# Secorvo Security News

Oktober 2022

## SPoTs

Viele Desaster haben ihren Ursprung in einem „Single Point of Failure“ (SPoF) – einem Glied in einer wichtigen Prozesskette, dessen Ausfall nicht kompensiert werden kann und den Prozess zum Stillstand (oder, schlimmer noch, zum Kippen oder Aufschwingen) bringt. So gab es auf der Titanic, als nach der Kollision mit einem Eisberg sechs statt maximal vier geschottete Bereiche voll Wasser liefen, nicht genügend Rettungsboote, um alle Passagiere aufzunehmen. Und in Tschernobyl löste eine Stromabschaltung im Rahmen eines Sicherheitstests die Katastrophe aus.

Besonders bei der Digitalisierung ist ein SpoF schnell übersehen: Analoge Fall-Back-Lösungen, auf die man sich bei der Prozesseinführung noch verlassen konnte, verschwinden unvermittelt, ohne dass ihre Rolle im Prozess bedacht wird. Oder ein SPoF wird „sehenden Auges“ in Kauf genommen, weil die Alternativlösung teuer ist oder ein Ausfall unwahrscheinlich erscheint – und schon steht die Gasversorgung auf der Kippe.

Eine ähnliche Rolle spielen „Single Points of Trust“ (SPoT) in IT-Infrastrukturen. Sie werden besonders leicht übersehen, weil ihre Bedeutung meist nur Experten verständlich und selbst diesen nicht immer präsent ist. So hängt die Sicherheit einer Verschlüsselungslösung beispielsweise am Zufallszahlengenerator oder die des Unternehmensnetzwerks am Zugang zum Domain-Controller. Angreifer und Nachrichtendienste lieben SPoTs, denn sie erlauben fokussierte Angriffe mit großer Wirkung und eher geringem Entdeckungsrisiko.

Die SPoTs des Internet sind die Root-Zertifikate in Browsern und Betriebssystemen. Wer darüber verfügt, kann vertrauenswürdige Software, Webseiten und E-Mails erzeugen. Nach einer Untersuchung der Washington Post vom 08.11.2022 könnte das amerikanischen Nachrichtendiensten über einen Spyware-Spezialisten unter dem Decknamen TrustCor gelungen sein. Mehr als 10.000 Zertifikate sind betroffen. Nicht zum ersten Mal.

## Security News

### ITSIG 2.0-Umsetzung

Für Unternehmen, die zur kritischen Infrastruktur zählen, dürfte die am 29.09.2022 vom BSI veröffentlichte finale Version der Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung von großer Bedeutung sein. Darin konkretisiert das BSI die Umsetzung der Anforderungen aus § 8a BSI Absatz 1a. Vor dem Hintergrund, dass das ITSIG 2.0 bereits im Mai 2021 verabschiedet wurde und die Anforderungen daher bis Mai 2023 umgesetzt werden müssen, kommt die Veröffentlichung überraschend spät – umso mehr, als die

Orientierungshilfe sehr umfangreiche Detailanforderungen stellt.

## Safe Harbor III

Die am 07.10.2022 von US-Präsident Biden unterzeichnete Executive Order soll das neue transatlantische Data Privacy Framework vorbereiten. Die Verordnung sieht ein Datenschutzüberprüfungsgericht vor und führt den Verhältnismäßigkeits- und Notwendigkeitsgrundsatz für den Zugriff auf Daten durch US-Geheimdienste ein. Damit wollen die USA die Anforderungen aus dem Schrems-II-Urteil des EuGH (siehe SSN 8/2020) umsetzen.

Doch es gibt bereits Kritik. So ist zum einen eine Executive Order kein Gesetz, sondern lediglich eine interne Anweisung an US-Bundesbehörden. Zum anderen ist das zu gründende „Gericht" lediglich eine beim Director of National Intelligence angesiedelte Verwaltungsstelle zur Entgegennahme und Prüfung von Beschwerden. Der LfDI Baden-Württemberg, Dr. Stefan Brink, hat am 26.10.2022 erhebliche Zweifel geäußert, dass damit den Anforderungen des EuGH entsprochen wird.

Auch Max Schrems hat bereits am 07.10.2022 eine detaillierte Prüfung angekündigt. Nun muss die EU-Kommission entscheiden, ob sie auf dieser Basis einen neuen Angemessenheitsbeschluss erlassen kann. Eines ist jedenfalls sicher: Sollte es zu einer Anerkennung der EU kommen, ist ein weiteres EuGH-Urteil unausweichlich.

