secorvo
security consulting

Secorvo Security News

Dezember 2017

Bärendienst

Noch fünf Monate bis zum Inkrafttreten der Datenschutz-Grundverordnung. Kaum ein Magazin, das nicht mahnt und erinnert – und an prominenter Stelle mit den Sanktionen droht: bis zu 20 Mio. € oder 4 % des weltweiten Vorjahresumsatzes.

Das sind Zahlen, die jede Geschäftsleitung erblassen lassen. Stand der Datenschutz bisher abgeschlagen auf der „Da-sollte-ich-mich-vielleicht-auch-mal-drum-kümmern"-Liste, hat er es nun unter die Top 10 der „Wichtig-und-dringend"-Liste geschafft. Datenschützer frohlocken, Aufsichtsbehörden schwitzen unter den signifikant gestiegenen Beratungsanfragen und Datenschutzexperten schießen allerorts wie Pilze aus dem Boden.

Dabei gibt es für Torschlusspanik nicht den geringsten Grund, ist die DS-GVO doch wenig mehr als eine Kopie des BDSG: Kaum eine Bestimmung, die (zumindest in Deutschland) nicht bereits heute gilt. Neu sind die erweiterten Dokumentationspflichten – aber das kann auch als Ruf nach einem höheren „Reifegrad" des Datenschutz-Managements verstanden werden: Wie die Informationssicherheit wird sich zukünftig auch der Datenschutz mit Prozessen und deren Nachweisbarkeit beschäftigen müssen.

Aber diese Anpassungen rechtfertigen kaum den Handlungsdruck, der mit Blick auf den 25. Mai 2018 aufgebaut wird. Denn wie viele Besuche von Aufsichtsbehörden gab es 2017 tatsächlich? Und woher soll das Personal kommen, das diese Anzahl erhöhen könnte? Wenn aber der letzte Vorstand verstanden hat, dass die DS-GVO doch nicht so heiß gegessen wird, wie sie gekocht wurde, kann der Datenschutz schnell wieder in der Asche landen, aus der er gerade aufsteigt. Und dann könnte es sich als Fehler erweisen, dass es Ordnungsgelder waren, die ihn wichtig gemacht haben – und nicht die Einsicht, dass es beim Datenschutz gar nicht um den Schutz von Daten, sondern von Persönlichkeitsrechten geht. Vermutlich ist es nie eine gute Idee, Grundrechte einem Ablasshandel zu überlassen.

Inhalt

secorvo
security consulting

Security News

Geschenktipp 1

Nachdem am 16.12.2017 bekannt wurde, dass Firefox unerwünscht ein Plug-In installiert, das Daten über die Firefox-Nutzung erhebt, empfehlen wir, Chrome mit den folgenden Plug-Ins zu bescheren, die unerwünschte Werbung und Skripte abschalten.

Das wohl interessanteste ist Privacy Badger der Electronic Frontier Foundation, das über einen lernenden Algorithmus unerwünschte Tracker, Werbung und Cookies zu blockieren versucht. Eine ähnliche Funktionalität bietet das von Firefox bekannte Ghostery. Das Besondere: es kann Tracker verschiedener Kategorien selektiv deaktivieren. Ein klassischer Werbeblocker ist uBlock Origin, der die gängigen Listen unterstützt und nutzt. Erfahrene Anwender können zu uMatrix greifen, das ähnliche Funktionen wie NoScript für Firefox mitbringt.

Am sinnvollsten ist eine Kombination der genannten Plug-Ins: Privacy Badger oder Ghostery als Grundgerüst und als Ergänzung einen Werbeblocker wie uBlock oder uMatrix. Von allen oben genannten Plug-Ins gibt es übrigens auch eine Firefox-Version.

Geschenktipp 2

Sich selbst beschenkt haben die beiden Autodiebe, die in dem am 26.11.2017 von der West Midlands Police veröffentlichten Video die Funkstrecke zwischen dem Autoschlüssel hinter der verschlossenen Eingangstür und dem in der Einfahrt geparkten Wagen mit passender Gerätschaft verlängern.

Uns bescheren sie damit zweierlei: Einerseits eine schöne bildliche Illustration des Man-in-the-Midde Prinzips. Und andererseits die Bestätigung, dass Videoüberwachungen oft nur von beschränktem Nutzen sind – von den Dieben und dem Wagen fehlt bis heute offenbar jede Spur.

Geschenktipp 3

Am 23.11.2017 veröffentlichte Matt Edmondson in seinem Blog, wie sich ein exemplarischer Hidden Service im Tor-Netzwerk durch das Tool Burp Collaborator deanonymisieren lässt: Hidden Services erlauben es, über das Tor-Netzwerk Dienste wie Webserver anzubieten, ohne die IP-Adresse des Servers preiszugeben.

