secorvo
security consulting

Secorvo Security News

Januar 2021

Gretchenfrage

Die nicht unerwartete Außerkraftsetzung des Privacy Shields durch den EuGH hat eine Welle von Vertragsneugestaltungen und viel Unsicherheit ausgelöst. Darf man personenbezogene Daten noch von US-Unternehmen verarbeiten lassen? Und wenn ja: wie?

Dabei gerät zunehmend die entscheidende Frage aus dem Blick. Denn worum geht es im Kern? Wir möchten einem fremden Dritten Daten anvertrauen, für die wir verantwortlich sind – und es, Vertrag hin oder her, auch bleiben. Die von der DSGVO geforderten vertraglichen Vereinbarungen und technisch-organisatorischen Zusicherungen, die wir mit dem Verarbeiter abschließen, sind dabei nur ein Instrument, um die Vertrauenswürdigkeit des Dritten zu untermauern. Sie sollten selbstverständlich sein.

Denn jedes Vertrauen braucht Fundierung: langjährige Zusammenarbeit, eigene Inspektion (Audits), Prüfung durch anerkannte Institutionen (Zertifikate), klare Vereinbarungen und rechtliche Absicherungen. Und selbst dann ist ein wenig verbleibende Skepsis kein Fehler.

Doch vertrauensbildende Maßnahmen erfordern die tiefere Beschäftigung mit Dienst und Dienstleister – keine gute Überlebensbedingung in einer schnelllebigen Zeit. Daher mutiert unser immer blinderes Vertrauen in die IT (in Programme, in Dienste und in Dienstleister) zu Vertrauensseligkeit. Ein perfekter „Nährboden“ für Täuschung und Betrug, siehe Enron, FlowTex oder Wirecard.

Während nicht nur unsere Abhängigkeit von der IT sondern auch die von kaum noch austauschbaren Diensten wächst, schrumpft zugleich das Fundament, auf dem Zusammenarbeit immer gründen sollte: solides Vertrauen. Wer seine Risiken beherrschen will, sollte sich daher häufiger die Frage stellen: Vertraue ich diesem Dienst, dieser Software wirklich? Und wenn die Antwort kein klares „Ja“ ist, sollte man sich besser damit beschäftigen. Oder zumindest nicht verwundert die Augen aufreißen, wenn der Blindflug schief geht.

Inhalt

secorvo
security consulting

Security News

Datenschutz im Homeoffice

Am 27.01.2021 trat die SARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV) des Bundesministeriums für Arbeit und Soziales in Kraft, befristet bis zum 15.03.2021. Nach § 2 Abs. 4 „hat der Arbeitgeber den Beschäftigten im Fall der Büroarbeit oder vergleichbaren Tätigkeiten anzubieten, diese Tätigkeiten in deren Wohnung auszuführen, wenn keine zwingenden betriebsbedingten Gründe entgegenstehen“. Homeoffice kann Telearbeit oder mobiles Arbeiten sein – in jedem Fall trägt der Arbeitgeber die datenschutzrechtliche Verantwortung. Dabei sind besondere Schutzmaßnahmen angezeigt. Die Checkliste des Bayerischen Landesamts für Datenschutzaufsicht kann dabei eine Hilfestellung sein.

Aus rechtlicher Perspektive ist die Norm problematisch, weil die Begrifflichkeiten des § 2 Abs. 4 teilweise unbestimmt sind. Was ist unter „zwingenden betriebsbedingten Gründen“ zu verstehen? Genügt es bereits, wenn im Homeoffice dem Datenschutz nicht hinreichend Rechnung getragen werden kann? Dann könnten sich fast alle Arbeitgeber auf den Ausnahmetatbestand berufen, denn eine gleichwertig sichere Infrastruktur ist zuhause selten gegeben.

DNSpooq

Ende Januar 2021 veröffentlichten Sicherheitsforscher von JSOF unter dem Namen DNSpooq sieben Schwachstellen für den DNS-Server dnsmasq, der in eingebetteten Systemen wie Routern und IoT-Geräten weit verbreitet ist. Meist übernimmt er darin die Rolle des DNS-Forwarders und leitet Namensanfragen zur Auflösung an DNS-Server weiter; die Antworten hält er in einem Cache vor. in einem Whitepaper erläutern die Forscher, wie die gefundenen Schwachstellen kombiniert werden können, um gefälschte Einträge in diesen Cache einzuschleusen. Damit tritt dieser Cache-Poisoning-Angriff in die Fußstapfen des 2008 von Dan Kaminski gezeigten Angriffs auf DNS. Die Angriffe können über das Internet, aus dem lokalen Netz oder sogar vom Browser des Opfers aus erfolgen.

