Secorvo Security News

April 2021

Lesen bildet.

Häufig sind es Schriftsteller, die technische und gesellschaftliche Entwicklungen lange zuvor erahnen und beschreiben; manchmal prägen sie damit den gesellschaftlichen Diskurs der Technikfolgen. Kein Wunder, werden doch die theoretischen Möglichkeiten oft erst durch eine realistische Erzählung konkret vorstellbar. Gelingt es einem Autor dabei, in seiner Geschichte – meist einer Dystopie – die zentralen Fragen aufzuwerfen, kann eine solche Erzählung mehr Grundverständnis vermitteln als hundert Vorträge.

Das gilt vielleicht ganz besonders für den Datenschutz und die Informationssicherheit, leiden beide doch unter demselben Dilemma: Je erfolgreicher der Schutz, desto abstrakter und unkonkreter die Gefahr. Aus einer Diskussion mit Datenschutz- und Datensicherheitsexperten in Süddeutschland entstand daher kürzlich die folgende, zweifellos nicht vollständige Liste von zehn belletristischen Werken, die die Bedeutung von Datenschutz und Datensicherheit in besonders beeindruckender Weise konkret werden lassen:

1. George Orwell: 1984 (1948)
2. Clifford Stoll: Das Kuckucksei / Cuckoo's Egg (1989)
3. Robert Harris: Enigma (1995)
4. John Katzenbach: Der Patient (2006)
5. Jeffery Deaver: Der Täuscher (2009)
6. Marc Elsberg: Blackout (2012)
7. Dave Eggers: Der Circle (2013)
8. Marc Elsberg: ZERO (2014)
9. Marc-Uwe Kling: Quality Land (2017)
10. Andreas Eschbach: NSA (2018)

Einige werden Ihnen zweifellos bekannt sein. Die Lektüre der anderen legen wir Ihnen wärmstens ans Herz. Und wenn Sie das nächste Mal gefragt werden, warum Datenschutz oder Datensicherheit bloß so wichtig genommen werden: Empfehlen Sie einfach – ein Buch.

Security News

Urheberzensur

Am 11.03.2021 hat die „Clearingstelle Urheberrecht im Internet“ (CUII) ihre Arbeit aufgenommen. Ihr gehören Urheberrechtsvertreter (wie der Börsenverein des deutschen Buchhandels oder der Verband der Filmverleiher) sowie die größten deutschen Internet-Zugangsprovider an. Ihr Ziel: Die Ahndung von Urheberrechtsverletzungen im Internet in Gestalt von DNS-Sperren durch die Provider.

Voraussetzung für die Beantragung der Sperrung einer „strukturell urheberrechtsverletzenden Webseite“ (SUW) ist, dass die Inanspruchnahme des Webseitenbetreibers durch den Rechteinhaber keine Erfolgsaussichten hat, dieser aber „zumutbare Maßnahmen“ zur Aufdeckung der Identität des Webseitenbetreibers unternommen hat.

Die Entscheidung über eine Sperrung trifft ein Prüfausschuss einstimmig, den ein „unbefangener Vorsitzender“ mit Befähigung zum Richteramt leitet. Vor der Sperrung durch die Provider wird die Einhaltung der Netzneutralitätsvorgaben (EU 2015/2120) durch die Bundesnetzagentur geprüft. Ein sechsköpfiger Steuerkreis überwacht die Arbeit der CUII und beschließt über den Verhaltenskodex, in dem Antrags- und Sperrverfahren beschrieben sind.

Diese „Notwehrmaßnahme“ der Urheberrechtsinhaber hinterlässt trotz der Selbstbeschränkung auf jährlich maximal 200 Anträge einen schalen Beigeschmack, entscheidet doch ein privates Gremium statt unabhängiger Gerichte über die Zugänglichkeit von Webseiten – und damit über die Grundrechte Dritter, wie der Verfassungsblog am 24.03.2021 kritisierte.

Auch die Rolle der Bundesnetzagentur bleibt nebulös, denn sie ist „durch Briefwechsel“ nichtöffentlich vereinbart und schließt offenbar eine inhaltliche Prüfung der Sperrempfehlung nicht ein. Ein Verfahren also, bei dem sich erst erweisen muss, ob die Trennlinie zu „sonstigen unerwünschten Webseiten“ (SUW) klar gezogen bleibt.

