Secorvo Security News

September/Oktober 2021

Aufgelöste Verantwortung

Schneller als gedacht sind Cloud-Dienste zum neuen Standard geworden. Doch unsere Vorstellung, dass es dabei im Wesentlichen auf die Wahl eines vertrauenswürdigen Anbieters ankäme, ist zu kurz gesprungen.

Denn tatsächlich bestehen viele Cloud-Lösungen selbst wieder aus zahlreichen Einzeldiensten, die über die Cloud eingebunden werden: Ticketsystem, E-Mail-Services, Zahlungssystem, Benutzersupport, Shopsystem, Chat, Telefonie, Adressdatenbank, Tracking, Videostreaming ... – warum sollte ein Anbieter das auch neu implementieren, wenn er es günstig hinzukaufen kann?

Das Ergebnis ist – zumindest aus der Perspektive eines Datenschützers – fatal. Die Auftragsverarbeitungsverträge der Lösungsanbieter lesen sich wie das Who-is-who einschlägiger Cloud-Dienstleister: seitenlange Tabellen mit Unterauftragnehmern. Und schaut man sich deren AV-Verträge an, finden sich dort weitere Listen. Viele Unterauftragnehmer haben ihren Sitz im nichteuropäischen Ausland; wenn nicht, dann nutzen sie selbst nichteuropäische Dienstleister. Dass alle Verträge in dieser Kette korrekt geschlossen und die dokumentierten Schutzmaßnahmen sowie die Listen der Unterauftragnehmer der Wirklichkeit entsprechen, ist wenig wahrscheinlich – und praktisch nicht mit vertretbarem Aufwand überprüfbar.

Die Idee der Auftragsverarbeitung wird damit ad absurdum geführt. Denn im zerstückelten „Klein-Klein" atomarer Cloud-Dienste bleibt die Verantwortung auf der Strecke. Wie sollte der Anbieter, dessen Sub-Sub-Sub-Auftragsverarbeiter seine Tickets in den USA verarbeiten lässt, den datenschutzkonformen Umgang sicherstellen?

Das erinnert ein wenig an die Finanzkrise 2008. Damals wurden die Ausfallrisiken von Immobilienkrediten durch Zerstückelung und Verteilung auf Investitionspapiere marginalisiert. Bis sie sich durch das Platzen der Immobilienblase plötzlich wirkungsvoll manifestierten.

Security News

Augen überall

Am 24.08.2021 berichtete das ZDF Magazin „frontal", dass die von Tesla-Fahrzeugen regelmäßig in die Cloud des Herstellers hochgeladenen Daten auch die Bilddaten der am Auto verbauten acht hochauflösenden Kameras umfassen. Ob dafür der Hersteller (weil das Auto ohne die Übermittlung nicht vollumfänglich funktioniert) oder der Halter (da er der Übermittlung zugestimmt hat) die datenschutzrechtliche Verantwortung trägt, ist ungeklärt. Nach Auffassung der

Aufsichtsbehörden sind Aufzeichnungen mit Dashcams nur in sehr engen Grenzen zulässig. Die niedersächsische Aufsichtsbehörde hält eine Speicherung nur bis maximal 30 Sekunden für rechtmäßig. Ähnliches gilt für die Video Doorbell von Ring, einer Amazon-Tochter, über die der SWR am 05.10.2021 berichtete. Über die mit Mikrofon ausgestattete Kamera können Hausbesitzer auf dem Mobilgerät verfolgen, was sich vor der heimischen Haustür so tut – und mit Besuchern Kontakt aufnehmen.

In beiden Fällen muss der Verantwortliche die Betroffenen nach Art. 12 ff. DSGVO über Art und Zweck der Verarbeitung informieren; dabei darf keine Erfassung des öffentlichen Raums erfolgen.

Die ggf. heimliche Tonübertragung der Video Doorbell kann zudem eine strafrechtlich relevante Verletzung der Vertraulichkeit des Wortes (§ 201 StGB) darstellen. Auch sind die Geräte vor einiger Zeit durch Schwachstellen aufgefallen.

Bis zu einer datenschutzkonformen Lösung muss man wohl empfehlen, um Teslas und Video Doorbells einen großen Bogen zu machen.