## Grundschutz-Renovierung

Wegen der kontinuierlichen Weiterentwicklung des IT-Grundschutzes müssen zertifizierte Organisationen neue Bausteine im Blick behalten. Dazu pflegt das BSI eine Liste der Final-Draft-Versionen der Bausteine, die überarbeitet oder neu im IT-Grundschutz-Kompendium erscheinen werden, ggf. ergänzt um ein Änderungsdokument. Kürzlich wurden in der Liste 11 Bausteine als Final Draft publiziert, die 2023 in das Kompendium aufgenommen werden sollen. Die beiden prominentesten sind wohl SYS.1.1 Allgemeiner Server und SYS.1.2.3 Windows Server. Hier stechen vor allem die Hinweise auf die Modellierung vom Baustein SYS.1.1 und die Veröffentlichung eines Bausteins für Windows Server unabhängig von einem konkreten Release ins Auge.

## Unvollstreckbar

Am 20.10.2022 hat die französische CNIL, wie zuvor bereits die italienische, die griechische und die britische Datenschutzaufsichtsbehörde, gegen das US-Unternehmen Clearview AI ein Bußgeld in Höhe von 20 Mio. € verhängt. Clearview AI durchsucht das Internet nach öffentlich verfügbaren Fotografien von Gesichtern, erfasst diese und bietet u. a. Strafverfolgungsbehörden Zugriff auf diese Datenbank an, um Personen mit Gesichtserkennungsverfahren zu identifizieren (siehe SSN 1/2020). Dagegen haben Einzelpersonen sowie Privacy International Einspruch erhoben.

Zuvor hatten die Aufsichtsbehörden in Absprache unabhängig voneinander Clearview AI aufgefordert, auf

ihrem Staatsgebiet die Erhebung und Nutzung von Daten von Personen ohne Rechtsgrundlage einzustellen und die Ausübung der Betroffenenrechte sicherzustellen. Clearview AI reagierte nicht oder verwies darauf, dass es keiner Geschäftstätigkeit innerhalb der EU nachgehe.

Da Clearview AI nicht über einen europäischen Repräsentanten oder eine europäische Niederlassung verfügt, können die verhängten Bußgelder und Bescheide nicht vollstreckt werden. Das neue Data Privacy Framework mit den USA sollte daher auch die Durchsetzung europäischer Sanktionen regeln.

## AV mit US-Konzerntöchtern

Am 07.09.2022 hob das Oberlandesgericht (OLG) Karlsruhe eine Entscheidung der Vergabekammer Baden-Württemberg auf, die den Einsatz von Infrastrukturdiensten europäischer Tochterunternehmen von US-Cloud-Anbietern als grundsätzlich datenschutzwidrig eingestuft hatte.

Ganz so einfach ist es demnach nicht: Allein aus der Tatsache, dass ein Dienstanbieter die europäische Tochter eines US-Konzerns ist, darf nicht geschlossen werden, dass das Unternehmen sein Leistungsversprechen nicht erfüllen kann. Die Konzernbindung führt nicht zwangsläufig zu rechts- und vertragswidrigen Weisungen der Konzernmutter, und es darf auch nicht unterstellt werden, dass die Geschäftsführung solche Weisungen ohne weiteres umsetzen wird. Wenn die europäische Gesellschaft vertraglich zusichert, dass sie die Daten nur innerhalb der EU verarbeitet, darf man darauf vertrauen.

## BCM-Standard

Am 26.09.2022 machte das BSI den zweiten Community Draft des Standards BSI 200-4 Business Continuity Management zugänglich. Anders als in der ersten Entwurfsversion richtet sich der Standard nicht mehr an einem Stufenmodell aus, sondern ist nach den einzelnen Prozessschritten strukturiert. Für die Umsetzung von Business oder IT-Service Continuity ist der Standard auch im derzeitigen Entwurfsstadium bereits eine hilfreiche Leitlinie.

## Cookie-Nervenschoner

Die Verbraucherzentrale Bayern hat am 11.10.2022 den „Nervenschoner" vorgestellt, ein Browser-Plugin für Firefox und Chrome, das Cookie-Banner auf Webseiten blockiert. Da der EuGH für das Setzen von Cookies eine Einwilligung des Webseitenbesuchers fordert, kann bei einem blockierten und ausgeblendeten Cookie-Banner keine Einwilligung erteilt werden – was einem Click auf „Alles Ablehnen" entspricht. Der „Nervenschoner" basiert auf dem bekannten Browser-Plugin uBlock Origin und blockiert neben dem Einwilligungsbanner auch die zugehörigen Tracker. Er ist genau wie uBlock Origin Open Source Software.

