secorvo
security consulting

Secorvo Security News

Januar 2022

Rechtsstaatsprinzip

Vor fünf Jahren hat das BVerfG in seinem Urteil zum NPD-Verbot die Prinzipien der freiheitlich-demokratischen Grundordnung präzisiert – die Wesenseigenschaften unserer politischen Ordnung, die uns von einer Diktatur unterscheiden. Darunter: die „Rechtsbindung der öffentlichen Gewalt" nach Art. 20 Abs. 3 GG. Polizei, Verwaltung und Regierung müssen sich an geltende Gesetze halten.

Zugegeben: Gesetze gibt es viele in Deutschland, und manche davon mögen mit heißer Nadel gestrickt sein. Doch das entbindet kein Organ der Exekutive von der im Grundgesetz verankerten Pflicht, sich daran zu halten. Damit ist es allerdings gelegentlich nicht weit her.

§ 28a Abs. 4 des Infektionsschutzgesetzes in der Fassung vom 18.11.2020 regelt den Umgang mit Corona-bedingt erhobenen Kontaktdaten unmissverständlich: „Eine Weitergabe der übermittelten Daten durch die zuständigen Stellen nach Satz 3 oder eine Weiterverwendung durch diese zu anderen Zwecken als der Kontaktnachverfolgung ist ausgeschlossen."

Am 07.01.2022 meldete der SWR, dass die Mainzer Polizei für Ermittlungen in einem Unfall mit Todesfolge vom Gesundheitsamt die Kontaktdaten von 21 Gästen einer Mainzer Gaststätte angefordert und (unter Vortäuschung einer Infektion durch das Gesundheitsamt) erhalten hat – aufgrund einer „fehlerhaften Bewertung des Infektionsschutzgesetzes". Weitere Fälle seien nicht bekannt.

Inzwischen schon. In über 100 Fällen haben Staatsanwaltschaft und Polizei Kontaktlisten oder Kontaktdaten der Luca-App ausgewertet, wie das ZDF am 20.01.2022 berichtete. Soweit bekannt.

Offenbar gibt es Strafverfolger, die der Überzeugung sind, dass es in ihrer Entscheidungshoheit liegt, an welche Gesetze sie sich halten müssen – und an welche nicht. Genau diese Haltung ist es, die einen funktionierenden Rechtsstaat schleichend zu einem Unrechtsstaat mutieren lässt.

Inhalt

secorvo
security consulting

Security News

Videokonferenzen sind Telekommunikation

Mit Inkrafttreten der am 07.05.2021 verabschiedeten TKG-Novelle am 01.12.2021 fallen nun auch nummernunabhängige interpersonelle Telekommunikationsdienste (§ 3 Nr. 40 TKG) unter das TKG. Dahinter verbergen sich Messenger- und Videokonferenzdienste wie Teams oder Zoom. Statt der Datenschutzaufsichtsbehörden ist nun die Bundesnetzagentur zuständige Aufsichtsbehörde. Wichtige Folge: Für Telekommunikationsdienste müssen keine Auftragsverarbeitungsverträge nach Art. 28 DSGVO geschlossen werden, denn die Kommunikation fällt unter das Telekommunikationsgeheimnis des Art. 10 GG. Die Grundsätze des Datenschutzes bleiben gültig und sind nach wie vor zu beachten; dennoch wird der Einsatz in Unternehmen dadurch wesentlich erleichtert.

Aus für Google Analytics?

Vor dem Hintergrund der Schrems II-Entscheidung des EuGH vom 16.07.2020 (C-311/18), nach der es für eine Übermittlung personenbezogener Daten in die USA entweder einer Einwilligung der Betroffenen oder eines Vertrags nach den aktuellen Standardvertragsklauseln der EU-Kommission sowie „zusätzlicher effektiver Maßnahmen" zur Herstellung eines gleichwertigen Schutzniveaus bedarf, entschied die österreichische Datenschutzbehörde (DSB) am 22.12.2021, dass die Datenübermittlung eines Webseitenbetreibers an Google mittels Google Analytics nicht mit der DSGVO vereinbar und somit illegal ist. Nach Ansicht der DSB verhindern die zusätzlichen Maßnahmen einen Zugriff der US-Behörden auf die übermittelten Daten nicht.

Zwar wurde weder entschieden, ob eine Anonymisierung der IP-Adressen eine Vereinbarung entbehrlich macht, noch, ob eine Übermittlung an Google Irland zulässig wäre. Die DSB weist jedoch darauf hin, dass eine IP-Adresse nur ein Teil des „digitalen Fußabdrucks" eines Nutzers sei.

Die Entscheidung kann als Indiz für die künftige Position der deutschen Aufsichtsbehörden gelten, zumal die europäischen Datenschutzbehörden bei diesem Thema offenbar in einer Task-Force zusammenarbeiten. Solange Google keine tiefgreifenden Änderungen an Google Analytics vornimmt, ist Betreibern von Webseiten ein Wechsel zu europäischen Anbietern zu empfehlen.

Ransomware-Prävention

Am 30.11.2021 hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) ein anlassloses Prüfverfahren zur Ransomware-Prävention gestartet. Die Fragen der Aufsichtsbehörde zielen auf die in den geprüften Einrichtungen getroffenen Schutzmaßnahmen vor Ransomware-Angriffen. Der Fragebogen, die Handreichung und ein Informationsblatt des BayLDA ist auch für nicht betroffene Unternehmen eine gute Orientierung hinsichtlich der zu treffenden Mindestschutzmaßnahmen.

MFA wird Standard

Für Kunden von Salesforce wird ab dem 01.02.2022 die Multi-Faktor-Authentifizierung (MFA) zum Standard. Eine begrüßenswerte Maßnahme, gilt doch eine Kennwort-Authentifikation bei Cloud-Diensten als Schwachstelle. Zwar schützt eine MFA nicht vor allen Angriffen, aber eine solche Vorgabe (vgl. SSN 09+10/2021) verbessert die Sicherheit signifikant.

Bei der Wahl der Authenticator App sollte der Fokus auf Benutzerfreundlichkeit, Sicherheit und Datenschutzaspekten liegen. So sollte die App für mehrere Dienste nutzbar sein und die Authentifizierungsdaten ausreichend geschützt speichern.

Koalitionsvorhaben

Informationssicherheit und Datenschutz misst die neue Bundesregierung nach dem am 07.12.2021 unterzeichneten Koalitionsvertrag erhebliches Gewicht bei: Im Abschnitt „Digitale Bürgerrechte und IT-Sicherheit" werden ein „Recht auf Verschlüsselung" und ein „wirksames Schwachstellenmanagement" gefordert. Außerdem sollen Hersteller für Schäden durch fahrlässige IT-Sicherheitslücken in ihren Produkten haften. Staatliche Stellen sollen verpflichtet werden, „ihnen bekannte Sicherheitslücken beim BSI zu melden" und ihre IT-Systeme regelmäßig einer externen Prüfung zu unterziehen. Dem staatlichen Ankauf von Sicherheitslücken erteilt die Koalition eine klare Absage, und im Bundespolizeigesetz soll es keine Ermächtigung mehr zu Quellen-TKÜ und Onlinedurchsuchung geben.

Zum Datenschutz plant die Regierung einen weiteren Anlauf für ein Beschäftigtendatenschutzgesetz (inzwischen ein „running gag"), will in einem „ambitionierten Abkommen" mit den USA wieder datenschutzkonforme Datenübermittlungen auf europäischem Schutzniveau ermöglichen und die schon totgesagte E-Privacy-Verordnung wiederbeleben.

Orientierung im Einwilligungs-Dschungel

§ 25 des kürzlich in Kraft getretenen Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) regelt die Anforderungen an Einwilligungen. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (DSK) hat daraufhin am 20.12.2021 eine

neue Version ihrer Orientierungshilfe für Anbieter:innen von Telemedien veröffentlicht. Darin weist sie ausdrücklich darauf hin, dass nicht nur Cookies, sondern alle Tracking-Technologien einwilligungsbedürftig sind. Wichtig ist auch die Unterscheidung zwischen der Einwilligung nach DSGVO und TTDSG, da es für letztere eben nicht auf den Personenbezug ankommt.

Hinsichtlich der Einwilligungsverwaltung für Cookies zeigt der aktuelle Beschluss des VG Wiesbaden vom 01.12.2021, dass die Aufklärung bei Aufruf einer Webseite transparent erfolgen und zu dem passen muss, was im Hintergrund abläuft. Werden Funktionen bspw. zur Anzeige von Informationen verwendet, die eine Verbindung mit Servern im Nicht-EU-Ausland herstellen, muss die Einwilligung hierfür vor deren Ausführung eingeholt werden.

Datenschutz-Zertifizierungen

Bis zum Inkrafttreten der DSGVO waren das Gütesiegel und das Audit des Unabhängigen Landeszentrums für Datenschutz in Schleswig Holstein (ULD) die bekanntesten Datenschutzzertifizierungen. Mit Art. 42 und 43 DSGVO wurden datenschutzspezifische Zertifizierungsverfahren und Datenschutzprüfzeichen zum Nachweis der DSGVO-Konformität bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern eingeführt.