Warnung vor IT-Produkten

Dürfen (Datenschutz-) Aufsichtsbehörden vor dem Einsatz bestimmter IT-Produkte warnen, wenn hierzu datenschutzrechtliche Bedenken bestehen? Die Zwischenergebnisse zu dieser Frage hat der Arbeitskreis (AK) “Grundsatz der DSK zu den Rahmenbedingungen für aufsichtsbehördliche Produktwarnungen der Datenschutzkonferenz” (DSK) bereits am 09.11.2020 in einem noch abzuschließenden Gutachten vorgestellt. Dabei wird auch die Frage beleuchtet, ob sich die aufsichtsrechtliche Legitimation aus Art. 57 Abs. 1 lit. b i.V.m. Art. 58 Abs. 3 lit. b DSGVO ergibt. Das Gutachten kommt zu dem Zwischenergebnis, dass eine Warnung unter drei Voraussetzungen rechtens sei:

- Richtigkeit der Information,
- Sachlichkeit der Information und
- Berücksichtigung des Verhältnismäßigkeitsgrundsatzes (Erforderlichkeit und Angemessenheit).

Überdies bestehe die Notwendigkeit der Überprüfung einer zeitlichen Befristung der Produktwarnung, die sich insbesondere aus § 40 Lebensmittel- und Futtermittelgesetzbuch (LFGB) ergebe. Noch nicht abschließend bewertet ist die Frage, ob den betroffenen Herstellern vor Publikation die Möglichkeit einer Stellungnahme gewährt werden sollte.

Noch gibt es zahlreiche offene Fragen. So werden nicht alle Aufsichtsbehörden dieselbe Einschätzung vertreten. Und welche Bewertungsmaßstäbe und -kriterien werden zu Grunde gelegt, um Einheitlichkeit und Vergleichbarkeit zu schaffen? Diese Fragen sollen auf der nächsten Datenschutzkonferenz am 28./29.04.2021 geklärt werden.

Trotz des offensichtlichen Nutzens einer im Idealfall einheitlichen Bewertung der Aufsichtsbehörden sind grundsätzliche Bedenken angebracht. Denn an Lebensmittelwarnungen werden sehr hohe Anforderungen gestellt, die weit über die des DSK hinausgehen:

So müssen „hinreichende Anhaltspunkte dafür vorliegen, dass von einem Erzeugnis eine Gefährdung für die Sicherheit und Gesundheit ausgeht oder ausgegangen ist“. Ob Anhaltspunkte für eine Gefährdung beispielsweise bei den von der Berliner LDSI inkriminierten Videokonferenz-Lösungen (SSN 3/2021) vorliegen, muss ernsthaft bezweifelt werden.

Kryptotrojaner ohne Lösegeld

Danny Palmer beschrieb am 25.03.2021 auf ZDnet, wie die Firma Spectra Logic einen Kryptotrojaner loswurde – ohne Lösegeld zu bezahlen. Zwei Dinge waren dafür erforderlich: Die Entscheidung der Geschäftsführung gegen eine Lösegeldzahlung und eine IT-Abteilung, die bis zum Umfallen Überstunden machte, um die Firma wieder „ans Laufen“ zu bringen. Nach acht Tagen waren zumindest die wichtigsten Systeme wieder betriebsbereit. Das mutet an wie ein Königsweg – doch vor dem erleichterten Aufatmen sollte man zunächst drei Fragen beantworten:

- Wie würde Ihre Geschäftsführung entscheiden – für oder gegen eine Lösegeldzahlung?
- Gibt es in Ihrer IT-Abteilung Bereitschaftsregelungen für Notfälle? Können externe Dienstleister eingebunden werden – und wenn ja: welche und wie?
- Kennen Sie Ihre kritischen Prozesse und Systeme? Wie viele Tage würden Sie voraussichtlich benötigen, um die IT für die wesentlichen Geschäftsprozesse wiederherzustellen? Ab welcher Dauer ist ein IT-Ausfall existenzbedrohend?

Wer sich auf eine Selbstmedikation im Falle eines erfolgreichen Kryptotrojaner-Angriffs vorbereiten will, sollte sich dabei an Standards wie dem BSI-Standard 200-4 orientieren – und seine Backup- und Notfall-Pläne auch üben. So realistisch wie möglich. Und sie vor allem ausdrucken, damit der Kryptotrojaner sie nicht mitverschlüsselt.

