Secorvo Security News

September 2020

Wehret den Anfängen

Ganz gleich ob im Verein, im Unternehmen oder in einer Behörde: Fehler in und mangelnde Aktualität von Namens- und Adresseinträgen verursachen Jahr für Jahr Millionenkosten. Sendungen erreichen ihr Ziel nicht, Personen werden mehrfach in Datenbanken geführt und zusammengehörende Vorgänge werden nicht miteinander verknüpft. Ein teures Ärgernis.

Diesem Missstand will nun das Registermodernisierungsgesetz (mehr dazu in diesen SSN) amtlicherseits einen Riegel vorschieben: Zukünftig sollen Bundesbürger in über 50 öffentlichen Registern einheitlich unter ihrer Steuer-ID geführt werden. Doppelte Datenhaltung und komplizierte Identifikationen („Wie schreibt sich doch gleich Ihr Name?“) sollen damit der Vergangenheit angehören.

Ein kühner Traum. Und eine fragwürdige Hoffnung – ist doch ein Tippfehler in einer Nummer kaum unwahrscheinlicher als ein Fehler in der Namensangabe und dabei weit schwieriger zu entdecken; mit dem Risiko für den Betroffenen, dass die Ursache für einen solchen fehlerhaften Eintrag in einer Datenbank nicht so leicht nachvollziehbar ist.

Wirklich bedenklich aber ist der Zweck des Gesetzes selbst. Eine einheitliche Identifikation vereinfacht die Verknüpfung und Zusammenführung von Angaben aus unterschiedlichen Datensammlungen. Datenschützer nennen das „Profilbildung“: Es ist genau die Art „angereicherten Wissens“ über Menschen, vor der das Grundrecht der informationellen Selbstbestimmung den Einzelnen schützen soll. Ein ungutes Gefühl hinterlässt auch die Verwendung einer abstrakten Nummer statt des Namens für die eindeutige Identifikation einer Person. Das gab es schon einmal in Deutschland; damals war es Teil eines systematischen Prozesses der Entwürdigung und Verdinglichung von Menschen. Einen Sieg der Bürokratie über die Unordnung sollten wir auch aus diesem Grund verhindern.

Security News

Keine Biometrie zur Zeiterfassung

Das Landesarbeitsgericht Berlin-Brandenburg hat in einem nun veröffentlichten Urteil vom 04.06.2020 die Anforderungen an den Einsatz von Biometrie im Arbeitsverhältnis konkretisiert und elektronische Fingerabdrücke bei der Zeiterfassung für nicht erforderlich und damit unzulässig erklärt.

Bereits das erstinstanzliche Gericht hatte die für den Fingerabdruckabgleich gespeicherten „Minuten“ als biometrische Daten gemäß Art. 9 Abs. 1, 4 Nr. 14 DSGVO eingeordnet. Demzufolge sei nach der Eignung zunächst zu prüfen, ob kein gleich wirksames, das Persönlichkeitsrecht weniger beeinträchtigendes Mittel

existiere. Trotz der vorgetragenen abstrakten Manipulationsgefahr hat das LArbG Chipkarten oder Tokensysteme als gleich wirksam angesehen und damit die Erforderlichkeit im Kontext der betrieblichen Zeiterfassung verneint. Erst wenn die Erforderlichkeit bejaht worden wäre, hätten die vorgetragenen Schutzmaßnahmen (Nichtauslesbarkeit, Pseudonymisierung u.a.) im Rahmen einer Abwägung berücksichtigt werden können.

Das Urteil konkretisiert die Prüfanforderungen an den Einsatz von biometrischen Merkmalen. Bei der Zutrittskontrolle für besonders schutzbedürfte Bereiche bspw. kann der Biometrieeinsatz weiter gerechtfertigt sein, nicht jedoch lediglich zur Vermeidung vermuteter sonstiger Manipulationsgefahren.

Schlüsselkasten

Kryptografische Schlüssel müssen zufällig gewählt werden – für Computer ist das eine Herausforderung. DiceKeys kündigte am 19.08.2020 an, endlich eine Lösung für dieses Dauerproblem gefunden zu haben: rein mechanisch – durch würfeln. Für 25 US$ wird ein spezieller Würfelsatz im Kasten geliefert. Das Ergebnis kann mit einer App abfotografiert werden, sodass man den 192-bit-Schlüssel weiterverwenden kann. Den Schlüssel schützt man, indem man den Kasten mit den Würfeln möglichst feuerfest hinterlegt. Unterhaltsam ist dies in einem Video dargestellt.

