secorvo
security consulting

Secorvo Security News

Juli 2022

Moderne Abhängigkeiten

Lange schon sind die Produktlebenszyklen bei IT-Produkten – verglichen mit anderen Branchen – recht kurz. Das gilt besonders für Software. Solange die Produkte in Organisationen oder bei Privatpersonen betrieben wurden, erwuchs daraus selten ein Problem: Man nutzte ein Programm so lange, bis ein nicht behebbarer Fehler oder fehlende Features eine Migration erzwangen.

Inzwischen sind immer mehr Organisationen und Menschen von IT-Diensten abhängig, die sie nicht mehr selbst kontrollieren, wie bspw. Cloud-Dienste, Steuersysteme in Fahrzeugen oder auch Lösungen, die bedeutsam für die Gesundheit von Menschen sind.

Die Abgabe von Kontrolle und der Einsatz von fremdbetreuten Diensten sind verlockend, weil sie einige unmittelbare Vorteile bieten: Zeitersparnis und die Kompensation von fehlendem Know-How. Und häufig betreiben Anbieter die Lösungen zudem effizienter und professioneller als ihre Kunden das selbst könnten.

Manchmal geht aber auch etwas schief. So gibt es zahlreiche Beispiele für Störungen – u. a. bei Amazon, Microsoft, Google, Facebook und Atlassian. Auch werden Dienste eingestellt, siehe die umfangreiche Killed by Google-Liste. Und was passiert, wenn darunter ein kritischer Dienst ist? Das ist keine hypothetische Frage: Wegen wirtschaftlicher Schwierigkeiten stellte 2020 ein Unternehmen aus dem Medizinbereich seinen Support für ein Retina-Implantat ein. Bei ca. 350 Betroffenen, die temporär wieder sehen konnten, bleibt nun im Falle eines Defekts Medizinschrott ohne Funktion im Körper.

Daher ist es ratsam, sich nicht blind in die Cloud zu stürzen, sondern nüchtern mögliche Risiken zu betrachten und sich über kompensierende Maßnahmen Gedanken zu machen. Eine Hilfestellung können dabei Anleitungen sein wie der Grundschutzbaustein Cloud-Nutzung oder der Kriterienkatalog Cloud Computing C5 des BSI.

Inhalt

Security News

Dünne Luft für Google Analytics

Die am 17.08.2020 publizierten 101 Beschwerden der noyb zu EU-US-Datentransfers wirken weiter: Nach der österreichischen dsb (SSN 1/2022) und der französischen CNIL (SSN 2/2022) hat nun auch die italienische Datenschutzbehörde GPDP entschieden, dass die Verwendung von Google Analytics gegen die DSGVO verstößt.

Eine Risikobewertung, die annimmt, dass US-Behörden wahrscheinlich nicht nach den Daten fragen, lehnt sie ab. Vielmehr müssen Unternehmen garantieren, dass das Grundrecht auf informationelle Selbstbestimmung weiterbesteht, wenn die Daten den Europäischen Wirtschaftsraum verlassen. Gekürzte IP-Adressen sind für die GPDP personenbezogene Daten; die Kürzung sei keine ausreichende Anonymisierung. Angesichts dieser Entwicklung sollten Analytics-Kunden ihr Tracking zügig auf datenschutzkonforme Alternativen umstellen.

Post-Quantum-Kryptoverfahren

Quantencomputer bedrohen die Sicherheit aller heute eingesetzten asymmetrischen Kryptoverfahren, denn mit dem von Peter Shor 1994 entwickelten Quanten-Algorithmus ist eine effiziente Faktorisierung großer Zahlen und Berechnung diskreter Logarithmen möglich. Damit wären RSA und DSA gebrochen.

Zwar benötigen solche Quantencomputer mehr als 2000 Qubits – heutige erreichen gerade einmal 127 (IBM, 2021). Aber es ist nur eine Frage der Zeit, bis es so weit ist. Um rechtzeitig gut untersuchte neue Verfahren zu etablieren, schrieb das NIST daher 2016 einen Wettbewerb für Post-Quantum-Algorithmen aus. Aus ursprünglich 69 Vorschlägen wählte das NIST am 05.07.2022 einen Kandidaten für Verschlüsselung und Key Exchange (CRYSTALS-KYBER) und drei für digitale Signaturen (CRYSTALS-Dilithium, FALCON und SPHINCS+) zur Standardisierung aus, die 2024 abgeschlossen werden soll. Vier weitere Verfahren nahm das NIST in die vierte Evaluationsrunde auf (vollständiger Bericht). Kurz darauf wurde eines davon, SIKE, am 30.07.2022 von Forschern der Universität Leuven gebrochen.