Nach der in der DSGVO gewählten Formulierung können Datenschutz-Produkte, -Prozesse oder -Dienstleistungen zertifiziert werden, nicht jedoch Datenschutz-Managementsysteme, obwohl diese Systeme oft Grundlage für datenschutzgerechte Produkte sind. Der größte Bedarf an Zertifizierungen liegt sicherlich in der Zertifizierung von Auftragsverarbeitungen.

Als europaweit gemeinsame Grundlage für die Akkreditierung von Zertifizierungsstellen nach Art. 43 DSGVO hatte der Europäische Datenschutzausschuss im Dezember 2018 Leitlinien veröffentlicht. Daran anknüpfend haben die deutschen Datenschutzaufsichtsbehörden und die Deutsche Akkreditierungsstelle (DAkkS) einen Akkreditierungsprozess erarbeitet, der der DIN EN ISO/IEC 17065 und den ergänzenden Anforderungen der Datenschutzkonferenz folgt. Für in Deutschland tätige Zertifizierungsstellen wird die Akkreditierung durch die DAkkS zusammen mit der zuständigen Datenschutzaufsichtsbehörde erteilt.

Das von der DAkkS in einem Merkblatt veröffentlichte Musterzertifikat und die Ankündigungen verschiedener Datenschutzaufsichtsbehörden wie dem ULD lassen erwarten, dass es im Laufe des Jahres erste Datenschutz-Zertifizierungen geben wird.

Gefragter Staat

Beim Onlinekongress 2021 des Chaos Computer Club (CCC) stellte ReclaimYourFace das Ergebnis von 195 Anfragen zu Videoüberwachung im öffentlichen Raum vor, die sie über Fragdenstaat.de (auf Grundlage des Informationsfreiheitsgesetzes des Bundes und mehrerer Länder) an Polizeibehörden, Innenministerien und Datenschutzbehörden gesendet hatten. Nur auf 70 Anfragen erfolgte überhaupt eine Reaktion. 13 Angefragte lehnten eine Auskunft ab, 31 Anfragen wurden weiterverwiesen oder waren ergebnislos. Nur auf 26 Anfragen (13%) wurden Informationen herausgegeben, teilweise sehr ausführlich. In einigen Bundesländern wurden jedoch hohe Gebühren verlangt, zog sich der Vorgang über mehrere Monate hin oder kam erst auf Intervention von Datenschutzbeauftragten ins Rollen.

Kein besonders rühmliches Bild.

Secorvo News

T.I.S.P. und IT Security Insights

Wir hoffen, die nächsten Seminare wieder wie geplant in unseren Räumen in Karlsruhe durchführen zu können – das Zertifizierungsseminar T.I.S.P. (**07.–11.03.2022**) und das T.I.S.P.-Update-Seminar IT Security Insights (**15.–17.03.2022**) – und freuen uns auf Ihre Anmeldung.

Willkommen bei den Quanten

Der amerikanische Forscher Peter Shor schockte 1997 die Welt mit der Publikation eines Algorithmus', mit dem die Zerlegung sehr großer Zahlen in ihre Primfaktoren auf Quantencomputern in polynomieller Zeit gelingt – damit könnte man die wichtigsten der heute verwendeten asymmetrischen Kryptoverfahren brechen. Wie aber funktionieren Quantencomputer eigentlich? Warum lässt sich mit ihnen das „Faktorisierungsproblem" lösen? Sind auch symmetrische Verfahren wie der AES gefährdet? Bis wann müssen wir Ersatzverfahren verfügbar haben? Worauf sollten wir schon heute achten?

Um diese und weitere Fragen rund um Quantencomputer dreht sich das Expertengespräch von Professor Dr. Müller-Quade (KASTEL), Oliver Winzenried (WIBU-SYSTEMS) und Dirk Fox (Secorvo Security Consulting) auf dem Jahresstartevent der KA-IT-Si am **03.02.2022**. Die limitierten Präsenzplätze im jüngst eröffneten IT Security Club des „House of IT Security" der Karlsruher WIBU Systems sind bereits ausgebucht, aber Sie können das Expertengespräch per Livestream miterleben (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2022	
01.-02.02.	18. Deutscher IT-Sicherheitskongress (BSI, virtuell)
03.02.	KA-IT-Si-Event „Willkommen bei den Quanten“ (KA-IT-Si, hybrid)
02.-04.02.	29. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
März 2022	
07.-11.03.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
15.-17.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, virtuell)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)
April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Nicolas Blum, Milan Burgdorf, André Domnick, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

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

secorvo
security consulting

Secorvo Security News

Februar 2022

Zutatenverzeichnis

Ende des kommenden Jahres feiert die Regelung ihren 40. Geburtstag: Seit dem 26.12.1983 kennt das deutsche Lebensmittelrecht die Pflicht, jedem Produkt auf der Verpackung eine Zutatenliste in absteigender Reihenfolge der Zugabemenge beizufügen. Dank dieser Transparenz kennen Verbraucher seitdem die Bestandteile ihrer Nahrungsmittel und können somit Unverträglichkeiten vermeiden und die Qualität angebotener Lebensmittel einschätzen. Das ist sicherlich eine der wichtigsten Regelungen des Lebensmittelrechts, die zweifellos bereits viele Menschen mit schweren Allergien das Leben gerettet hat.

Leider sind wir in der Informationstechnik von einer solchen Offenheit weit entfernt. Dabei mixt inzwischen jeder Softwareentwickler unzählige Bibliotheken und Codefragmente beliebiger Provenienz in „seine" Programme – dank Cloud-Services, Open Source und offenen APIs mit steigender Tendenz. Kaum eine Entwicklungsumgebung, die ohne eigene Bibliotheksfunktionen daherkommt, kaum ein Softwareprodukt, das keinen Open Source-Code unter seiner Haube verbirgt. Letzteres unterliegt zwar klaren Offenlegungsregeln, die aber bei weitem nicht von jedem Hersteller beachtet werden.

Das Ergebnis dieser wachsenden Code-Mehrfachnutzung kann ein erheblicher Risikoanstieg sein: Wird ein Sicherheits-Bug in einer der verwendeten Bibliotheken oder Open-Source-Code-Basen bekannt, erfahren Nutzer davon nur, wenn der Hersteller sie warnt und Patches liefert. Das setzt allerdings voraus, dass der Hersteller die verwendeten Code-Teile sauber dokumentiert – und auch seine „Code-Zulieferer" dasselbe bei ihrem Programmcode tun.

Verlass ist darauf keineswegs: Wird ein Bug bekannt, geht die Suche los – und die Schwachstelle wird in einigen Anwendungen erst nach Wochen gefixt. Wäre der Hersteller zur Dokumentation seiner Code-Zutaten verpflichtet, könnte der Käufer das diesbezügliche Risiko schon vor dem Erwerb einschätzen.

Inhalt

secorvo
security consulting

Security News

TCF nicht DSGVO-konform

Die belgische Datenschutzbehörde (APD) hat am 02.02.2022 entschieden, dass das Transparency and Consent Framework (TCF) der IAB Europe gegen die DSGVO verstößt. Das TCF ordnet mittels eines sogenannten TC-Strings und eines Consent-Cookies das Verhalten des Nutzers dessen IP-Adresse zu und ermöglicht die Versteigerung zielgruppenspezifischer Werbeplätze. Nach Ansicht der ADP mangelt es dabei an einer Rechtsgrundlage, transparenten Informationen sowie ausreichenden technischen und organisatorischen Maßnahmen. IAB Europe sei zudem ihren Pflichten als Verantwortliche nicht nachgekommen. IAB will die Entscheidung rechtlich prüfen, zeigt sich aber optimistisch, dass die Verstöße behoben werden können. Sollte IAB nicht nachbessern, bleibt möglicherweise das RTB-Protokoll von Google als einzige technische Alternative.

Die Entscheidung gilt nach dem „one-stop-shop"-Prinzip für die gesamte Europäische Union und dürfte sich erheblich auf die digitale Werbewirtschaft auswirken.

Nun auch Frankreich „ohne"

Nach der österreichischen Datenschutzbehörde (siehe SSN 01/2022) untersagte am 10.02.2022 auch die französische Datenschutzbehörde CNIL Webseiten-Betreibern die Nutzung von Google Analytics. Zur Begründung führt die CNIL aus, dass die von Google getroffenen Maßnahmen nicht ausreichten, um das fehlende Schutzniveau in den USA auszugleichen und daher Art. 44 DSGVO verletzt sei. Betreibern empfiehlt sie, Dienste zu verwenden, die nur anonyme statistische Daten produzieren, um die sonst notwendige Einwilligung zu vermeiden. Zudem kündigte sie ein Evaluierungsprogramm an, mit dem festgestellt werden soll, welche Lösungen von der Einwilligungspflicht ausgenommen sind.