Dagegen schützen würde der flächendeckende Einsatz von HSTS oder DNSSEC, die jedoch noch viel zu selten eingesetzt werden. Doch auch in der DNSSEC-Implementierung von dnsmasq entdeckten die Forscher Buffer Overflows, die es einem Angreifer ermöglichen könnten, Server aus der Ferne zu übernehmen. Von den Schwachstellen sind mehr als 40 Hersteller betroffen, von denen einige bereits aktualisierte Software zur Verfügung stellen. Doch ist zu vermuten, dass viele eingebettete Geräte verwundbar bleiben, da sie keine Updates erhalten. Schlimmstenfalls muss man die Geräte ersetzen. Wer Sicherheits-Schrott kauft, kauft oft zweimal.

Post-Brexit-Datenschutz

Am 01.01.2021 begann die Übergangsfrist von vier Monaten, innerhalb derer die Übermittlung von personenbezogenen Daten in das Vereinigte Königreich Großbritannien und Nordirland noch als Übermittlung innerhalb der EU behandelt werden darf (siehe Art. FINPROV.10A Abs. 4 b) des Handels- und Kooperationsabkommens vom 30.12.2020). Sofern weder die EU noch Großbritannien widersprechen, kann die Übergangsfrist um weitere zwei Monate verlängert werden.

Anschließend wird das Vereinigte Königreich in Bezug auf die Übermittlung von personenbezogenen Daten ein Drittland sein. Dann wird es zusätzlicher Garantien (Art. 44 ff DSGVO) für die Datenübermittlung bedürfen. Diese könnten in einem das Vereinigte Königreich betreffenden Angemessenheitsbeschluss (Art. 45 DSGVO) bestehen. Auch ohne Angemessenheitsbeschluss kann die Datenübermittlung zulässig sein, wenn ein Vertrag nach den Standardvertragsklauseln geschlossen wird. Dabei kann es allerdings erforderlich sein, dass deren effektive Einhaltung durch weitere Maßnahmen sichergestellt wird.

Unerwünschte Anrufe

Am 04.01.2021 teilte die Bundesnetzagentur mit, dass sie gegen den Betreiber eines Call-Centers ein Bußgeld in Höhe von 145.000 Euro verhängt hat. Dessen Anrufe dienten u. a. der Neukundenakquise für einen Pay-TV Anbieter. Weder Call-Center noch Auftraggeber hatten vor dem Kauf der Adressdaten geprüft, ob die angeblich erteilten Werbeeinwilligungen auch tatsächlich vorlagen. Dies ist aber im B2C-Bereich unerlässliche Voraussetzung für datenschutz- und wettbewerbsrechtlich zulässige Werbeanrufe. Auch im B2B-Bereich werden die Grenzen der mutmaßlichen Einwilligung von den Gerichten sehr eng gesteckt. Adresskauf und Auftrag entbinden den Werbetreibenden nicht von der Pflicht, die Einwilligungen nachzuweisen.

Vor einer anderen Art unerwünschter Anrufe, auch als Vishing (Voice Phishing) bezeichnet, warnte das FBI am 14.01.2021 in einer PIN (Private Industry Notification)-Warnung: Durch Anrufe über VoIP-Systeme wird versucht, ähnlich wie mit Links in Phishing-Mails, Angestellte dazu zu verleiten, Webseiten zu besuchen, auf denen Zugangsdaten abgefischt werden. Ähnliche Angriffe gibt es seit Jahren im privaten Bereich (z. B. von angeblichen Mitarbei-

tern des Microsoft-Support) – eine offenbar nach wie vor erfolgreiche Masche.

BSI-Standard zu BCM 2.0

13 Jahre nach der Veröffentlichung des IT-Grundschutz-Standards 100-4: Notfallmanagement hat das BSI am 19.01.2021 dessen grundlegende Überarbeitung als Community Draft BSI 200-4 Business Continuity Management (BCM) publiziert. Der Standard gibt auf 298 Seiten neben einer theoretischen Einordnung der verschiedenen BCM-Aspekte praktische Hilfestellung für den schrittweisen Aufbau eines BCM. Beispielsweise ist eine Abgrenzung zwischen BCM und IT-Service-Continuity-Management (ITSCM) hilfreich, um falsche Erwartungen zu vermeiden.

