secorvo
security consulting

Secorvo Security News

März 2020

Panikresistenz

Seit drei Wochen befindet sich die Welt im Ausnahmezustand. Für Sicherheits- und Datenschutzbeauftragte ist das eine harte Belastungsprobe – denn angesichts der drohenden Überlastung unseres Gesundheitssystems und der teilweise existenziellen Auswirkungen des „Social Distancing" auf die wirtschaftliche Situation vieler Unternehmen stehen Datenschutz und Sicherheit derzeit hinter anderen Prioritäten zurück.

An keinem Thema wird das gerade deutlicher als an der Diskussion über ein Handy-Tracking zur Kontaktnachverfolgung. Zwar wurden die Verkehrs- und Standortdaten am 25.03.2020 doch nicht auf dem Altar des „Gesetzes zum Schutz der Bevölkerung bei einer epidemischen Lage von nationaler Tragweite" geopfert – aber wohl nur, weil der Gesetzgeber in letzter Sekunde verstand, dass die Daten der Mobilfunknetze viel zu ungenau sind, um feststellen zu können, ob der Abstand zweier Smartphone-Nutzer zueinander kleiner als zwei Meter ist: Eine einzelne Funkzelle kann schließlich eine Fläche mit einem Durchmesser von bis zu 35 km abdecken.

Nun aber wird es spannend. Denn die derzeit diskutierte „Corona-App", die via Bluetooth Kontaktpersonen registriert und nach einem positiven Corona-Test alle bis zu 20 Tage zurückliegenden Kontakte informiert, erfordert die freiwillige Mitwirkung der Smartphone-Nutzer: Auch die Kontaktperson benötigt die App, und flächendeckend funktioniert das System erst mit mindestens 60% aller Bürger.

Anders als die Tracking-Lösungen, die in China, Polen oder Israel eingesetzt werden, soll die App anonym arbeiten – aber die Warnung zentral absetzen. Man darf gespannt sein, wie dieser Zielkonflikt gelöst wird – und ob man die Chance für „Privacy by Design" auch diesmal verspielt. Denn Anonymität ist tatsächlich möglich – erfordert aber eine dezentrale Datenhaltung, Verschlüsselung und wechselnde Pseudonyme. Das Ergebnis wird zeigen, wie panikresistent unser Grundrechtsverständnis wirklich ist.

Inhalt

secorvo
security consulting

Security News

Datenschutz-Abmahnung

Am 27.02.2020 entschied das OLG Stuttgart, dass Unternehmen wegen fehlender Datenschutzerklärungen abgemahnt werden können. Das Gericht musste zunächst klären, ob § 13 Telemediengesetz oder die Datenschutz-Grundverordnung (DSGVO) anzuwenden war. Letztere genießt Vorrang, da sie die EU-Datenschutz-Richtlinie ersetzt hat. Nach Auffassung des Gerichts handelt es sich bei den Vorschriften der DSGVO um Marktverhaltensregeln – nur dann ist eine Abmahnung nach dem Wettbewerbsrecht (UWG) möglich. Da Art. 80 DSGVO nicht abschließend regelt, wie Verstöße gegen die DSGVO rechtlich durchzusetzen sind, sind außerdem Wettbewerbsverbände klagebefugt.

Wer keine Datenschutzerklärung auf seiner Webseite vorhält, verstößt damit nicht nur gegen seine (Informations-) Pflichten aus Art. 13 DSGVO, sondern auch gegen § 3a UWG, da die Erfüllung von Informationspflichten einen Wettbewerbsbezug aufweist: Kommt man seinen Informationspflichten nicht nach, macht man sich das Leben (zu) leicht, deshalb darf abgemahnt werden. Es wäre nicht überraschend, wenn diese Rechtsprechung zukünftig auf unvollständige Datenschutzerklärungen ausgeweitet wird – hier können also Abmahnungen von Wettbewerbern drohen.

Kritische Leitsystem-Lücken

Sicherheitsforscher der Kaspersky Lab Security Services hatten bereits am 28.12.2019 auf dem Chaos Computer Congress (36c3) gravierende Lücken im Prozessleitsystem Siemens SPPA-T3000 offengelegt, das hauptsächlich in Kraftwerken eingesetzt wird. Am 21.02.2020 veröffentlichten sie nun ein White Paper mit Details. In diversen Komponenten des T3000 entdeckten sie sowohl veraltete Software-Versionen (wie Windows Server 2003) als auch Schwachstellen in den T3000-Anwendungen, Standardpasswörter und gravierende Konfigurationsfehler. Die Angriffsfläche ist dabei vergleichsweise groß: Angreifer können zentrale Komponenten übernehmen, Informationen extrahieren, Rechte erweitern und somit schlimmstenfalls die vollständige Kontrolle über ein Kraftwerk gewinnen. Hierfür ist jedoch eine Verbindung zum internen Leittechnik-Netz notwendig, die normalerweise den Zutritt zur Anlage erfordert. Allerdings wird manchmal aus anderen Netzen Zugriff auf die Leittechnik-Netze gestattet.