Nach 45 Jahren mit sicheren asymmetrischen Verfahren bricht nun eine Phase der Unruhe an – mit bisher noch ungewissem Ausgang.

Cloud Encryption

Der stärkste Vorbehalt gegen die Nutzung von Cloud-Diensten ist die Zugriffsmöglichkeit des Anbieters auf die verarbeiteten Daten – die in einigen Drittstaaten auch Nachrichtendiensten einen Datenzugang eröffnet. Davor schützt auch keine Datenverschlüsselung – denn während der Verarbeitung liegen die Daten und der Entschlüsselungsschlüssel offen im Arbeitsspeicher (RAM) des Servers. Abhilfe soll das am 19.07.2022 von Corey Sanders im Microsoft-Blog vorgestellte „Azure Confidential Computing“ schaffen. Dabei kommen spezielle Eigenschaften neuerer Prozessoren von AMD und Intel zum Einsatz (SME/SEV bzw. SGX): die Verschlüsselung aller vom Prozessor als Cache genutzten RAM-Bereiche. Damit liegen auch in einem Memory Dump Daten, Passwörter oder Schlüssel, die der Prozessor genutzt hat, nur verschlüsselt vor.

Sofern die Passwörter und Schlüssel für diese RAM-Verschlüsselung selbst in einem zugriffsgesicherten Bereich (Hardware Security Module, HSM) gehalten werden und die Verfahren keine Hintertür für behördlichen Zugriff haben, könnte eine solche Lösung den „zusätzlichen Garantien“ entsprechen, die der EuGH im Schrems-II-Urteil bei Verarbeitungen in datenschutzrechtlich unsicheren Drittstaaten fordert (SSN 10/2020).

Rechtswidrige Wächter-Modi

Am 19.07.2022 hat der Verbraucherzentrale Bundesverband (vzbv) bekanntgegeben, dass er Tesla wegen des (in den SSN 9+10/2021 vorgestellten) „Wächter-Modus“ im Model 3 verklagen wird. Dabei filmt das geparkte Fahrzeug mit den eingebauten Kameras die Umgebung; auf die Livebilder kann mit der Tesla Mobile App zugegriffen werden. Bei nahenden Passanten wird der Warnzustand aktiviert, in dem die Videobilder zusätzlich im Fahrzeug gespeichert werden.

Nach Ansicht des vzbv ist eine datenschutzkonforme Nutzung im öffentlichen Raum nicht möglich und die Datenverarbeitung damit unzulässig. Grundsätzlich bedürfe es dafür entweder einer Einwilligung der Passanten (praktisch nicht umsetzbar) oder eines überwiegenden Interesses des Fahrzeughalters oder -fahrers (bei anlassloser Überwachung nicht begründbar).

Auch bei dem anderen in den SSN 9+10/2021 vorgestellten „Wächter-Modus“ regt sich Widerstand: Am 13.07.2022 erklärte US-Senator Ed Markey nach einer Befragung von Amazon Ring das von über 2.100 US-Strafverfolgungsbehörden genutzte Angebot, direkten Zugriff auf die Geräte von Ring-Nutzern zu erhalten, für rechtswidrig. Zudem habe Amazon 2022 in elf Fällen Bildmaterial ohne Einwilligung der betroffenen Ring-Nutzer weitergegeben.

Nutzer solcher Wächter-Lösungen sollten sich nicht darauf verlassen, dass der Hersteller für die Einhal-

tung der datenschutzrechtlichen Anforderungen sorgt. Bußgeldbewehrt ist der rechtswidrige Betrieb – und verantwortlich der Betreiber. Das gilt nach der DSGVO auch für Privatpersonen.

Ampeln zur Klassifizierung

Die Forderung nach Informationsklassifizierung und angemessener Kennzeichnung sind seit jeher Bestandteil der Anforderungen der ISO 27002, wie schon des Vorgängers BS 7799-2. Bei der Umsetzung kann der Standard „Traffic Light Protocol (TLP)“ helfen, dessen Version 2.0 das Forum of Incident Response and Security Teams (FIRST) am 05.08.2022 veröffentlichte. Darin hat sich die CERT-Community auf eine einheitliche Nomenklatur für Vertraulichkeitsklassen geeinigt. Die Verwendung einheitlicher Bezeichnungen kann für die Kommunikation zwischen Organisationen hilfreich sein – z. B. indem Organisationen die FIRST-TLP adaptieren, ähnlich wie das BSI am 12.05.2022.