Der Burp Collaborator ist eine 2015 erschienene Erweiterung für das verbreitete Pentesting-Tool Burp Suite, das hilft, Schwachstellen durch die zeitlich versetzte Verarbeitung von Daten zu erkennen – sogenannte Out-of-Band-Angriffe. Dafür werden Hostnamen und URLs mit eindeutigen Merkmalen für jede Anfrage injiziert und danach überwacht, ob diese durch den Server oder nachgelagerte Systeme per DNS aufgelöst bzw. per HTTP angefragt werden. Mit der Erweiterung Collaborator Everywhere lassen sich solche Payloads noch flexibler und großflächiger injizieren.

Der verwundbare Hidden Service löste den HTTP-Header X-Forwarded-For auf und verriet dabei seine tatsächliche IP-Adresse. Der Angriff stellt zwar keine grundsätzliche Verwundbarkeit der Hidden Services dar, illustriert jedoch sehr gut, wie sich der Collaborator einsetzen lässt. Deshalb ist er unser diesjähriger Geschenktipp für Pentester.

Geschenktipp 4

Das Ergebnis des dreijährigen, gemeinsamen Normungsprojekts von Deutscher Bahn, Blancco, DATEV, Secorvo und Toll Collect, die Ende 2016 verabschiedete DIN 66398 („Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“) ist nun, immerhin noch vor Inkrafttreten der Datenschutz-Grundverordnung, in englischer Sprache erschienen und kann beim Beuth Verlag bezogen werden.

Für international tätige Unternehmen – insbesondere mit europäischen Tochter- oder Muttergesellschaften – gehört sie zwingend unter den Weihnachtsbaum.

Geschenktipp 5

Das Bundesarbeitsgericht hat in einem bereits am 25.04.2017 verkündeten und nun schriftlich begründeten Urteil sehr deutlich Grenzen für die Leistungs- und Verhaltenskontrolle gesetzt. Es führt beispielhaft den Abwägungsprozess zwischen Persönlichkeitsrechten und dem Interesse der Arbeitgeber anhand eines Tools zur Erstellung einer „Belastungsstatistik“ vor.

Gegenstand war ein Einigungsstellenspruch über die Auswertung der Schadensfallabwicklung in verschiedenen Außenstellen einer Versicherung. Während der Betriebsrat wegen der – allerdings nicht ausreichend dargelegten – Gesundheitsgefährdung klagte, befand das Bundesarbeitsgericht die gesamte Auswertung für unzulässig. Nach dem aufgeführten Zweck sollten Auslastungsunterschiede der Außenstellen analysiert werden. Hierzu sollte anhand von wöchentlichen bis halbjährlichen, auf den einzelnen Mitarbeiter bezogenen Kennzahlen die quantitativ gemessene Leistung erfasst und bei Abweichung von Schwellenwerten individuell untersucht werden. Das BAG sieht hierin eine unverhältnismäßige ständige Überwachung. Zuvor äußerte es bereits Zweifel an der Eignung und

Erforderlichkeit zum behaupteten, grundsätzlich anzuerkennenden Zweck.

Ausgedruckt ein perfektes Last-Minute-Geschenk für Betriebsräte – Datenschützer müssen hingegen die Kröte schlucken, dass das Bundesarbeitsgericht strikt mit dem Persönlichkeitsrecht argumentiert und weder die informationelle Selbstbestimmung noch § 32 BDSG heranzieht.

Geschenktipp 6

Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) informierte am 24.11.2017 über ein interessantes Angebot: Über einen spielerischen Onlinetest können Unternehmen kostenfrei ihre DS-GVO Konformität überprüfen. Hintergrund der Sensibilisierungsaktion ist u. a., dass das BayLDA mit Anfragen zur DS-GVO überhäuft wird. Auf Basis der Online-Selbsteinschätzung wird Unternehmen die Möglichkeit gegeben, ihren aktuellen Datenschutzreifegrad bewerten zu lassen. Die Test-Ergebnisse inklusive Erläuterungen werden in Berichtsform zum Download bereitgestellt. Das perfekte Geschenk für die Geschäftsleitung, falls das Datenschutzbudget 2018 noch umstritten sein sollte...

Geschenktipp 7

Die CNIL (Commission Nationale de l'Informatique et des Libertés) hat neben den bereits veröffentlichten Leitfäden zur Durchführung von Datenschutz-Folgenabschätzungen nach Art. 35 DS-GVO nun ein Open-Source-Software-Tool bereitgestellt.