Da die für Google Europa zuständige Datenschutz-Aufsichtsbehörde in Irland nicht aktiv wird, treibt derzeit die Schrems-Initiative noyb mit Beschwerden alle anderen europäischen Aufsichtsbehörden in Sachen Google Analytics vor sich her. Eine Entscheidung der deutschen Datenschutzaufsicht ist wohl nur noch eine Frage der Zeit. Daher empfehlen wir dringend einen Wechsel zu europäischen Anbietern – oder eine effektive Anonymisierung.

IT-GSK 2022 in XML

Am 08.02.2022 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das IT-Grundschutz-kompendium in der Version 2022 veröffentlicht. Wie jedes Jahr finden sich im neuen Kompendium redaktionelle und inhaltliche Änderungen sowie Ergänzungen, darunter vor allem neue Bausteine zur „Containerisierung" und Fernwartung. Eine wichtige Neuerung ist, dass das BSI das Kompendium nun nicht mehr nur in traditionellen „Lese-Formaten" wie PDF bereitstellt, sondern mit der Veröffentlichung als DocBook-XML-Version Anwendern die Möglichkeit gibt, recht einfach mit eigenen Tools den operativen Umgang mit den Bausteinen zu verbessern.

Patches erscheinen früher

Am 10.02.2022 wurden in Googles Project Zero Blog einige interessante Statistiken über die Behebung von gemeldeten Schwachstellen durch Herstellerpatches veröffentlicht. Während 2018 noch durchschnittlich 90 Tage von der Meldung bis zur Behebung einer Schwachstelle verstrichen, waren es 2021 im Schnitt nur noch 52 Tage. Diese deutlich beschleunigte Bereitstellung von Patches ist sehr zu begrüßen, sie hilft jedoch nur, wenn die Patches auch zügig eingespielt werden.

Wir empfehlen: Patchen Sie so schnell wie möglich – und sehen Sie Methoden zur Zurückführung auf einen stabilen Betriebszustand sowie Ersatzmaßnahmen vor, falls es zu Störungen kommt. Verzögerungen durch ausgiebige Tests der Patches sollte man nach Möglichkeit vermeiden – das Risiko eines Angriffs ist inzwischen größer als das eines durch einen Patch verursachten Ausfalls. Schließlich drohen bei verspätetem oder unterlassenem Patchen Datenschutz-Bußgelder (vgl. SSN 11/2021).

US-Überwachungsrecht begutachtet

Die Datenschutzkonferenz (DSK) hat am 25.01.2022 ein Gutachten von Stephen I. Vladeck zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse veröffentlicht. Das Gutachten zeigt detailliert die Anwendungsbereiche der einzelnen amerikanischen Gesetze und die theoretisch möglichen Rechtsbehelfe auf, was insbesondere für Transfer Impact Assessments (TIA) bei Datenübermittlungen in die USA relevant sein dürfte. Laut DSK sind wesentliche Befunde, dass die Anwendbarkeit der bereits im Schrems-II-Urteil behandelten Section 702 FISA sehr weit ist und dass die Aspekte Extraterritorialität und Rechtsschutzmöglichkeiten behandelt werden. Diese knappen Ausführungen der DSK werden dem Detailgrad des Gutachtens ebenso wenig gerecht, wie die teilweise verbesserungsbedürftige deutsche Übersetzung.

Die Datenschutz-Aufsichtsbehörden bewerten derzeit die Konsequenzen aus dem Gutachten. Eine ist zweifellos, dass bei Übermittlungen in die USA immer an ein TIA gedacht werden muss.

CDN und Datenschutz

Ein Content Delivery Network (CDN) hostet Kopien von Webseiten, um deren Laden zu beschleunigen. Der Nutzung stehen jedoch erhebliche datenschutzrechtliche Bedenken entgegen, da ein Hosting auf global verteilten Servern unweigerlich zur Problematik der Zulässigkeit einer Drittlandsübermittlung nach Art. 44 ff. DSGVO führt, wenn über das CDN personenbezogene Daten wie IP-Adressen übermittelt werden.

Insbesondere amerikanischen Anbietern fehlt in der Regel ein angemessenes Datenschutzniveau. So entschied am 01.12.2021 das VG Wiesbaden, dass ein Cookie-Dienst, der für das Abrufen eines Einwilligungsskripts auf das CDN einer US-Firma zurückgreift, wegen fehlender Einwilligung rechtswidrig sei. Eine Information in der Datenschutzerklärung genügt nicht.

Pfeift, gepfiffen, verpfiffen

Bis 17.12.2021 hätte die EU-Richtlinie 2019/1937, besser bekannt als „Whistleblower-Richtlinie", in deutsches Recht umgesetzt werden müssen. Dies ist bisher nicht erfolgt, und wann die neue Bundesregierung die Umsetzung angeht, ist nicht bekannt.

Die Regelungen betreffen Meldungen von Verstößen gegen ausgewählte Bestimmungen des EU-Rechts; sie richten sich sowohl an Unternehmen als auch an den öffentlichen Sektor. Bemerkenswert ist, dass eine von einem Hinweis betroffene Person im Vergleich zum Hinweisgeber eher dürftig geschützt wird. Zwar legt Art. 22 fest, dass deren Identität während der Untersuchung geschützt und selbstverständliche Rechte wie der Anspruch auf wirksame Rechtsbehelfe und ein faires Gerichtsverfahren gewährt werden sollen. Allerdings trägt die betroffene Person die Beweislast dafür, dass erteilte Hinweise falsch sind. Der Hinweisgeber soll bei Falschinformationen nur dann sanktioniert werden, wenn er von der Unrichtigkeit wusste. Immerhin weist Art. 16 Abs. 2 darauf hin, dass der Hinweisgeber gegenüber der betroffenen Person offengelegt werden muss, damit diese von ihren Verteidigungsrechten Gebrauch machen kann.

Secorvo News

Verstärkung im Datenschutz

Wir freuen uns über eine erneute Verstärkung unseres Datenschutz-Teams: Im Februar konnten wir den Volljuristen Christian Blaicher für das Secorvo-Team gewinnen. Herzlich willkommen!

Secorvo Seminare

Ab März finden unsere Präsenz-Seminare nach mehrmonatiger Pause endlich wieder statt. Freie Plätze gibt es noch auf unserem viertägigen PKI-Seminar (**25.–28.04.2022**). Wir freuen uns auf Ihre Teilnahme!

Lesen bildet II

Wir laden Sie herzlich zu unserem zweiten „Literarischen KA-IT-Si-Kabinett" am **10.03.2022** ein. An diesem Abend werden wir Ihnen weitere Werke der (Welt-)Literatur vorstellen, die sich mit dem Thema Datenschutz oder Datensicherheit beschäftigen und die Sicherheits- und Datenschutzexperten daher gelesen haben „müssen". Dabei freuen wir uns nicht nur auf Ihre Anmeldung, sondern auch über Ihre persönliche Rückmeldung: Welche weiteren Bücher gehören Ihrer Ansicht nach unbedingt auf diese „Liste"?

Expertengespräch verpasst?

Sie haben die Jahresauftaktveranstaltung „Willkommen bei den Quanten" der KA-IT-Si am 03.02.2022 verpasst oder möchten sich das Expertengespräch zur Bedrohung heutiger Kryptosysteme durch Quantencomputer noch einmal ansehen? Wir haben die Veranstaltung aufgezeichnet und auf unserem YouTube-Kanal veröffentlicht. Im Gespräch diskutieren Professor Dr. Müller-Quade (KASTEL), Oliver Winzenried (WIBU-SYSTEMS) und Dirk Fox (Secorvo Security Consulting) darüber, wie ernst die Bedrohung durch Quantencomputer genommen werden muss und was das für Hersteller und Anwender kryptografischer Systeme bedeutet.

Geld oder Leben

Wie erpressbar sind deutsche Unternehmen und Institutionen? Wer bei einem gezielten Hacker-Angriff seine gesamten Daten verliert und auf einen Schlag ohne IT-Dienste dasteht, wird geneigt sein, nahezu jeden Preis für die Wiederherstellung seiner Infrastruktur zu zahlen. Ein Unternehmen, das genau das nicht getan hat, ist das in Baden-Württemberg ansässige Familienunternehmen Pilz. Die Unternehmensleitung hat sich 2019 trotz eines Totalausfalls der gesamten IT dagegen entschieden, den Kriminellen Lösegeld zu zahlen – und ist durch eine harte Zeit gegangen.

Was Pilz aus diesem einschneidenden Erlebnis gelernt hat und anderen Unternehmen und Unternehmern mitgeben möchte, wird Herr Thomas Pilz, geschäftsführender Gesellschafter der Pilz GmbH & Co. KG, auf dem KA-IT-Si-Event am **07.04.2022** vorstellen. Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2022	
07.-11.03.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.03.	KA-IT-Si-Event „Lesen bildet II“ (KA-IT-Si, virtuell)
23.03.	31. ID:SMART Workshop (Fraunhofer SIT, virtuell)
24.-26.03.	ShmooCon 2022 (The Schmoo Group, Washington/US)
25.03.	Datenschutztag 2022 (COMPUTAS, Köln)
28.-31.03.	DFRWS EU 2022 (DFRWS, hybrid)
29.-31.03.	secIT 2022 (Heise Medien, Hannover)
April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)
Mai 2022	
03.-04.05.	Security Forum 2022 (Hagenberger Kreis, Hagenberg/AT)
05.05.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
09.-13.05.	T.I.S.P. - TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Nicolas Blum, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

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

secorvo
security consulting

Secorvo Security News

März 2022

Warnung

Am 15.03.2022 veröffentlichte das BSI eine Warnung vor dem Einsatz von Kaspersky-Virenschutzprodukten – und löste damit in den IT-Abteilungen vieler Unternehmen und Behörden hektische Betriebsamkeit aus.