TKG novelliert

Am 22.04.2021 wurde die Novelle des Telekommunikationsgesetzes (TKG) verabschiedet. Wer gehofft hatte, dass damit Klarheit hinsichtlich der rechtlichen Behandlung von Videokonferenzen geschaffen würde, wurde enttäuscht. Aber es ist ein Trend erkennbar, der zumindest für das in Abstimmung befindliche Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) hoffen lässt. Mit den Regelungen über die sog. Universaldienste (§§ 78 ff. TKG) wird klar, dass die Ausweitung des Fernmeldegeheimnisses (§ 88 TKG) auf Anbieter von sog. Over-the-top-Diensten näher rückt.

Damit wäre die Forderung der Aufsichtsbehörden nach Auftragsverarbeitungsverträgen hinfällig: Die Verantwortlichkeit für die Sicherheit der Dienste läge bei den Dienstanbietern und nicht bei den Nutzern; zuständige Kontrollinstanz wäre die Bundesnetzagentur. Diese Entwicklung ist aus unserer Sicht dringend geboten und wird bereits seit langem gefordert (siehe z. B. das ZEW-Gutachten von Prof. Thomas Fetzer, Universität Mannheim, aus dem Jahr 2016).

Secorvo News

Enigma zum Selberdrucken

Die ENIGMA zählt zweifellos zu den faszinierendsten Verschlüsselungsverfahren in der Geschichte der Kryptografie. Berühmt wurde sie nicht nur durch ihre bedeutende Rolle im Zweiten Weltkrieg, sondern vor allem auch durch ihre geniale Entschlüsselung unter Mitwirkung des Informatik-Pioniers Alan Turing.

Enigma I aus dem 3D-Drucker (Foto: Prof. Wiest)

Seit 2017 rekonstruieren Studierende der Hochschule der Medien in Stuttgart im Projekt „ENIGMA R.D.E.“ diese berühmteste Chiffriermaschine der Welt, von der nur wenige Originalgeräte erhalten sind, im 3D-Druckverfahren. Ziel ist eine Konstruktionsanleitung, mit der Laien für unter 300 € Materialkosten ein funktionierendes Gerät in Originalmaßen anfertigen können. Das Projekt wurde 2019 mit dem Landeslehrpreis des Ministeriums für Wissenschaft, Forschung und Kunst Baden-Württemberg ausgezeichnet.

Die Veröffentlichung der Anleitung ist für den Spätsommer 2021 geplant. Bei unserem kommenden KA-IT-Si-Event am **20.05.2021** dürfen Sie bereits einen Blick auf ein funktionierendes Modell werfen: Prof. Wiest wird von der bewegten Geschichte des Projekts berichten, gibt Einblicke in die Besonderheiten des Nachbaus und entschlüsselt selbstverständlich auch live Geheimbotschaften mit seiner ENIGMA.

Diesmal erhalten Sie kurz vor dem Event nicht nur eine kleine Stärkung per Post von uns, sondern auch Ihre ganz persönliche Enigma, damit Sie die Nachricht des Referenten entschlüsseln können. Lassen Sie sich überraschen! Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen – nach den überwältigenden Teilnehmerzahlen der letzten Events auch diesmal online – und kostenlos (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2021	
04.-07.05.	Blackhat Asia 2021 (Blackhat, virtuell)

17.-20.05.	Security Cruise (Connecting Media, virtuell)
19.-21.05.	BvD Verbandstage 2021 (BvD, virtuell)
19.-20.05.	22. Datenschutzkongress (EUROFORUM, virtuell)
20.05.	Enigma zum Selberdrucken (KA-IT-Si, virtuell)
Juni 2021	
08.06.	Datenschutztag 2021 (COMPUTAS, Berlin)>
09.-11.06.	Entwicklertag 2021 (VKSI, GI, ObjektForum , virtuell)
14.-15.06.	DuD 2021 (COMPUTAS, Berlin)
17.-18.06.	Annual Privacy Forum 2021 (ENISA, DG Connect, Católica University of Portugal, virtuell)

Fundsache

Neben Kali Linux gibt es weitere Linux-Distributionen, die einen umfassenden Werkzeugkasten für Penetrationstester bieten, wie beispielsweise BlackArch und Parrot OS. Von letzterer erschien am 28.03.2021 Version 4.11. Zu den Änderungen zählen sowohl eine Vielzahl aktualisierter und besser kurierter Hacking-Werkzeuge als auch der Umstieg auf eine LTS-Version. Auch ARM-Architekturen werden wieder unterstützt. Wer in der Vergangenheit Schwierigkeiten mit Kali hatte, dem sei Parrot OS ans Herz gelegt – unseren Erfahrungen nach ist Parrot OS an einigen Stellen gepflegter, zuverlässiger und stabiler.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, 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