichkeit gibt, recht einfach mit eigenen Tools den operativen Umgang mit den Bausteinen zu verbessern.

Patches erscheinen früher

Am 10.02.2022 wurden in Googles Project Zero Blog einige interessante Statistiken über die Behebung von gemeldeten Schwachstellen durch Herstellerpatches veröffentlicht. Während 2018 noch durchschnittlich 90 Tage von der Meldung bis zur Behebung einer Schwachstelle verstrichen, waren es 2021 im Schnitt nur noch 52 Tage. Diese deutlich beschleunigte Bereitstellung von Patches ist sehr zu begrüßen, sie hilft jedoch nur, wenn die Patches auch zügig eingespielt werden.

Wir empfehlen: Patchen Sie so schnell wie möglich – und sehen Sie Methoden zur Zurückführung auf einen stabilen Betriebszustand sowie Ersatzmaßnahmen vor, falls es zu Störungen kommt. Verzögerungen durch ausgiebige Tests der Patches sollte man nach Möglichkeit vermeiden – das Risiko eines Angriffs ist inzwischen größer als das eines durch einen Patch verursachten Ausfalls. Schließlich drohen bei verspätetem oder unterlassenem Patchen Datenschutz-Bußgelder (vgl. SSN 11/2021).

US-Überwachungsrecht begutachtet

Die Datenschutzkonferenz (DSK) hat am 25.01.2022 ein Gutachten von Stephen I. Vladeck zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse veröffentlicht. Das Gutachten zeigt detailliert die Anwendungsbereiche der einzelnen amerikanischen Gesetze und die theoretisch möglichen Rechtsbehelfe auf, was insbesondere für Transfer Impact Assessments (TIA) bei Datenübermittlungen in die USA relevant sein dürfte. Laut DSK sind wesentliche Befunde, dass die Anwendbarkeit der bereits im Schrems-II-Urteil behandelten Section 702 FISA sehr weit ist und dass die Aspekte Extraterritorialität und Rechtsschutzmöglichkeiten behandelt werden. Diese knappen Ausführungen der DSK werden dem Detailgrad des Gutachtens ebenso wenig gerecht, wie die teilweise verbesserungsbedürftige deutsche Übersetzung.

Die Datenschutz-Aufsichtsbehörden bewerten derzeit die Konsequenzen aus dem Gutachten. Eine ist zweifellos, dass bei Übermittlungen in die USA immer an ein TIA gedacht werden muss.

CDN und Datenschutz

Ein Content Delivery Network (CDN) hostet Kopien von Webseiten, um deren Laden zu beschleunigen. Der Nutzung stehen jedoch erhebliche datenschutzrechtliche Bedenken entgegen, da ein Hosting auf global verteilten Servern unweigerlich zur Problematik der Zulässigkeit einer Drittlandsübermittlung nach Art. 44 ff. DSGVO führt, wenn über das CDN personenbezogene Daten wie IP-Adressen übermittelt werden.

Insbesondere amerikanischen Anbietern fehlt in der Regel ein angemessenes Datenschutzniveau. So entschied am 01.12.2021 das VG Wiesbaden, dass ein Cookie-Dienst, der für das Abrufen eines Einwilligungsskripts auf das CDN einer US-Firma zurückgreift, wegen fehlender Einwilligung rechtswidrig sei. Eine Information in der Datenschutzerklärung genügt nicht.

Pfeift, gepfiffen, verpfiffen

Bis 17.12.2021 hätte die EU-Richtlinie 2019/1937, besser bekannt als „Whistleblower-Richtlinie“, in deutsches Recht umgesetzt werden müssen. Dies ist bisher nicht erfolgt, und wann die neue Bundesregierung die Umsetzung angeht, ist nicht bekannt.