Natürlich stimmt das Argument, dass die hohen lokalen Berechtigungen eines Virenschutzprodukts, das zudem regelmäßig große Datenmengen (Signaturdateien) nachlädt, sich für einen (nachrichtendienstlichen) IT-Angriff geradezu anbieten. Nur: Kein Geheimdienst der Welt, der einen solchen Angriff plant, würde damit wochenlang warten – vor „Cyberattacken" aus Russland hatte das BSI bereits im Februar gewarnt.

Die Empfehlung, Kaspersky-Produkte zu ersetzen, greift damit viel zu kurz. Wer solche Angriffe befürchtet, sollte sofort seine gesamte Infrastruktur analysieren – denn wenn sie geplant waren, muss man davon ausgehen, dass bereits Schadsoftware auf diesem Weg installiert wurde. Davon ist in der BSI-Warnung jedoch nichts zu lesen.

Auch ist unverständlich, warum sich die Warnung auf Kaspersky-Produkte beschränkt. Alle relevanten Geheimdienste der Welt bauen seit Jahr(zehnt)en Cybercrime-Abteilungen auf – und warten für ihre Attacken nicht auf einen begleitenden physischen Krieg. Neben Russland sind auch China, Israel und die USA sowohl technisch in der Lage als auch gesetzlich autorisiert, solche Angriffe in „Friedenszeiten" durchzuführen. Wer Kaspersky verbannt, darf auch keine Checkpoint-Firewalls, Huawei-Smartphones, Lenovo-Laptops, Intel-Prozessoren und Cisco-Router einsetzen – und sollte besser auf die Nutzung von Microsoft-Programmen, Apple-Apps und Google-Diensten verzichten.

Nicht möglich, sagen Sie? Richtig. Daher kommt es darauf an, bei der Angriffserkennung seine Hausaufgaben zu machen – damit man im Falle eines solchen Falles wenigstens zügig reagieren kann.

Inhalt

secorvo
security consulting

Security News

Behördliche Unterstützung

Am 24.02.2022 veröffentlichte das BSI einen „Maßnahmenkatalog Ransomware“, in dem eine Vielzahl von ineinander greifenden Schutzmaßnahmen beschrieben wird. Das erste Kapitel enthält eine Checkliste mit konkreten Prüfpunkten zur Selbsteinschätzung und Beispiele, wie die Anforderungen des Maßnahmenkatalogs zu erfüllen sind.

Das ist wahrscheinlich hilfreich. Wie Behörden aber nicht nur Dokumente erzeugen, sondern auch konkrete Unterstützungsdienste erbringen können, zeigt die amerikanische Cybersecurity & Infrastructure Security Agency (CISA): Sie bietet Organisationen und Regierungseinrichtungen eine Reihe von kostenfreien Services zum Schutz vor Angriffen. So kann man über das Internet erreichbare Netzbereiche und Webanwendungen einer automatisierten Überprüfung auf typische Schwachstellen unterziehen lassen oder mit dem auf GitHub zum Download bereitgestellten Cyber Security Evaluation Toll (CSET) ein Ransomware Readiness (Self-) Assessment (RRA) durchführen (siehe SSN 7/2021). Diese Angebote ersetzen keinen Penetrationstest, sind aber eine einfache Maßnahme, um offensichtliche Mängel zu identifizieren und abzustellen – und damit ein wichtiger Beitrag zu einer wirkungsvollen Prävention.

Interessenskonflikte des DSB

Am 16.12.2021 verhängte die belgische Datenschutzbehörde aufgrund eines Interessenskonflikts des Datenschutzbeauftragten einer Bank ein Bußgeld von 75.000 €. Der interne Datenschutzbeauftragte war zugleich Leiter von drei Abteilungen, die das operative Risikomanagement, das Informationsrisikomanagement sowie eine Sonderermittlungsstelle umfassten. In seiner Funktion sei er nicht nur beratend oder überwachend tätig geworden, sondern habe aufgrund seiner Befugnisse über die Verarbeitung personenbezogener Daten entscheiden können. Nach Auffassung der belgischen Behörde darf ein Datenschutzbeauftragter keine Position innehaben, die Mittel und Zweck der Verarbeitung von personenbezogenen Daten festlegen kann.

Interessenskonflikte können durch eine sorgfältige Zuweisung von Aufgaben und vertragliche Regelungen vermieden werden. Sobald sich ein Datenschutzbeauftragter selbst überwachen müsste, sind Interessenskonflikte unvermeidbar. Die Entscheidung der belgischen Behörde ist daher nicht überraschend und sollte zum Anlass genommen werden, die sonstigen Aufgaben und Befugnisse des internen Datenschutzbeauftragten zu überprüfen.

Kali Linux 2022

Pünktlich zum Valentinstag kündigte Kali das neue Release „Kali Linux 2022.1“ an. Neben visuellen Änderungen wie einheitlichen BIOS/UEFI Boot-Menus und „professionelleren“ Shell-Prompts ziehen neue Tools in die offiziellen Repositories ein – eine umfangreiche Ergänzung zum bisherigen Toolset und eine Alternative zu gängigen Tools in den Bereichen OSINT, Port- und Schwachstellenscannern sowie Proxies. Zusätzlich wurde das „Kali Everything Image“ als optionaler Download eingeführt, ein Komplettpaket mit allen möglichen vorinstallierten Tools. Für bestimmte Situationen ist dieses Angebot sicherlich nützlich – auch die Hacking-Distribution BlackArch Linux bietet seit 2020 ein derartiges Komplettpaket an. Mit rund der Hälfte der Download-Größe (ca. 9.4 GB) ist das „Kali Everything Image“ eine zumindest platzsparende Alternative zum „Black Arch Full ISO“ (ca. 18 GB).

Data-Act-Entwurf

Die Europäische Kommission hat am 23.02.2022 einen Vorschlag zur Data-Act-Verordnung vorgelegt. Die Verordnung ist Teil einer groß angelegten Datenstrategie der Europäischen Union, die unter Wahrung von Datenschutzstandards und Verbraucherrechten die branchenübergreifende Nutzung von Daten fördern und die Vormachtstellung großer Konzerne zugunsten von KMUs und vor allem der Nutzer eindämmen soll.

Der Data Act ist bei der Verarbeitung personenbezogener Daten neben der DSGVO anwendbar, sodass Betroffene ihre Rechte aus beiden Verordnungen geltend machen können. Dabei sind die Rechte aus dem Data Act umfassender als die der DSGVO, da Daten nicht nur einmalig, sondern kontinuierlich in Echtzeit zur Verfügung gestellt werden sollen.

Die Zielsetzung des Entwurfs darf als gelungen, die Umsetzung muss aber als nicht ausreichend bewertet werden. Die Regelung des behördlichen Zugriffs ist schwammig und wird als rechtsstaatlich problematisch und als intensiver Eingriff in die Vertragsfreiheit sowie als eine Gefährdung der Wettbewerbsfähigkeit europäischer Unternehmen kritisiert. Auch wenn der Entwurf nachgebessert werden sollte, ist bereits jetzt erkennbar, dass die Auswirkungen der Verordnung auf die Wirtschaft in jedem Fall erheblich sein werden.

#airtagged

Seit dem 30.04.2021 verkauft Apple münzgroße Anhänger („AirTags"), die von Apple-Geräten im Umkreis von 10-50 m via Bluetooth und vom iPhone 11+ auf wenige cm genau geortet werden können. Das funktioniert über beliebige Distanzen weltweit: Entdeckt ein iPhone ein fremdes AirTag, schickt es die Geo-Koordinaten in die iCloud, wo sein Besitzer mit Apples „Find My"-App die Bewegung des AirTags auf einer Karte verfolgen kann. Die Idee ist bestechend: Einfach einen der rund 25 € teuren Anhänger am Hundehalsband, unter dem E-Bike-Sattel oder am Schlüsselbund befestigen, und Suchen ist Finden. Offenbar billigend in Kauf genommen hat Apple, dass sich damit auch fremde Habseligkeiten „markieren" lassen. So wurde z. B. am 15.12.2021 über AirTags berichtet, die an neuen Autos angebracht werden, um sie unbemerkt zu verfolgen – und einen guten Ort für einen Diebstahl abzupassen. Dass AirTags, in einer fremden Hand- oder Jackentasche versenkt, auch zu einem wertvollen Werkzeug für Stalker werden, ist inzwischen ebenfalls bekannt. Unterstützt wird der Missbrauch dadurch, dass die Identifikation des Eigners zu dessen Schutz technisch verhindert wird.