Ähnlich wie beim modernisierten IT-Grundschutz im Standard 200-2 werden verschiedene Ausbaustufen eines BCM vorgestellt und deren Vorteile und Grenzen beschrieben. Diese Ausbaustufen erlauben einen Einstieg mit überschaubaren Aufwänden. Vor dem Hintergrund verschärfter Anforderungen an die Notfallvorsorge ist diese aktualisierte Handreichung sehr zu begrüßen. Fazit: Lesenswert.

BND im Visier

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat am 11.01.2021 eine Beschwerde der Organisation „Reporter ohne Grenzen“ und des Rechtsprofessors Niko Härting aus dem Jahr 2017 gegen die Überwachungspraktiken des Bundesnachrichtendienstes (BND) angenommen. Die Beschwerde betrifft die Befugnisse nach dem G10-Gesetz und die Frage, ob gegen die Überwachung von E-Mail, Post und Telekommunikation effektive Rechtsmittel zur Verfügung stehen.

Nun muss die Bundesregierung Stellung nehmen, inwieweit tatsächlich Nachrichten der Beschwerdeführer abgefangen wurden und ob ihnen ein effektives Rechtsmittel zur Verfügung gestanden hat, denn die vorbefassten Gerichte hatten einen direkten Nachweis der Beobachtung von den Beschwerdeführern verlangt.

Das anstehende Verfahren entbehrt nicht einer gewissen Ironie, da der EuGH in seinem Schrems-II Urteil wegen genau solcher Einblicksbefugnisse ohne adäquaten Rechtsschutz ein angemessenes Datenschutzniveau in den USA verneint und mit den geäußerten Zweifeln an dessen Herstellbarkeit mittels Standardvertragsklauseln große Rechtsunsicherheit geschaffen hat.

CrypTool in Java

Das erfolgreiche CrypTool-Projekt, das Professor Esslinger aus Siegen seit mehr als 20 Jahren mit einem Team ehrenamtlicher Mitwirkender vorantreibt, hat Ende November 2020 die Java-Version des Kryptologie-Lernprogramms publiziert. Sie ergänzt das Windows-CrypTool 2 um eine vom Betriebssystem unabhängige Version. Mit Release 2020.1 war es im März 2020 um zahlreiche Funktionen (wie zum Beispiel einem visualisierten Tutorial zur Differentiellen Kryptoanalyse) erweitert worden.

Secorvo News

Secorvo-Seminare

Trotz der erfreulicherweise sinkenden Infektionszahlen ist derzeit schwer vorhersehbar, wann wir unsere Präsenz-Seminare wieder durchführen können – noch sind Hotels und Gastronomie geschlossen. Dennoch planen wir.

Sofern auch Sie planen möchten, können Sie Ihre Seminarteilnahme gerne buchen – selbstverständlich stornieren wir Ihre Buchung kostenfrei, wenn Ihnen die Teilnahme oder uns die Durchführung des Seminars aufgrund der Pandemie-Maßnahmen nicht möglich sein sollte.

Im September 2020 konnten wir unsere Infektionsschutzmaßnahmen noch auf mehreren Seminaren erfolgreich umsetzen: Durch eine Begrenzung der maximalen Teilnehmerzahl, interne „Wegführungen“, Lüftungspausen und Desinfektionsmaßnahmen sorgen wir während der Seminare für einen wirksamen Infektionsschutz.

Krypto-at-Home

Über 4.700 Schülerinnen und Schüler sowie ältere Kryptografie-Fans tauchten im Advent 2020 in die Welt der Verschlüsselung ein: Ein erneuter Teilnahmerekord bei unserem Online-Adventskalender "Krypto im Advent".

Als Beitrag der KA-IT-Si zum Home-Schooling haben wir nun die 36 Rätsel (und Lösungen) zusammengefasst und zum Download und Nachrätseln unter www.krypto-im-advent.de bereitgestellt. Perfektes Lernmaterial – nicht nur für den Informatik-Unterricht in den siebten Klassen. Verraten Sie es gerne weiter!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
22.-26.02.	T.I.S.P. (TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, virtuell)
März 2021	
15.-18.03.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
23.-25.03.	IT Security Insights – T.I.S.P. Update (Secorvo, Karlsruhe)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
20.-21.04.	Datenschutztage 2021 (FFD Forum für Datenschutz, Mainz)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
27.-30.04.	BvD Verbandstag 2021 (BvD, Berlin)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Milena Jutz, Michael Knopp, Sarah Niederer, 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