KISS

Am 02.09.2020 erlangte ein Feature der auf jedem modernen Windows-Rechner standardmäßig installierten Microsoft Malware Protection traurige Bekanntheit: Über das Programm „MpCmdRun.exe“ konnten mit der Option „-DownloadFile“ Dateien heruntergeladen werden. Ein Angreifer könnte dies z. B. im Rahmen eines „Living off the Land“-Angriffs (LOL) nutzen. Darunter wird der Missbrauch von auf einem System bereits vorhandenen Funktionen und Programme für bösartige Zwecke verstanden. In den vergangenen Jahren nahm die Zahl der LOL-Angriffe laut Symantec deutlich zu. Angriffe über solche „Seitentüren“ sind oft einfach; auch hinterlässt ein Angreifer meist weniger Spuren, löst mit niedrigerer Wahrscheinlichkeit Alarme aus und kann über längere Zeit unentdeckt agieren. Anfang 2020 hatten die Entwickler der 49 kB großen Ragnar Locker Ransomware diese für einen LOL-Angriff genutzt, indem sie sie in einer 282 MB großen MicroXP-basierten virtuellen Maschine versteckten.

Ob und warum das Download-Feature in der Microsoft Malware Protection notwendig ist, teilte Microsoft nicht mit. Mittlerweile ist die Funktion offenbar wieder deaktiviert: So ergaben Tests von Secorvo, dass Downloadversuche verschiedenster Dateien von Microsoft Defender selbst als Angriffsversuch („Trojan:Win32/MpUtilAbuse.A“) erkannt wurden. Bleibt zu hoffen, dass unnötige Features von Microsoft in Zukunft gleich weggelassen werden, anstatt sie im Nachhinein als Trojaner zu identifizieren…

Minimalismus als Grundprinzip für Container, Bibliotheken (SSN 03/2019) und (Browser-)Plugins (SSN

04/2020) hilft auch gegen LOL-Angriffe: Die Angriffsfläche wird reduziert, die Angriffsresilienz erhöht. Lassen Sie weg, was nicht unbedingt nötig ist.

Darf ich mal sehen?

Am 03.09.2020 hat die Datenschutzkonferenz (DSK) ihre neue Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen“ veröffentlicht. Darin werden im Wesentlichen die 2019 vom European Data Protection Board in einer Leitlinie zusammengefassten Grundsätze übernommen. Interessant aus deutscher Sicht sind vor allem die Ausführungen zur Überwachung von Beschäftigten: Hier werden die wichtigsten rechtlichen Rahmenbedingungen erläutert, die ihre Rechtsgrundlage im BDSG haben. Enthalten ist auch eine Checkliste, die auf den ersten Blick zwar hilfreich erscheinen mag, deren Umsetzung dann aber doch entsprechende technische und rechtliche Kenntnisse erfordert. Dies ist insbesondere deshalb wichtig, weil Videoüberwachungssysteme nicht ohne Datenschutz-Folgenabschätzungen eingesetzt werden dürfen.

Wenn Sie also ein Videoüberwachungssystem installieren möchten oder bereits betreiben, sollten Sie sich dringend informieren, ob die in der Regel durchzuführende Interessenabwägung zu Ihren Gunsten ausgeht und ob die Anlage auch sonst den gesetzlichen Anforderungen entspricht.

Einwilligungs-Standards

Mit der seit dem 15.08.2020 zur Verfügung stehenden zweiten Auflage des Transparency & Consent Frameworks (TCF 2.0) hat das Interactive Advertising Bureau ein ambitioniertes Konzept für die Gestaltung datenschutzrechtlicher Einwilligungen auf Webseiten vorgelegt – und mit Google gleich einen zugkräftigen Teilnehmer gewonnen.

Das TCF legt fest, welche Informationen über die Datenverarbeitung mitgeteilt werden müssen und wie die Einwilligungen an die „Vendors“ weitergeleitet werden. Dabei wird das Zusammenwirken von veröffentlichenden Seitenbetreibern, Werbetreibenden, Betreibern von Werbenetzen und Plattformen sowie Einwilligungs-Tools beschrieben (*Consent Management Platform*). Herz des Konzepts ist, wie sichergestellt werden soll, dass neben den Seitenbetreibern auch die Werbeinhaltsanbieter einen Nachweis der Nutzer-Einwilligung erhalten.

Das TCF 2.0 erweitert die „Cookie-Einwilligungen“ auf im Hintergrund aktive Marketingdienstleister wie bspw. Google. Google unterstützt den Standard, setzt bei seinen Kunden die Anwendung aber bislang nicht voraus und betrachtet die eigenen Nutzungsrichtlinien als strenger.