ISO-Leitlinie Löschkonzept

Als praxisbewährte Hilfestellung für die Entwicklung von Löschkonzepten wurde bis 2016 unter der Federführung von Secorvo und mit Unterstützung der Unternehmen Blancco, DATEV, Deutsche Bahn und Toll Collect die „Leitlinie Löschkonzept" entwickelt und schließlich als DIN 66398 verabschiedet (SSN 4/2016). 2018 startete die DIN das Projekt ISO/IEC 27555 zur Überführung der Leitlinie in einen internationalen Standard (SSN 7/2018). Jetzt ist es so weit: Am 08.10.2021 wurde die ISO/IEC 27555:2021 (Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion) publiziert. Die Vorgehensweise entspricht der DIN 66398; im Detail gibt es einige wenige Unterschiede. Der Text wurde redaktionell überarbeitet und deutlich gekürzt. Die DIN 66398 wurde im Juni 2021 vom zuständigen Arbeitskreis bestätigt und wird zunächst beibehalten.

Bad Practice 1FA

Wie u. a. im SANS-Newsletter vom 30.08.2021 gemeldet, hat die amerikanische Cybersecurity & Infrastructure Security Agency (CISA) die Single-Factor-Authentifizierung auf die Liste der Bad Practices gesetzt. Aus unserer Sicht eine sinnvolle Ergänzung, nicht nur Best Practices sondern auch verbreitete „No Gos" als Bad Practice zu „brandmarken".

In internen Netzen und geschlossenen Umgebungen kann ein Kennwort als einziger Faktor ggf. noch angemessen sein. Bei über das Internet genutzten (Cloud-) Diensten ist das aufgrund der zahlreichen mit Kennworten verbundenen Gefährdungen wie Brute-Force-Angriffen, Phishing oder der Wiederverwendung von Kennworten nicht zu empfehlen.

One Time Token und Zertifikate haben sich in der Praxis bewährt. Wer darauf verzichtet, sollte sich darüber im Klaren sein, dass er bei einer Kompromittierung zu Recht eine Tasse mit Aufschrift „Das kannste schon so

machen, aber dann isses halt …“ auf den Tisch gestellt bekommt. Auch die weiteren Anti-Empfehlungen der CISA Bad Practices lohnen einen genaueren Blick.

Willkommen 2FA

Viele Dienste bieten zur Verbesserung der Sicherheit zusätzlich eine Zwei-Faktor-Authentifizierung an. Ursprünglich waren dies TAN-Listen auf Papier. Mittlerweile werden die zusätzlichen Geheimnisse in Hardware-Token oder in Smartphone-Apps gespeichert wie die Authenticator-Apps von Google und Microsoft.

Privatanwendern wird nun für das Microsoft-Konto eine kennwortlose App-Authentifikation angeboten, die sie in den Sicherheitseinstellungen aktivieren können. Unternehmen und Bildungseinrichtungen steht diese Funktion bereits länger zur Verfügung. Statt der App kann z. B. auch ein FIDO2-Key verwendet werden. Angriffe auf gut zu merkende, aber zu einfache Passwörter sollen so der Vergangenheit angehören.

Prinzipiell kann das Verfahren als 2FA angesehen werden: Der Zugang erfordert den physischen Besitz des Smartphones, und beim iPhone ist die Authentikator-App zusätzlich durch einen Fingerabdruck gesichert. Damit das Entsperren des Smartphones dauerhaft nur dem Besitzer möglich ist, sind regelmäßige Sicherheitsupdates und eine komplexe PIN (oder gute Biometrie) essentiell. Damit zukünftig nicht jeder Dienst eine eigene Authentikator-App benötigt, bleibt zu hoffen, dass sich Standards wie FIDO2 durchsetzen.

Faxen unter der DSGVO

Nach der Bayrischen, der Niedersächsischen und der Bremischen Aufsichtsbehörde hat am 14.09.2021 auch der Hessische Datenschutzbeauftragte den Faxversand als unsicheres Übermittlungsverfahren eingestuft. Zwar verneint er die Zulässigkeit einer Fax-Übertragung personenbezogener oder auch besonders schutzbedürftiger Daten nicht generell, begrenzt sie jedoch auf dringliche Ausnahmefälle.

Der Vergleich der Aufsichtsbehörde mit dem E-Mail-Versand hinkt jedoch. Denn nach wie vor gilt (SSN 03/2021): Ein Fax ist genauso sicher wie ein Telefonat – beide nutzen heute TCP/IP-basierte Paketvermittlung. Und beide Übertragungen unterliegen dem Telekommunikationsgeheimnis, das die TK-Provider durch geeignete Schutzmaßnahmen sicherstellen müssen.