Zwar meldet sich ein AirTag mit einem Ton, wenn es acht bis 24 Stunden keinen Kontakt zum iPhone seines Besitzers hatte – aber das kann überhört oder mit einer einfachen Bohrung ausgeschaltet werden – auch werden inzwischen „Silent AirTags" mit deaktiviertem Lautsprecher angeboten. Die von Apple publizierte App zur Feststellung von längere Zeit in der Nähe befindlichen fremden AirTags warnt nach mehreren Stunden – befindet sich das „Opfer" aber mit Unterbrechungen in der Nähe des AirTags oder besitzt es kein iPhone, funktioniert der Alarm nicht. Offenbar fällt dieser Missbrauch sogar in eine „Strafbarkeitslücke", wie Lena Leffer und Michelle Weber in der DuD 3/2022 nachweisen.

Am 21.02.2022 veröffentlichte Fabian Bräunlein den Code für einen „Stealth AirTag Clone" auf Basis eines ESP32, der alle Schutzfunktionen des „Find My"-Protokolls von Apple umgeht. Und er macht klar, dass nicht die AirTags das eigentliche Problem sind – sondern die Tracking-Infrastruktur, die Apple mit dem „Find My"-Netzwerk schon vor Jahren etabliert hat.

Signatur als werbefreie Zone

Am 15.09.2021 befand das Kammergericht Berlin den Zusatz in der E-Mail-Signatur eines Unternehmens „[...] Organisiert, denkt mit, erledigt. Nutzen Sie www.[...].de" als unerlaubte Werbung im Sinne des § 7 UWG und gestand dem Kläger einen Unterlassungsanspruch gegen das Unternehmen zu. Der geringe Umfang dieses Zweizeilers und die Positionierung am Ende der Nachricht seien hier unerheblich: „Nach der Rechtsprechung des BGH" könne dieser kleine Zusatz auch nicht durch den vorangestellten, legitimen Inhalt der E-Mail gerechtfertigt werden. Auch diese sehr geringfügige Beeinträchtigung sei generalpräventiv zu untersagen, um ein Um-sich-Greifen solcher Werbung durch Nachahmung zu verhindern.

In welchem Maß und Format Hinweise auf das eigene Unternehmen in der E-Mail-Signatur überhaupt zulässig sind, dazu bietet das rechtskräftige Urteil leider keine Anhaltspunkte. Immerhin sprach das Gericht der Sache eine „grundsätzliche Bedeutung" zu, d. h. das Gericht sieht eine endgültige Klärung durch den Bundesgerichtshof für zumindest wünschenswert an. Bis dahin sollten E-Mail-Signaturen kritisch auf eine mögliche Werbewirkung überprüft werden.

Secorvo News

BSI Vorfall-Experte

Die „Einschläge kommen näher" – daher gewinnt die Vorbereitung auf einen Sicherheitsvorfall als Teil des Sicherheitsmanagements an Bedeutung. Seit dem vergangenen Jahr bietet das BSI eine Zertifizierung zum „Vorfall-Experten" an. Voraussetzung ist die Teilnahme an einer Aufbau-Schulung auf der Grundlage des Leitfadens des BSI zur Reaktion auf IT-Sicherheitsvorfälle.

Die dreitägige Aufbauschulung zum BSI Vorfall-Experten bietet Secorvo erstmals vom **17. bis 19.05.2022** an. Wir freuen uns auf Ihre Anmeldung – natürlich auch zum PKI-Seminar (**25.–28.04.2022**) oder dem Vorbereitungsseminar auf die T.I.S.P.-Zertifizierung (**09.–13.05.2022**).

Wer besitzt mein Smartphone?

Auch wenn wir uns kaum noch daran erinnern können, wie wir ohne sie klarkamen: Smartphones gibt es erst seit 15 Jahren. Genauso alt wie das Smartphone ist die Geschichte der Smartphone Hacks – von den ersten Jailbreaks über die Celebrity Nudes bis hin zu kommerzieller und staatlicher Spyware.

Anhand von Attack Trees und Live-Hacking-Demos zeigen Ihnen Armin Harbrecht und Maximilian Stauß (aramido) beim kommenden KA-IT-Si-Event am **19.05.2022**, wie Smartphones angegriffen werden. Dieses Verständnis ist Voraussetzung für effektive Schutzmaßnahmen. Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" – bei schönem Wetter auf der herrlichen Dachterrasse von aramido (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

April 2022	
05.-08.04.	GI Sicherheit 2022 (KIT, Karlsruhe)
07.04.	„Geld oder Leben“ (KA-IT-Si, Karlsruhe)
25.-28.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-27.04.	Datenschutztage 2022 (FFD, hybrid)
Mai 2022	
03.-04.05.	Security Forum 2022 (Hagenberger Kreis, Hagenberg/AT)
05.05.	Anwendertag IT-Forensik (Fraunhofer SIT, Darmstadt)
09.-13.05.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
10.-13.05.	Blackhat Asia 2022 (Blackhat, hybrid)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)
10.-11.05.	BvD Verbandstage 2022 (BvD, Berlin)
16.-17.05.	23. Datenschutzkongress (EUROFORUM, Berlin)
16.-18.05.	Entwicklertag 2022 (VKSI, GI, ObjektForum, Karlsruhe)
17.-19.05.	BSI Vorfall-Experte – Aufbauschulung (Secorvo, Karlsruhe)
19.05.	„Wer besitzt mein Smartphone?“ (KA-IT-Si, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), Christian Blaicher, Nicolas Blum, Milan Burgdorf, Enes Erdoğan, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende, Jochen Schlichting, Nils Wiedemann

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

secorvo
security consulting

Secorvo Security News

April 2022

Cyber, Cyber, Cyberagentur

Mit der von der Bundesregierung 2020 gegründeten „Agentur für Innovation in der Cybersicherheit“ soll Deutschland „bei der Cybersicherheit im internationalen Vergleich die Führung, zumindest eine Spitzenposition übernehmen.“ Um das zu erreichen, soll sie Forschung und bahnbrechende Innovationen im Bereich der Cybersicherheit vorantreiben (Strategie 2022-2025). Bis 2023 stehen ihr dafür zunächst 280 Mio. € Steuergeld zur Verfügung. Wem hilft das? Seit 1991 gibt es das BSI mit inzwischen über 1.300 Mitarbeitern (Jahresetat 200 Mio. €), es forschen das Horst-Görtz-Institut für IT-Sicherheit in Bochum, das Helmholtz-Zentrum für Informationssicherheit in Saarbrücken, die KASTEL Security Research Labs am Karlsruher KIT und seit 2004 das Fraunhofer Institut für Sichere Informationstechnologie an der TU Darmstadt sowie die Lehrstühle für IT-Sicherheit an 50 deutschen Hochschulen und Universitäten und die Kompetenzzentren für IT-Sicherheit der 16 Bundesländer. An Institutionen und Agenturen mangelt es nun wirklich nicht.

Die Herausforderungen der Informationssicherheit liegen jedoch nicht in fehlenden Technologien, die auf zauberhafte Weise Sicherheit produzieren: Es mangelt an der Umsetzung bekannter Schutzmaßnahmen. Schließlich ist in der ISO 2700x, dem BSI IT-Grundschutz und vielen weiteren Standards ordentlich definiert, wie Unternehmen sich wirksam schützen können. Doch es fehlen nicht zuletzt Experten für die Umsetzung. Wie sinnvoll ist es, weitere Technologien am Ende der Fahnenstange zu erforschen, wenn die Stange selbst wackelig im Morast steckt? Wenn Hersteller mangels Produkthaftung Security Engineering und sichere Softwareentwicklung nicht ernst nehmen? Ein Auto braucht kein Radar zur Fußgängererkennung, wenn nicht mal die Bremsen zuverlässig funktionieren. Da könnte schon helfen, wenn Kinder bereits in der Grundschule lernen würden, besser nicht auf jeden Anhang zu klicken.

Inhalt

secorvo
security consulting

Security News

Cloud-Ausfallerscheinungen

Den meisten Verantwortlichen, die Dienste und Anwendungen „in die Cloud“ auslagern, dürfte klar sein, dass man damit Risiken verlagert: Der Ausfall eigener Systeme wird weniger relevant, und eigene Maßnahmen zur Absicherung von Systemen und Räumlichkeiten können eingespart werden.

Im Gegenzug begibt man sich in eine Abhängigkeit: Bei Ausfall der Internetanbindung oder des Cloud-Anbieters selbst können die Dienste nicht genutzt werden. In den meisten Fällen wird man dieses Risiko tragen und in Kauf nehmen, dass ein Anbieter mal einzelne Stunden bis hin zu ein oder zwei Tagen nicht zur Verfügung steht.

Wie sieht es aber aus, wenn Dienste – wie am 05.04.2022 bei Atlassian – für bis zu zwei Wochen ausfallen? Welche Auswirkungen hat das auf die Geschäftsprozesse? Müssen Entwickler nach Hause geschickt werden, da sie ohne ihre Cloud-Werkzeuge keine Software entwickeln können? Gibt es zeitkritische Prozesse, die nicht mehr funktionieren, wenn ein Dienst länger nicht zur Verfügung steht? Werden möglicherweise Sicherheitsprobleme übersehen, wenn Alarmierungen aus der Cloud nicht mehr eingehen?