Siemens hatte schon im Dezember ein Advisory veröffentlicht und viele der Schwachstellen in Updates beseitigt. Allerdings werden diese nach unserer Erfahrung häufig nicht oder erst stark verzögert eingespielt. Die Forscher veröffentlichten zusätzlich Anweisungen und Tools für T3000 Assessments, mit denen das Vorhandensein einiger der Schwachstellen festgestellt und deren Ausnutzung vermieden werden können. Bei bedachtem Vorgehen wird von einer solchen Prüfung der Betrieb nicht beeinträchtigt.

Wiederbelebungsversuch

Am 21.02.2020 hat Kroatien einen neuen Entwurf für die ePrivacy-Verordnung – die die ungeliebte Cookie-Richtlinie ersetzen soll – an die Delegationen der anderen EU-Mitgliedstaaten versandt, nachdem der vorherige Entwurf (SSN 6/2019) gescheitert war. Ein „vereinfachter" Text soll nun mit der DSGVO in Einklang gebracht werden. Dieser Versuch besteht vor allem darin, Einwilligungen durch das berechtigte Interesse an der Datenverarbeitung zu ersetzen. Beim berechtigten Interesse wird wie in der DSGVO eine Interessenabwägung vorgenommen.

Kroatien macht dabei für das Tracking Vorschläge, wann ein berechtigtes Interesse ausreichen soll und welche Interessen der Verbraucher dem entgegenstehen können. Bei der Abwägung ist zu berücksichtigen, ob der Endnutzer vernünftigerweise damit rechnen kann, dass der Verantwortliche dessen personenbezogene Daten verarbeitet. Dabei wird auf die Vorgaben der DSGVO Bezug genommen.

Im Hinblick auf die Rechtsprechung des Europäischen Gerichtshofs (EuGH), der nicht zuletzt in der Planet-49-Entscheidung (SSN 10/2019) den Schwerpunkt auf die Erteilung von Einwilligungen gelegt hat, muss man sich fragen, warum die Ansätze des EuGH im Hinblick auf das Verhältnis von Einwilligung und berechtigtem Interesse nicht berücksichtigt und nicht einmal in der Begründung angesprochen werden.

Datenschutz und Social Media

Der LfDI Rheinland-Pfalz hat am 06.03.2020 einen neuen Handlungsrahmen für öffentliche Stellen im Umgang mit Social-Media-Plattformen bereitgestellt. Anhand des EuGH-Urteils zu Facebook-Fanpages, des anschließenden Urteils des Bundesverwaltungsgerichts zur Möglichkeit der Datenschutzaufsichtsbehörden, sich statt an Facebook auch an den Fanpage-Betreiber zu halten und ergänzenden Beschlüssen der Datenschutzkonferenz führt das Papier die Anforderungen an Behörden-Präsenzen bei Social-Media-Plattformen aus. Für den rechtskonformen Betrieb benötigt man zunächst eine Rechtsgrundlage für die Weitergabe von Daten an den Social-Media-Anbieter, i.d.R. eine Nutzer-Einwilligung. Der LfDI akzeptiert eine Einwilligung re-

gistrierter Nutzer gegenüber dem Social-Media-Anbieter, sofern diese auf ausreichender Transparenz beruht; nicht registrierte Nutzer müssten gesondert einwilligen oder ausgeschlossen werden.

Eine weitere Anforderung ist eine transparente Vereinbarung des Betreibers mit dem Plattformanbieter nach Art. 26 DSGVO. Diese muss Antworten auf alle Fragen aus dem DSK-Beschluss vom September 2018 bieten, was die aktuelle Facebook-vereinbarung z. B. zu Löschfristen der Daten nicht erfüllt. Weiter sind die Informationspflichten aus Art. 13 DSGVO zu erfüllen und es wird ein Datenschutz-Konzept für das Angebot gefordert.

Die Forderungen sind auf private Stellen übertragbar. Fazit: Derzeit kann kein Social-Media-Angebot datenschutzkonform betrieben werden. Abhilfe könnten nur die Plattform-Anbieter schaffen.

Apple begrenzt Zertifikatsgültigkeit

Beim Treffen des CA/Browser Forums in Bratislava am 19./20.02.2020 kündigte Apple an, ab September 2020 keine neu erstellten TLS-Zertifikate mehr zu akzeptieren, die länger als 13 Monate (398 Tage) gültig sind. Die am 03.03.2020 veröffentlichte Regelung bezieht sich nicht nur auf den Safari-Browser, sondern auf alle Apps, die TLS-Funktionen eines Apple-Geräts nutzen – vom Mac bis zur Apple Watch. Betroffen sind ausschließlich öffentliche Zertifikate, die unterhalb der im Apple-Ökosystem vorinstallierten Root CAs ausgestellt wurden. Wer eine interne PKI betreibt, kann weiterhin länger gültige Zertifikate nutzen.