Das Tool führt anhand von Fragen mit Erläuterungen zu den erwarteten Antworten durch die Datenschutz-Folgenabschätzung eines Verfahrens und unterstützt deren Dokumentation. Die Erfassung ist gegliedert in die Verfahrenserfassung (Beschreibung der Verarbeitung), die Abfrage der Rechtsgrundlage und der Verhältnismäßigkeit, die ergriffenen Schutzmaßnahmen und die Bewertung der Risiken nach Eintrittswahrscheinlichkeit und Folgen für die Betroffenen. Als Risiken sind pauschal unbefugter Zugriff, unbefugte Veränderung und Datenverlust vorgegeben. Umfangreicher sind die vorgegebenen und anhand der Hinweise zu beschreibenden Schutzmaßnahmen.

Für Datenschutzbeauftragte, die nur vereinzelt Datenschutz-Folgenabschätzungen durchzuführen haben, kann diese mit dem Tool dokumentiert werden. Es bietet zudem eine gute Orientierung, wenn es auch nur wenige Anpassungen zulässt.

Secorvo News

Wie ich lernte, die Blockchain zu lieben.

Blockchain, die Technologie hinter der Kryptowährung Bitcoin, hat einen regelrechten Hype ausgelöst. Mit ihr können Transaktionen unveränderlich und für jedermann nachvollziehbar erfasst werden, und das ohne eine zentrale Vertrauensinstanz. Viele reagieren auf dieses Versprechen mit Begeisterung: So habe die Blockchain-Technologie noch ganz andere Anwendungen über elektronische Währungen hinaus: In der Musikindustrie ebenso wie zur Absicherung von Militärsystemen. Andere begegnen der Blockchain mit zurückhaltender Skepsis.

Dirk Achenbach erklärt auf dem Jahresstartevent der KA-IT-Si am **01.02.2018** die Blockchain aus kryptographischer Sicht – und stellt in seinem Vortrag dar, wie seine Skepsis der Begeisterung wich. Blockchain ist nämlich keine Universallösung, sondern eine Technologie, die spannende Fragen aufwirft. Im Anschluss haben Sie, wie gewohnt, Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking". Wegen der großen Nachfrage empfehlen wir eine baldige Anmeldung.

Who watches the watchmen?

Wie weit sind wir tatsächlich noch von einem Überwachungsstaat entfernt? Vorratsdatenspeicherung, Sammlung von Nutzungs- und Bewegungsprofilen durch Internet-Dienstleister, Massenüberwachung durch Nachrichtendienste – die Informationstechnik ist dabei, aus Verbrauchern „gläserne Bürger" zu machen. Doch was, wenn die Kontrolleure unkontrollierbar werden?

Als einer der Partner der IT-Sicherheitsregion Karlsruhe lädt die Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) zusammen mit dem ZAK | Zentrum für Angewandte Kulturwissenschaft und Studium Generale am **27.02.2018** wieder zum Filmevent in die Karlsruher Schauburg.

Bei der Abschlussveranstaltung der Traumfabrik #14/2017-18 „BIG BROTHER – Surveillance Cinema" wird der Film „THE CIRCLE" von James Ponsoldt gezeigt. Wolfgang Petroll wird in den Film einführen; im Anschluss folgt eine Diskussion mit Dr. Stefan Brink (Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg), Beate Bube (Präsidentin des Landesamtes für Verfassungsschutz Baden-Württemberg) und Thomas Rüttler (Leiter der Kriminalpolizeidirektion des Polizeipräsidiums Karlsruhe). Danach bieten wir Ihnen wie gewohnt die Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus http://www.veranstaltungen-it-sicherheit.de

Januar 2018	
19.-21.01.	ShmooCon 2018 (The Shmoo Group, Washington/US)
22.-24.01.	Omnisecure 2018 (in TIME berlin, Berlin)
28.-29.01.	AppSec California 2018 (OWASP Foundation, L.A./US)
Februar 2018	
01.02.	Wie ich lernte, die Blockchain zu lieben. (KA-IT-Si)
21.-22.02.	28. SIT-SmartCard Workshop (Fraunhofer-Institut SIT, Darmstadt)
27.02.	Who watches the Watchmen? (IT-Sicherheitsregion Karlsruhe)
27.-28.02.	25. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT Services GmbH, Hamburg)
März 2018	
12.-15.03.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
20.-22.03.	IT-Sicherheit heute - praxisnah, zielsicher, kompakt (Secorvo, Karlsruhe)
21.-23.03.	DFRWS EU Conference (DFRWS, Florenz/IT)

Impressum

http://www.secorvo-security-news.de

ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Dr. Volker Hammer, Hans-Joachim Knobloch, Michael Knopp, Sarah Niederer

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