Gerade versteckte Abhängigkeiten in immer stärker miteinander verzahnten digitalen Prozessen werden bei einer oberflächlichen Risikobewertung leicht übersehen – je mehr Cloud-Dienste in Anspruch genommen werden, desto genauer und häufiger sollte die Risiko-Prüfung wiederholt werden. Zur Sicherheit sollte man außerdem „analoge“ Ersatzprozesse vorsehen, um größere Ausfall-Schäden zu verhindern.

Drum prüfe, wer prüfen lässt

Der von Google angebotene Dienst VirusTotal überprüft hochgeladene Dateien kostenlos mit etwa 70 verschiedenen Antiviren-Programmen. Doch nur wenige Nutzer dürften zuvor die Benutzerhinweise gelesen haben, in denen darauf hingewiesen wird, dass keine personenbezogenen Daten hochgeladen werden sollen.

Am 15.03.2022 warnte das BSI vor möglichen Datenabflüssen bei VirusTotal, wenn statt Datei-Hashwerten beispielsweise unternehmensinterne Dokumente oder E-Mails hochgeladen werden. Neben den unternehmenseigenen Vorgaben zu Datenschutz und Informationssicherheit sind bei der Nutzung das Geschäftsgeheimnisgesetz und die DSGVO zu beachten.

Das kann auch für Antiviren-Programme gelten, bei denen die Virenerkennung cloudbasiert erfolgt. Hat der Hersteller seinen Sitz außerhalb der EU, müssen die hohen rechtlichen Anforderungen an eine Übermittlung personenbezogener Daten in Drittstaaten (wie bspw. die USA) erfüllt sein.

Cookie-Banner

Auf heutigen Webseiten sind (nervtötende) Cookie-Banner allgegenwärtig. Wer keine Cookies möchte, dem wird die Ablehnung meist obendrein durch „Dark Pattern“-Techniken erschwert, mit denen Besucher durch entsprechende Gestaltung der Banner dazu bewegt werden sollen, gegen ihren Willen eine Einwilligung zu erteilen. Um dieser Entwicklung entgegenzuwirken hat das European Data Protection Board (EDBP) am 15.03.2022 Richtlinien zur korrekten Bannergestaltung beschlossen.

Zuvor hatte die französische Datenschutzaufsicht CNIL am 31.12.2021 wegen eines zu umständlichen Verfahrens zur Cookie-Ablehnung ein 150-Mio.-€-Bußgeld gegen Google verhängt. In dieselbe Kerbe schlägt jetzt auch die Hamburgische Datenschutzaufsicht. Am 05.04.2022 forderte Thomas Fuchs (HmbBfDI) für Cookie-Banner einen „Alles ablehnen“-Knopf: Eine wirksame Einwilligung läge nur dann vor, wenn Zustimmung und Ablehnung gleichermaßen schnell und einfach zugänglich seien.

Doch auch diese Forderung greift noch zu kurz. Denn tatsächlich sind Cookie-Banner eine absurde Degeneration der datenschutzrechtlichen Einwilligung. Stellen Sie sich vor, in Ihrem örtlichen Supermarkt lägen ab sofort mehrere Packungen Kekse in jedem Einkaufswagen, die Sie vor Einkaufsbeginn aus dem Wagen herausnehmen müssten, wenn Sie sie nicht kaufen wollen. Genauso zwingen Cookie-Banner Seitenbesucher den Aufwand einer aktiven Ablehnung auf – anstatt bei Ignorieren des Banners automatisch von einer nicht erteilten Einwilligung auszugehen. Tatsächlich ist zu wünschen, dass die Aufsichtsbehörden bei Cookie-Bannern noch eine deutlich härtere Gangart wählen.

Bike Scamming

Schon am 07.08.2021 hatte die New York Post über Scamming-Angriffe auf das Buchungsverfahren der in New York verbreiteten City Bikes berichtet, nachdem der Angriff kurz zuvor bei Reddit beschrieben worden war. Die Attacke ist geradezu trivial und kommt gänzlich ohne IT aus: Zum Freischalten des Mietrads muss der Nutzer den auf dem Rad aufgeklebten QR-Code mit der Buchungs-App einscannen. Klebt man den QR-Code eines Rads auf ein anderes, kann man „sein“ Rad durch einen anderen Kunden (auf dessen Kosten) freischalten lassen.

Dieser simple Scamming-Angriff funktioniert bei allen Sharing-Systemen, bei denen die Identifikation

des Fahrzeugs über einen aufgebrachten Code erfolgt – eine verbreitete Methode übrigens auch bei E-Scootern. Es lohnt also, sich vor Freischalten des Fahrzeugs davon zu überzeugen, dass der aufgebrachte Code nicht überklebt oder ausgetauscht wurde.

Der geschilderte Angriff ist ein eindrückliches Beispiel dafür, dass die Optimierung des Benutzerkomforts schnell auf Kosten der Sicherheit geht. Da lohnt es, sich gelegentlich Einsteins Bonmot in Erinnerung zu rufen: „Mache die Dinge so einfach wie möglich. Aber nicht einfacher."

Neuer Auskunftsanspruch

Das am 01.12.2021 in Kraft getretene Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) regelt in §§ 21 ff. verschiedene Auskunftsansprüche. Neu ist § 21 Abs. 2 TTDSG, der Betreiber von Social-Media-Plattformen verpflichtet, Betroffenen mitzuteilen, wer als Verursacher einer Persönlichkeitsverletzung in Betracht kommt. Der Anspruch ist auch gegen Anbieter von Telemedien durchsetzbar, die zwar keinen Sitz in Deutschland haben, aber ihre Dienste auch in Deutschland erbringen.

Allerdings begrenzte das Schleswig-Holsteinische Oberlandesgericht am 23.03.2022 die Auskunft auf Bestandsdaten; Nutzungsdaten sind nicht mitzuteilen. Da die Verletzung der Auskunftspflicht nicht strafbewehrt ist und ohne Nutzungsdaten kein Nachweis für die Täterschaft vorliegt, ist der Anspruch in der Praxis eher ein stumpfes Schwert. Um wenigstens mittelbar an die Nutzungsdaten zu gelangen, bleibt den Betroffenen daher auch weiterhin nur der Weg über eine Strafanzeige.

Post-Corona-Aufräumarbeiten

Während der Corona-Pandemie wurden an vielen Orten – in Restaurants, Schulen, Krankenhäusern, Pflegeheimen und bei den Gesundheitsämtern – personenbezogene Daten von Bürgern erhoben und gespeichert. Nach Ablauf der jeweiligen Löschfrist, spätestens aber mit dem Wegfall der Rechtsgrundlagen wie den Corona-Verordnungen und dem Infektionsschutzgesetz sind diese Daten zu löschen.

Der Baden-Württembergische Landesdatenschutzbeauftragte Dr. Stefan Brink hat die wichtigsten Verarbeitungen in seiner Pressemitteilung vom 08.04.2022 („Zurück zur Freiheit") aufgelistet. Darin weist er auch darauf hin, dass Arbeitgeber (bis auf die Heil- und Pflegebranche) alle erhobenen Daten über den Impfstatus der Mitarbeiter unverzüglich löschen müssen – und kündigt stichprobenartige Überprüfungen an.

NEO-Innovationspreis

Die TechnologieRegion Karlsruhe hat den diesjährigen Innovationspreis NEO2022 dem Thema „Cybersecurity" gewidmet. Für den mit 20.000 € dotierten Preis können sich Unternehmen bundesweit bis zum 19.05.2022 online bewerben. Die Preisverleihung wird am 21.10.2022 in Karlsruhe stattfinden.

Secorvo News

Der frühe Vogel …

… fängt den Wurm: Das gilt auch für die Buchung Ihrer Weiterbildung. Melden Sie sich bereits jetzt zum T.I.S.P.-Seminar im September an (**19.–23.09.2022**) und bereiten Sie sich mit dem T.I.S.P.-Buch von Secorvo, das wir Ihnen nach Ihrer Anmeldung zusenden, entspannt darauf vor.

Bereits zertifizierten T.I.S.P.-Absolventen und erfahrenen Sicherheitsexperten bieten wir das Seminar IT Security Insights mit ausgewählten vertieften Beiträgen zu aktuellen Themen der IT-Sicherheit (**27.–29.09.2022**).

Wer eine gründliche Einführung in Theorie und Praxis von Public Key Infrastrukturen sucht, sollte sich unser viertägiges PKI-Seminar (**04.–07.11.2022**) im Kalender vermerken. Und Ende November bietet sich die nächste Möglichkeit, sich zum BSI Vorfall-Experten ausbilden zu lassen (**29.11.–01.12.2022**).

Die ausführlichen Seminarprogramme und die Möglichkeit zur Online-Anmeldung finden Sie unter https://www.secorvo.de/seminare.

Wer besitzt mein Smartphone?