Die Standardisierung der Informationen und deren Darstellung wäre allein bereits ein beachtlicher Erfolg angesichts der Schwierigkeiten jedes Seitenanbieters, aussagekräftige Datenschutzerklärungen zu erstellen. Allerdings betrachtet das TCF die Rolle von Seitenbetreibern, die selbst Werbenetze nutzen, und deren diesbezügliches Tracking nicht ausreichend.

Totgesagte leben ewig

Mit dem als Entwurf vorliegenden Registermodernisierungsgesetzes (RegMoG) will die Bundesregierung die Digitalisierung der öffentlichen Verwaltung voranbringen. Danach sollen über 50 Register der öffentlichen Verwaltung reformiert werden, darunter Melde-, Personenstands-, Personalausweis-, zentrales Fahrerlaubnis-, Bundeszentralregister und das Versichertenverzeichnis der Krankenkassen.

Zentrales Element des RegMoG ist die Einführung eines eindeutigen und veränderungsfesten Ordnungsmerkmals – die Steuer-ID. Dagegen hat sich am 26.08.2020 die Datenschutzkonferenz (DSK) ausgesprochen, auch gegen die Einführung einer anderen einheitlichen Identifikationsnummer für natürliche Personen in öffentlichen Registern.

Gegen die Steuer-ID spricht nach der DSK bereits deren völlige Loslösung aus ihrer steuerlichen Zweckbindung, gegen ein einheitliches Merkmal überhaupt die Gefahr der Bildung von umfassenden Persönlichkeitsprofilen. Bereits 1983 hat das Bundesverfassungsgericht im „Volkszählungsurteil" das Schaffen eines einheitlichen Personenkennzeichens als Vorstufe von Total- oder Teilabbildern der Persönlichkeit als mit der Würde des Menschen nicht vereinbar angesehen. Die DSK schlägt sektorspezifische Kennzeichen nach dem Vorbild Österreichs vor, die das Bundesinnenministerium allerdings mit Verweis auf deren Komplexität ablehnt.

Die Gesetzesbegründung beschreibt die Möglichkeiten der Profilbildung ausschließlich als Vorzüge und belegt damit bereits selbst ausführlich die absehbare Verfassungswidrigkeit.

Secorvo News

Seminarbetrieb wieder aufgenommen

Im September hat Secorvo nach sechsmonatiger Pause wieder die ersten Seminare (unter Beachtung aller Infektionsschutzauflagen) durchgeführt – sehr zur Freude aller Teilnehmer.

Im November bieten wir Ihnen zwei weitere Gelegenheiten, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren:

Das Grundlagen- und Vertiefungsseminar Public-Key-Infrastrukturen (PKI) (**09.–12.11.2020**) und das Zertifizierungsseminar TeleTrusT Information Security Professional – T.I.S.P. (**16.–20.11.2020**).

Zur Vorbereitung auf das T.I.S.P.-Seminar und die anschließende Prüfung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz", das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist – und sich inzwischen vieler positiver bis begeisterter Kritiken erfreut. Vielleicht suchen Sie ja auch noch nach einer Lektüre für die nun wieder längeren Herbstabende…

Ausführliche Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter

https://www.secorvo.de/seminare

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2020	
12.-14.10.	ISSE 2020 (IEEE, Wien/A)
13.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
22.-23.10.	heise devSec 2020 (dpunkt.verlag, heise Developer, heise Security, Heidelberg)
27.-28.10.	IDACON 2020 (WEKA-Akademie, München)
November 2020	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
09.-13.11.	ACM CCS 2020 (ACM/SIGSAC, Orlando/US)
09.-12.11.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
09.-12.11.	Black Hat Europe 2020 (BlackHat, London/UK)
13.-15.11.	FIfFKon20 (FIfF, Berlin)
16.-20.11.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
18.-20.11.	44. DAFTA (GDD, Köln)
19.-20.11.	DeepSec 2020 (DeepSec, Wien/AT)

Fundsache

Am 25.08.2020 veröffentlichte der TeleTrusT-Arbeitskreis „Security by Design“ eine Handreichung zu Design-Prinzipien und Security-Anforderungen an digitale Produkte. Auf 15 Seiten werden wesentliche Punkte kompakt und verständlich dargestellt sowie Handlungsempfehlungen für Hersteller, Anbieter und Betreiber gegeben.

Impressum

Secorvo Security News – ISSN 1613-4311

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