Apple widersetzt sich mit der neuen Regelung dem Ergebnis der Abstimmung SC22 des CA/Browser Forums vom September 2019, das eine Kürzung der maximalen Zertifikatsgültigkeit für öffentlich gültige TLS-Zertifikate auf 13 Monate abgelehnt hatte. Apple setzt die Verkürzung nun beim Endnutzer durch und erzwingt somit einen neuen de-facto Standard bei allen Webseitenbetreibern, die mit Apple-Geräten kompatibel bleiben wollen.

Aus Sicherheitssicht ist Apples Regelung zu unterstützen, da einerseits Webseitenbetreiber gedrängt werden, aktuelle Zertifikate mit ggf. angepassten Krypto-Standards zu nutzen und ihr Zertifikatsmanagement besser zu automatisieren, sowie andererseits die Risiken durch die häufig laxe (Nicht-)Nutzung von Sperrprozessen zeitlich begrenzt werden. Allerdings ist zu befürchten, dass andere Browser-Hersteller nachziehen und Abstimmungen im CA/Browser Forum durch eigene Wild-West-Regelungen unterminieren.

Wer öffentlich gültige Zertifikate nutzt, kann mit ACME das Zertifikatsmanagement automatisieren. Für interne Systeme unterstützt Sie dabei unsere Lösung Certificates ready2go.

Benachrichtigungspflicht

Datenschutzvorfälle müssen, sofern ein Risiko für die Rechte und Freiheiten der Betroffenen nicht ausgeschlossen werden kann, innerhalb von 72 h der Aufsichtsbehörde gemeldet werden (Art. 33 DSGVO). 2019 kam es allein in Baden-Württemberg zu 1.824 Meldungen, wie Dr. Stefan Brink (LfDI) am 13.02.2020 in seinem Vortrag bei der Karlsruher IT-Sicherheitsinitiative verriet. Und das ist wahrscheinlich nur die Spitze des Eisbergs. Ein zweiter Hinweis war aber noch wichtiger: Die Aufsichtsbehörde erwartet, sofern besondere personenbezogene Daten (wie medizinische) von dem Vorfall betroffen sind, eine unverzügliche Benachrichtigung der Betroffenen nach Art. 34 DSGVO.

Secorvo News

Rezensenten gesucht

Entschleunigung ist eine wichtige Voraussetzung dafür, dass Menschen sich nicht nur um Dringendes, sondern auch um Wichtiges kümmern. Wie zum Beispiel Weiterbildung. Im Oktober 2019 erschien die dritte, überarbeitete und erweiterte Auflage unseres Handbuchs „Informationssicherheit und Datenschutz“, zugleich Begleitbuch zum T.I.S.P.-Seminar, im dpunkt.verlag. Es zählt zu den umfassendsten Darstellungen des Themengebiets. Oder, wie ein Leser schrieb: „*Ich war auf der Suche nach einem Lehrbuch, das einerseits die Grundlagen umfassend abdeckt und andererseits eine gewisse technische Tiefe aufweist, was bei vielen amerikanischen Werken rund um die CISSP-Zertifizierung leider nicht der Fall ist. Das Buch erfüllt diese Anforderungen ganz hervorragend und ist für den Einsatz in der Hochschullehre sehr gut geeignet sowie als Schulungsunterlage für Praktiker und als Nachschlagewerk.*“ Für die Neuauflage suchen wir noch Rezensenten – und können dafür über eine (begrenzte) Anzahl von Freiexemplaren verfügen. Wir freuen uns auf Ihre Kontaktaufnahme.

RaSy/DaSy mit LDAP-Anbindung

Ende März 2020 erschien RaSy/DaSy, das in *ISMS ready2go* und *DSMS ready2go* integrierte Tool zur Durchführung von Risikoanalysen und Datenschutzfolgenabschätzungen (DSFA), in Version 1.5. Die darin neu geschaffene Möglichkeit, Nutzer über eine Anbindung an ein LDAP-Directory wie beispielsweise Microsofts Active Directory (AD) hinzuzufügen, vereinfacht die Administration deutlich. Das überarbeitete Design erleichtert zudem den täglichen Umgang mit RaSy/DaSy.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2020	
21.-22.04.	Datenschutztage 2020 (FFD Forum für Datenschutz, Wiesbaden)
Mai 2020	
06.-07.05.	BvD Verbandstag 2020 (BvD e.V., Berlin)
11.-15.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
12.-15.05.	European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München)
13.-14.05.	21. Datenschutzkongress (EUROFORUM, Berlin)
Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
09.07.	12. Tag der IT-Sicherheit (KA-IT-Si, IHK, CyberForum, KASTEL, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, 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