Auch wenn wir uns kaum noch daran erinnern können, wie wir ohne sie klarkamen: Smartphones gibt es erst seit 15 Jahren. Genauso alt wie das Smartphone ist die Geschichte der Smartphone Hacks – von den ersten Jailbreaks über die Celebrity Nudes bis hin zu kommerzieller und staatlicher Spyware.

Anhand von Attack Trees und Live-Hacking-Demos zeigen Ihnen Armin Harbrecht und Maximilian Stauß (aramido) beim kommenden KA-IT-Si-Event am **19.05.2022** um 18 Uhr, wie Smartphones angegriffen werden. Dieses Verständnis ist Voraussetzung für effektive Schutzmaßnahmen.

Die Veranstaltung führen wir hybrid durch. Die Vor-Ort-Plätze bei aramido sind bereits ausgebucht, aber für eine Online-Teilnahme können Sie sich noch anmelden (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Mai 2022	
10.-13.05.	Blackhat Asia 2022 (Blackhat, hybrid)
10.-13.05.	European Identity & Cloud Conference 2022 (KuppingerCole, Berlin/virtuell)
10.-11.05.	BvD Verbandstage 2022 (BvD, Berlin)
16.-17.05.	23. Datenschutzkongress (EUROFORUM, Berlin)
16.-18.05.	Entwicklertag 2022 (VKSI, GI, ObjektForum, Karlsruhe)
19.05.	Wer besitzt mein Smartphone? (KA-IT-Si, Karlsruhe)
30.05.-03.06.	Eurocrypt 2022 (IACR, Trondheim/NOR)
Juni 2022	
06.-10.06.	7th IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/I)
06.-08.06.	OWASP Global AppSec (OWASP Foundation, Dublin/IRL)
20.-21.06.	DuD 2022 (COMPUTAS, Berlin)

Fundsache

Am 31.03.2022 wurde Version 4.0 des PCI DSS Standards veröffentlicht. Der Standard legt umfangreiche technische und organisatorische Anforderungen an Zahlungssysteme und Dienstleistungen fest. Diese wurden konkretisiert und verschärft. Die Änderungen zur Vorgängerversion 3.2.1 sind ebenso wie der Standard selbst auf Englisch, Deutsch und Portugiesisch verfügbar. Einige neue Anforderungen müssen PCI-kompatible Anbieter bis spätestens 31.03.2025 umsetzen.

Impressum

Secorvo Security News – ISSN 1613-4311

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

secorvo
security consulting

Secorvo Security News

Mai 2022

Behind the Scenes

Die meisten Internet-Nutzer werden wissen, dass Webseiten, die sie besuchen, ihre Seitenaufrufe tracken – nicht selten ohne rechtswirksame Einwilligung. Weniger Internet-Nutzer werden wissen, dass die auf der Seite angezeigte Werbung meist von Dritten eingespielt wird. Doch die wenigsten Internet-Nutzer wissen, dass und wie die Werbung auf sie persönlich zugeschnitten wird.

Tatsächlich versteigern die meisten Portalseiten die Werbeplätze erst beim Aufruf der Seite über „Real Time Bidding“ (RTB) innerhalb weniger Millisekunden. Dazu schickt ein Werbeplatz-Anbieter (oder dessen Broker) über das OpenRTB-Protokoll einen „Ad Request“ an einen RTB-Exchange-Server, der daraus einen „Bid Request“ erzeugt und per Broadcast an alle Werbetreibenden verteilt. Dieses Datenpaket enthält alle bekannten Angaben über das die Seite aufrufende Gerät (u. a. Hersteller und Modell, Betriebssystem, IP-Adresse, Hash der MAC-Adresse und aktuelle GPS-Koordinaten) und den Nutzer (User ID, Geschlecht, Geburtsjahr, Keyword-Liste der Interessen und GPS-Daten des „Heimatstandorts“).

Nach einer am 14.05.2022 veröffentlichten Studie des Irish Council for Civil Liberties (ICCL) werden allein von Google Bid Requests an über 4.500 Unternehmen in den USA und über 1.000 in Europa geschickt – bei jedem deutschen Surfer im Schnitt im Minutentakt. Jeder Empfänger kann darüber benutzerbezogene Surf- und (bei mobilen Devices) Bewegungsprofile erstellen – eine Quelle, die in den USA auch bereits Sicherheitsbehörden nutzen.

Jeder Entwickler weiß, dass Real-Time-Bidding auch ohne die Verteilung der Anfragen funktioniert – ein Schelm, wer Arges dabei denkt. Vielleicht sollten wir uns ab und zu Immanuel Kants 1785 in der „Grundlegung der Metaphysik der Sitten“ formulierten praktischen Imperativ in Erinnerung rufen: „Handle so, dass du die Menschheit, sowohl in deiner Person, als in der Person eines jeden andern, jederzeit zugleich als Zweck, niemals bloß als Mittel brauchest.“

Inhalt

secorvo
security consulting

Security News

GPS-Tracking

In einem erst jetzt veröffentlichten Urteil vom 17.01.2022 hat das VG Wiesbaden Kriterien für den Einsatz von GPS-Tracking im Logistikbereich aufgestellt. Das klagende Unternehmen hatte Geo-Tracking in den Fahrzeugen verbaut, wodurch der Live-Standort der Fahrzeuge und der Benzinverbrauch feststellbar waren. Die Daten wurden mittels Fahrerkarte einzelnen Fahrern zugewiesen und 400 Tage in der Cloud gespeichert.

Begründet wurde das Tracking mit Effizienzsteigerung sowie Schutz vor Missbrauch und Diebstahl. Einwilligungen der betroffenen Arbeitnehmer lagen nicht vor, auch waren keine Maßnahmen ergriffen worden, um eine verdeckte Arbeitnehmerüberwachung zu verhindern. Das Gericht bestätigte die Einschätzung der zuständigen Aufsichtsbehörde: Eine Einwilligung der Arbeitnehmer sei als Rechtsgrundlage nicht ausreichend, da diese in der Regel von Arbeitnehmern nicht wirksam erteilt werden kann. In Betracht käme nur die Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO) nach sorgfältiger Interessensabwägung. Ohne Prüfung, ob es keine weniger einschneidenden Mittel zur Zweckerfüllung gibt, sei das Tracking rechtswidrig.

25-jähriger Bug in cmd.exe

Na, wenn das kein Geburtstagsgeschenk ist: Auf full disclosure wurde am 10.05.2022 eine Denial-of-Service-Schwachstelle im 25 Jahre alten, noch aus Windows-NT-Zeiten stammenden Kommandozeilen-Interpreter cmd.exe gemeldet. Auch wenn die Auswirkung sich auf das „Abschießen" einer eigenen Instanz des Interpreters beschränkt und eine gezielte Ausnutzung oder Angriffe gegen andere Benutzer darüber nicht möglich sind, bleibt die Frage, wie ein so offensichtlicher Fehler so lange unbemerkt bleiben konnte.

Merke: Software reift nicht über die Jahre bei ruhiger Lagerung (wie Whisky oder guter Wein), sondern sollte (wie Champagner) regelmäßig gerüttelt (sprich: untersucht) werden. Auch jahrelang bewährte Software ist nicht automatisch fehlerfrei. Der Fall zeigt, wie wichtig Aktivitäten zur systematischen Untersuchung von Software sind, wie z. B. die der Open Source Security Foundation, sowie die regelmäßige Durchführung von Penetrationstests. Im konkreten Fall besteht kein weiterer Handlungsbedarf – die eigene Kommando-Zeile kann man auch ohne Crash schließen.

Videokonferenzen ohne AV-Vertrag

In der DuD 05/2022 diskutieren Friederike Schellhas-Mende, Nils Wiedemann und Nicolas Blum die Auswirkungen des am 01.12.2021 in Kraft getretenen TTDSG und des neuen TKG auf Videokonferenzsysteme. So wechselt nicht nur die datenschutzrechtliche Zuständigkeit zum BDfI, sondern führt die Einordnung als „nummernunabhängiger interpersoneller Telekommunikationsdienst" dazu, dass für Videokonferenzdienste i.d.R. kein Auftragsverarbeitungsvertrag zu schließen ist.

Datenschutz-Bußgeldbemessung

Am 12.05.2022 hat der Europäische Datenschutzausschuss (EDSA) Leitlinien für die einheitliche Sanktionierung von Bußgeldern bei Datenschutzverstößen veröffentlicht und damit die Leitlinien vom 03.10.2017 (WP 253) präzisiert. Die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) hatte bereits am 14.10.2019 ein abgestimmtes Verfahren veröffentlicht (SSN 10/2019), das nun mit der Veröffentlichung der EDSA-Leitlinien seine Gültigkeit verliert.

Das Konzept des EDSA unterscheidet sich wesentlich von dem der DSK. Zwar betont es ebenfalls, dass Bußgelder auf die spezifischen Bedingungen des Einzelfalls zugeschnitten sein müssen. Doch es bleibt deutlich abstrakter als das deutsche Konzept, das aus dem Jahresumsatz des Unternehmens einen „Grundwert" (Umsatz pro Tag) ermittelte und diesen abhängig von dem Schweregrad des Verstoßes mit einem Faktor belegte.