Die Regelungen betreffen Meldungen von Verstößen gegen ausgewählte Bestimmungen des EU-Rechts; sie richten sich sowohl an Unternehmen als auch an den öffentlichen Sektor. Bemerkenswert ist, dass eine von einem Hinweis betroffene Person im Vergleich zum

Hinweisgeber eher dürftig geschützt wird. Zwar legt Art. 22 fest, dass deren Identität während der Untersuchung geschützt und selbstverständliche Rechte wie der Anspruch auf wirksame Rechtsbehelfe und ein faires Gerichtsverfahren gewährt werden sollen. Allerdings trägt die betroffene Person die Beweislast dafür, dass erteilte Hinweise falsch sind. Der Hinweisgeber soll bei Falschinformationen nur dann sanktioniert werden, wenn er von der Unrichtigkeit wusste. Immerhin weist Art. 16 Abs. 2 darauf hin, dass der Hinweisgeber gegenüber der betroffenen Person offengelegt werden muss, damit diese von ihren Verteidigungsrechten Gebrauch machen kann.

Secorvo News

Verstärkung im Datenschutz

Wir freuen uns über eine erneute Verstärkung unseres Datenschutz-Teams: Im Februar konnten wir den Volljuristen Christian Blaicher für das Secorvo-Team gewinnen. Herzlich willkommen!

Secorvo Seminare

Ab März finden unsere Präsenz-Seminare nach mehrmonatiger Pause endlich wieder statt. Freie Plätze gibt es noch auf unserem viertägigen PKI-Seminar (**25.–28.04.2022**). Wir freuen uns auf Ihre Teilnahme!

Lesen bildet II

Wir laden Sie herzlich zu unserem zweiten „Literarischen KA-IT-Si-Kabinett“ am **10.03.2022** ein. An diesem Abend werden wir Ihnen weitere Werke der (Welt-)Literatur vorstellen, die sich mit dem Thema Datenschutz oder Datensicherheit beschäftigen und die Sicherheits- und Datenschutzexperten daher gelesen haben „müssen“. Dabei freuen wir uns nicht nur auf Ihre Anmeldung, sondern auch über Ihre persönliche Rückmeldung: Welche weiteren Bücher gehören Ihrer Ansicht nach unbedingt auf diese „Liste“?

Expertengespräch verpasst?

Sie haben die Jahresauftaktveranstaltung „Willkommen bei den Quanten“ der KA-IT-Si am 03.02.2022 verpasst oder möchten sich das Expertengespräch zur Bedrohung heutiger Kryptosysteme durch Quantencomputer noch einmal ansehen? Wir haben die Veranstaltung aufgezeichnet und auf unserem YouTube-Kanal veröffentlicht. Im Gespräch diskutieren Professor Dr. Müller-Quade (KASTEL), Oliver Winzenried (WIBU-SYSTEMS) und Dirk Fox (Secorvo Security Consulting) darüber, wie ernst die Bedrohung durch Quantencomputer genommen werden muss und was das für Hersteller und Anwender kryptografischer Systeme bedeutet.

Geld oder Leben

Wie erpressbar sind deutsche Unternehmen und Institutionen? Wer bei einem gezielten Hacker-Angriff seine gesamten Daten verliert und auf einen Schlag ohne IT-Dienste dasteht, wird geneigt sein, nahezu jeden Preis für die Wiederherstellung seiner Infrastruktur zu zahlen. Ein Unternehmen, das genau das nicht

getan hat, ist das in Baden-Württemberg ansässige Familienunternehmen Pilz. Die Unternehmensleitung hat sich 2019 trotz eines Totalausfalls der gesamten IT dagegen entschieden, den Kriminellen Lösegeld zu zahlen – und ist durch eine harte Zeit gegangen.

Was Pilz aus diesem einschneidenden Erlebnis gelernt hat und anderen Unternehmen und Unternehmern mitgeben möchte, wird Herr Thomas Pilz, geschäftsführender Gesellschafter der Pilz GmbH & Co. KG, auf dem KA-IT-Si-Event am **07.04.2022** vorstellen. Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2022	
07.-11.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.03.	KA-IT-Si-Event „Lesen bildet II" (KA-IT-Si, virtuell)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, virtuell)
24.-26.03.	ShmooCon 2022 (The Schmoo Group, Washington/US)
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)
Mai 2022	
03.-04.05.	Security Forum 2022 (Hagenberger Kreis, Hagenberg/AT)
05.05.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
09.-13.05.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Nicolas Blum, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

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