Big Brother Deutsche Bahn

Am 11.04.2022 veröffentlichten der Blogger Mike Kuketz und Peter Hense das vernichtende Ergebnis ihrer datenschutzrechtlichen Untersuchung der DB Navigator-App. So hält die Bahn 10 Dienstleister, darunter Adobe Analytics und Optimizely, für erforderliche Adressaten sämtlicher Daten, die im Rahmen einer Ticketbuchung erfasst werden.

Eine rechtliche Grundlage gebe es dafür nicht, denn um diese Verarbeitung zu vermeiden müssten Reisende ihr Ticket entweder am Automaten oder im Reisezentrum erwerben. Für den kurzfristigen Ticketkauf gebe es keine Alternative zur App, da Schaffner keine Tickets mehr im Zug verkaufen. Am 20.07.2022 teilte Kuketz mit, dass er jetzt gemeinsam mit digitalcourage die Bahn verklage, da die DB Navigator App erfasste Daten auch dann noch sendet, wenn in den Einstellungen „Nur erforderliche Cookies verwenden“ ausgewählt wurde. Die Klage kann man auf der Seite von digitalcourage unterstützen.

Leaky Forms

Auf dem diesjährigen 31. Usenix Security Forum (10.-12.08.2022) stellten vier Forscher aus Leuven, Nijmegen und Lausanne die Ergebnisse ihrer Mitte 2021 durchgeführten umfangreichen Studie zum rechtswidrigen Tracking von Daten in Web-Formularen vor. Dazu hatten sie mit eigens entwickelten Crawlern auf den 100.000 meistbesuchten europäischen und amerikanischen Webseiten je rund 50.000 Formularseiten identifiziert, auf denen E-Mail-Adressen abgefragt wurde. Trugen die Crawler dort eine Adresse ein, so wurde sie von 1.850 europäischen (3,7%) und 2.950 amerikanischen (5,9%) Servern ohne Einwilligung des Nutzers – d. h. vor der Betätigung des „Senden“-Knopfes – an den Tracker übertragen. Eine solche Übermittlung ist rechtswidrig – und kann obendrein Daten umfassen, deren Übermittlung gar nicht beabsichtigt war, wenn beispielsweise der „Autofill“-Mechanismus des Browsers verwendet wird. Ihre Datenbasis und die verwendete Software zur Identifikation der rechtswidrigen Tracker haben die Autoren auf Github veröffentlicht.

Secorvo News

Wenn nicht jetzt – wann dann?

1.700 Experten haben es schon – das T.I.S.P.-Zertifikat. Regelmäßig treffen sie sich zum Erfahrungsaustausch auf dem T.I.S.P.-Community-Meeting.

Falls Sie noch nicht dazu gehören: Vom **19.09. bis 23.09.2022** bieten wir Ihnen mit unserem T.I.S.P.-Seminar die nächste Gelegenheit, sich auf die Prüfung vorzubereiten. Mit Ihrer Anmeldung zum Seminar erhalten Sie vorab unser T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“. Wir freuen uns auf Sie!

Alle weiteren Seminarthemen und Termine unter https://www.secorvo.de/seminare.

Hokus Pokus Fidibus

Wie geht das – Entwicklung und Produktion von Hardware-Security-Modulen in Deutschland? Welche Herausforderungen sind damit verbunden – und wie werden die von einem der wenigen deutschen Hersteller von IT-Security Hardware gemeistert, der WIBU-SYSTEMS aus Karlsruhe? Das grenzt manchmal schon an Zauberei …

Erfahren Sie bei unserem kommenden KA-IT-Si-Event am **15.09.2022** aus erster Hand, welche Hürden bei der Entwicklung, den Multiplattform-Tests, der Beschaffung und der sicheren Produktion von Security Controllern „Made-in-Germany“ zu bewältigen sind. Wir erhalten die seltene Gelegenheit, die Fertigung zu besichtigen und Einblick in die automatisierten Prozesse des Downloads finaler Firmware, der Schlüsselerzeugung und optional individueller Schlüsselspeicherung für kundenspezifische Produkte zu bekommen. Die Spezialisten von WIBU-SYSTEMS und der Vorstand Oliver Winzenried stehen Ihnen dabei Rede und Antwort.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ – diesmal mit einem phänomenalen Blick auf den Schwarzwald (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)
27.-29.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
November 2022	
07.-11.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
07.-11.11.	ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US)
09.-10.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)

Fundsache

TeleTrusT hat am 22.06.2022 einen Podcast zum "Stand der Technik in der IT-Sicherheit" veröffentlicht. Darin stellen Tomasz Lawicki (Leiter AK Stand der Technik) und Karsten U. Bartels (TeleTrusT Vorstand) die Methode zur Entwicklung der Handreichung "Stand der Technik", rechtliche Positionen und weitere Aspekte vor. Hörenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian (Editorial), 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