Die Technik der Faxübermittlung ist nicht unsicherer geworden. Die besonderen Gefahren beim Faxversand schützenswerter Daten liegen schon immer auf der „Benutzerebene“, wie Zahlendreher bei der Fax-Nummer, Nutzung der Wahlwiederholungstaste oder ein Empfangsgerät, das Unberechtigten zugänglich ist. Daher ist die Empfehlung der Aufsichtsbehörde zutreffend, nach Möglichkeit alternative Übertragungstechniken zu wählen.

Transnationale Verhaltensregeln

Noch immer herrscht große Unsicherheit, wie die Anforderungen aus dem EuGH-Urteil Schrems II an internationale Datentransfers zu erfüllen sind. Ein Weg ist die Auswahl von Dienstleistern, die sich zur Einhaltung

von der EU anerkannter transnationaler Verhaltensregeln verpflichten. Am 20.05.2021 wurden die Beschlussvorlagen zum EU Cloud Code of Conduct und zum Code of Conduct for Cloud Infrastructure Service Providers in der Version 2.11 als erster Transnational Code of Conduct vom Europäischen Datenschutzausschuss angenommen und damit deren DSGVO-Konformität bestätigt.

Datentransfer-Folgenabschätzung

Die am 04.06.2021 von der EU-Kommission verabschiedeten neuen Standardvertragsklauseln verlangen, dass im Hinblick auf internationale Datentransfers in Drittstaaten ohne anerkanntes angemessenes Datenschutzniveau sog. Transfer Impact Assessments (TIA) durchgeführt werden (Klauseln 14 a) - d)). Dabei ist eine mehrstufige Prüfung durchzuführen, die den besonderen Umständen der Datenübermittlung, also z. B. der Länge der Verarbeitungskette, den beabsichtigten Übertragungskanäle, den Kategorien und dem Format der über mittelten personenbezogenen Daten Rechnung tragen soll. Die relevanten Rechtsvorschriften des Bestimmungslandes müssen geprüft, die erforderlichen technischen und organisatorischen Schutzmaßnahmen (TOMs) müssen festgelegt werden.

Um hier eine Hilfestellung zu geben, hat die non-profit-Organisation iapp am 01.09.2021 ein Muster zur Durchführung eines solchen TIAs bereitgestellt, das für Übermittlungen in die USA hilfreich ist.

Secorvo News

Secorvo Seminare

Auf unserem letzten Seminar in diesem Jahr gibt es noch wenige freie Plätze: IT Security Insights, unser T.I.S.P.-Update (**30.11.–02.12.2021**). Natürlich freuen wir uns auch über Anmeldungen für unsere im kommenden Jahr geplanten Seminare. Eine Übersicht aller Termine und Seminarangebote finden Sie unter www.secorvo.de/seminare.

Schwarzer Gürtel

Unser Penetrationstester Enes Erdoğan hat jetzt ebenfalls den „schwarzen Gürtel" – seine OSCP-Zertifizierung. Herzlichen Glückwunsch!

Pilze und Sicherheitsstandards...

In den vergangenen Jahren ist die Zahl der Standards, Checklisten und Best Practices zur Informationssicherheit ständig gewachsen. Auf dem kommenden KA-IT-Si-Event am **18.11.2021** zeigt Ihnen Milan Burgdorf interessante Gebiete auf der Landkarte der Informationssicherheitsstandards und -frameworks. Dabei werden bekannte (ISO 2700x und IT-Grundschutz) und unbekannte Gegenden erkundet, damit Sie sich auf diesem unübersichtlichen Territorium besser zurecht finden. Wir freuen uns auf einen interessanten Abend mit Ihnen – diesmal wieder als Online-Event (zur Anmeldung).

Krypto im Advent

Mit unserem interaktiven Online-Adventskalender „Krypto im Advent“ lernen Schülerinnen und Schüler (3.-9. Klasse) seit 2015 auf spielerische Weise Verschlüsselungstechniken kennen und können dabei attraktive Sachpreise gewinnen. Zusammen mit der PH Karlsruhe haben wir uns auch diesmal wieder spannende Kryptografie-Rätsel ausgedacht. Schulklassen und Profis können ebenfalls „miträtseln“, letztere allerdings außer Konkurrenz. Anmeldungen sind ab dem 01.11.2021 auf Krypto-im-Advent.de möglich (Teilnahme kostenlos).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2021	
14.-19.11.	ACM CCS 2021 (ACM/SIGSAC, Seoul/KOR)
17.-19.11.	45. DAFTA (GDD, virtuell)
18.-19.11.	DeepSec 2021 (DeepSec, Wien/AT)
30.11.-02.12.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Januar 2022	
24.-26.01.	Omnisecure 2022 (in TIME berlin, Berlin)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

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