Neben dem „Nervenschoner" gibt es ähnliche Tools, auch für andere Browser (wie beispielsweise Hush für Safari auf macOS und iOS), für die der „Nervenschoner" bisher nicht verfügbar ist.

### Cybersecurity Skills

Die Agentur der Europäischen Union für Cybersicherheit (ENISA) veröffentlichte am 19.09.2022 das European Cybersecurity Skills Framework (ECSF). Es soll ein gemeinsames Verständnis der Rollen, Kompetenzen, Fähigkeiten und Kenntnisse schaffen, die zur Gewährleistung von Cybersecurity in Unternehmen zusammenwirken sollten. Neben dem Chief Information Security Officer (CISO) beschreibt das ECSF elf weitere Rollen wie den Cyber Incident Responder, den Cybersecurity Educator oder den Digital Forensics Investigator.

Ergänzend zum ECSF stellte die ENISA ein 50seitiges Benutzerhandbuch online, in dem der Aufbau einer Cybersecurity-Organisationsstruktur u. a. anhand von sieben Use Cases veranschaulicht wird.

Für kleine und mittelständische Unternehmen dürfte das Konzept wie ein „overkill" wirken – ist es doch schon herausfordernd genug, die Rolle des CISO kompetent zu besetzen. Es zeigt allerdings auch, dass der für einen wirksamen Schutz vor Cyberangriffen erforderliche Aufwand nicht unterschätzt werden sollte.

## Secorvo News

### Seminarangebote

Unser letztes T.I.S.P.-Seminar in diesem Jahr (**14.–18.11.2022**) ist ausgebucht. Für Schnellentschiedene: Die nächsten Gelegenheiten für eine T.I.S.P.-Qualifizierung bieten wir am **27.–31.03.2023** und **19.–23.06.2023**, jeweils optional mit anschließender Prüfung. Und zur Vorbereitung legen wir Ihnen unser T.I.S.P.-Begleitbuch ans Herz, das wir Ihnen nach Ihrer Anmeldung zusenden.

Eine letzte Chance für eine Weiterbildung in diesem Jahr bieten wir Ihnen mit unserem neuen dreitägigen Seminar BSI Vorfall-Experte (**29.11.–01.12. 2022**) – einige wenige Plätze haben wir noch frei.

Die vollständigen Programme und den Link zur Online-Anmeldung finden Sie auf unserer Webseite.

### Lernen wird überbewertet

Vor rund einem Jahr sorgte die Schwachstelle log4j für erhebliche Aufregung. Der Auslöser wurde mittlerweile beseitigt, und viele der betroffenen Softwareprodukte von den Herstellern gepatcht.

Doch die tiefere Ursache des Problems besteht weiterhin. Denn die Schwachstelle war gar kein Fehler, sondern eine gewünschte Funktionalität, die über viele Jahre in der Bibliothek enthalten war. Das eigentliche Problem bestand vielmehr darin, dass eine komplexe und leistungsfähige Bibliothek für sehr einfache Aufgaben eingesetzt und an der Schnittstelle nutzergenerierte Inhalte ohne Input-Validierung übergeben wurden. Verursacher war also nicht log4j, sondern die Tatsache, dass die Bibliothek verwendet wurde, ohne zuvor zu prüfen, ob die Funktionalität überhaupt gebraucht wird.

Security-by-Design geht anders, wie Johann Grathwohl (CONITAS) auf dem kommenden **KA-IT-**

**Si-Event am 08.12.2022** in seinem (Online-) Vortrag zeigen wird. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

## Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

| November 2022 | |
|---|---|
| 07.-11.11. | ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US) |
| 09.-10.11. | T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin) |
| 14.-18.11. | T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe) |
| 29.11.-01.12. | BSI Vorfall-Experte - Aufbauschulung (Secorvo, Karlsruhe) |
| **Dezember 2022** | |
| 05.-08.12. | Black Hat Europe 2022 (Blackhat, London/UK) |
| 08.12. | KA-IT-Si-Event „Lernen wird überbewertet“ (KA-IT-Si, online) |
| **Januar 2023** | |
| 20.-22.01. | ShmooCon 2023 (The Shmoo Group, Washington/US) |

## Fundsache

Auf iPhones und iPads dürfen Verschlusssachen der Kategorie VS-NfD „Nur für den Dienstgebrauch“ verarbeitet werden. Das hat das BSI am 05.10.2022 bestätigt. Voraussetzungen sind die Umsetzung von Vorgaben an das Nutzerverhalten, VPN-Anbindung und Mobile Device Management.

## Impressum

Secorvo Security News – ISSN 1613-4311

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