Ausgangspunkt des EDSA-Konzepts ist eine Bewertung der Art, Dauer und Schwere des Verstoßes, in die u. a. die Zahl der Betroffenen, der Zweck der Verarbeitung und die Größe des verursachten Schadens einfließen. Daraus wird ein „Startwert" als prozentualer Anteil des maximal möglichen Bußgelds abgeleitet. Aus dem Jahresumsatz des Unternehmens errechnet sich dann das minimal aufzuerlegende Bußgeld zu 0,2% (Kleinst-) bis 50% (Großunternehmen) des zuvor bestimmten Startwerts. Je nach Ernsthaftigkeit des Verstoßes und den Bedingungen des Einzelfalls, wie z. B. ergriffene Gegenmaßnahmen oder frühere Verstöße, wird von der zuständigen Aufsichtsbehörde dann das Bußgeld zwischen Minimal- und Startwert festgelegt.

Ob dieses Verfahren geeignet ist, die Höhe der verhängten Bußgelder europaweit zu vereinheitlichen und deren Bestimmung transparenter zu machen, darf bezweifelt werden: Als „Bußgeldrechner" eignet es sich noch weniger als das Konzept der DSA. Die Angemessenheit der europäischen Bußgelder wird also weiterhin vom Augenmaß der zuständigen Behörden (und ggf. der Gerichte) abhängen.

Klagerecht für Verbraucherschutzverbände

Am 28.04.2022 hat der EuGH Verbraucherschutzverbänden ein ähnliches Klagerecht eingeräumt wie schon bei Wettbewerbsfragen. Die Verbände dürfen demnach in Form von Verbandsklagen Unterlassungsklagen gegen Verletzungen des Schutzes personenbezogener Daten erheben. Damit erhalten auch diejenigen Verbraucherinnen und Verbraucher eine Stimme, die aus mangelnder Kenntnis ihrer Rechte nicht gegen Datenschutzverstöße vorgehen.

Cookie-Walls

Die französische CNIL hat am 16.05.2022 erste Empfehlungen für Cookie-Walls veröffentlicht. Cookie-Walls stellen Nutzer beim Aufruf einer Webseite vor die Wahl, entweder alle Cookies für Werbezwecke zu akzeptieren oder eine Gebühr für die werbefreie Nutzung zu zahlen. Zwar sei die Einwilligung freiwillig, jedoch müsse den Nutzern eine „echte und faire Alternative" angeboten werden, die sich an der Angemessenheit der Vergütung bemisst. Die CNIL gibt dafür keinen Schwellenwert an, sondern verlangt, dass diese begründbar ist und ermutigt zu einer transparenten Kostenfestsetzung.

Stimmt der Nutzer der kostenpflichtigen Alternative zu, dürfen nur für den Betrieb der Webseite erforderliche Cookies hinterlegt werden. Der Anbieter kann davon abweichen, wenn z. B. auf Webseiteninhalte von Dritten zugegriffen werden muss. Dafür wird wiederum eine Einwilligung benötigt. Umstritten ist, ob die CNIL als Datenschutzbehörde nicht ihre Kompetenzen überschreitet, indem sie sich zur Vergütung äußert. In ihren Leitlinien hatte die CNIL bereits 2019 Cookie-Walls als unzulässig bezeichnet, woraufhin ihr das oberste französische Verwaltungsgericht diesbezüglich die Zuständigkeit absprach. Die Datenschutzkonferenz (DSK) verweist in ihrer Orientierungshilfe für Anbieter von Telemedien vom 20.12.2021 hinsichtlich Cookie-Walls auf die Leitlinien zur Einwilligung der EDPB. Danach sind Cookie-Walls nur dann unzulässig, wenn sie keine echte Wahlmöglichkeit anbieten („is not presented with a genuine choice").

ISO 27002 – neu und sortiert

Im Februar 2022 wurde die dritte Überarbeitung der ISO 27002 veröffentlicht; eine neue Version der ISO 27001 ist wohl in Kürze zu erwarten. Die ISO 27001 legt die prüfbaren Anforderungen eines Informationssicherheitsmanagementsystems (ISMS) fest und listet im Annex A die Maßnahmen der ISO 27002 auf. Daher sollte die Anpassung des unternehmenseigenen ISMS an die überarbeiteten und neuen Maßnahmen frühzeitig eingeplant werden.

Neu sind elf der nunmehr 93 Maßnahmen; weitere wurden zusammengefasst oder um neue Inhalte wie Bezüge zum Datenschutz angereichert. Eine Hilfe ist die Einführung von Eigenschaften zu jeder Maßnahme. Darüber können Unternehmen die Maßnahmen nach fünf unterschiedlichen Kriterien sortieren: Art der Risikosteuerung, Informationssicherheitsziele, Cybersecurity-Methoden, Managementziele (wie in der ISO 27002:2013) oder Handlungsfelder nach der NIS-Richtlinie. Eine Übersicht der Änderungen und einen Vorschlag für den schrittweisen Umstieg von Version 2013 hat Milan Burgdorf in der DuD 05/2022 zusammengestellt.

Digital Services Act

Am 23.04.2022 haben sich Europäischer Rat und Parlament über den Digital Services Act (DSA) als Nachfolger der 20 Jahre alten E-Commerce-Richtlinie geeinigt. Dieser wird neben der DSGVO weitere Vorgaben für Online-Dienste wie Vermittlungsdienste, Hosting-Dienste und Online-Plattformen enthalten. So werden beispielsweise „Dark Patterns" und irreführende Benutzeroberflächen bei der Auswahl der Cookies verboten. Sensible Daten wie politische Ansichten, religiöse Überzeugungen und sexuelle Vorlieben dürfen in Zukunft nicht mehr für personalisierte Werbung verwendet werden. Auch dürfen über Minderjährige keine Daten mehr gesammelt und diesen auch keine personalisierte Werbung mehr angezeigt werden. Zudem schafft der DSA u. a. für Nutzer eine einfache Meldemöglichkeit, infolge derer die Online-Dienste illegale Inhalte wie Hassrede, Gewaltaufrufe oder Terrorpropaganda entfernen müssen.

Bußgelder bei Verstößen gegen den DSA fallen mit bis zu 6 % des weltweit erzielten Jahresumsatzes noch höher aus als bei der DSGVO. Betreiber von Online-Diensten müssen sich bald auf die Vorgaben des DSA einstellen, da die Verordnung nach einer nur dreimonatigen Übergangsfrist unmittelbar in allen EU-Staaten gelten wird.

Secorvo News

13. Tag der IT-Sicherheit

Wir freuen uns sehr, den 13. Karlsruher Tag der IT-Sicherheit am **14.07.2022** wieder als Präsenzveranstaltung durchführen zu können. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, dem Kompetenzzentrum für angewandte Sicherheitstechnologie am KIT (KASTEL) und dem CyberForum e.V. hat die Förderung des Erfahrungsaustauschs unter IT-Sicherheitsverantwortlichen (nicht nur) in der TechnologieRegion Karlsruhe zum Ziel. Das Programm und die Möglichkeit zur Anmeldung finden Sie unter www.tag-der-it-sicherheit.de.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2022	
06.-10.06.	7th IEEE European Symposium on Security and Privacy (IEEE, Genua/IT)
06.-08.06.	OWASP Global AppSec (OWASP Foundation, virtuell)
16.-17.06.	AREA41 Security Conference (DEFCON, Zürich/CH)
20.-21.06.	DuD 2022 (COMPUTAS, Berlin)
21.-23.06.	Omnisecure 2022 (in TIME, Berlin)
23.-24.06.	Annual Privacy Forum 2022 (ENISA, DG Connect Católica University of Portugal, Warschau/POL)
Juli 2022	
11.-15.07.	PETS 2022 (University of Minnesota, hybrid)
14.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
August 2022	
06.-11.08.	Blackhat USA 2022 (Blackhat, Las Vegas/US)
10.-12.08.	31st USENIX Security Symposium (usenix, Boston/US)
11.-14.08.	DEF CON 30 (DEFCON, Las Vegas/US)

Fundsache

Neben dem Bericht des BSI zur Lage der IT-Sicherheit sollte man auch einen Blick in das Bundeslagebild Cybercrime 2021 des BKA werfen: Sehr kompakt und übersichtlich wird darin über typische Angriffsziele und -methoden von Cyberkriminellen berichtet. Die erfassten Fälle nehmen zwar stetig zu, die aufgeklärten Fälle jedoch ebenfalls.

Impressum

Secorvo Security News – ISSN 1613-4311

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

secorvo
security consulting

Secorvo Security News

Juni 2022

Wer nicht hören will...

Dieser Grundsatz gilt fast überall, nur nicht für den Datenschutz im öffentlichen Bereich: Anlässlich des EuGH-Urteils vom 05.06.2018 hatte die Datenschutzkonferenz am 01.04. 2019 Anforderungen an den rechtskonformen Betrieb von Facebook-Fanpages aufgestellt. Zuletzt veröffentlichten die Datenschutzaufsichtsbehörden hierzu am 18.03.2022 ein Kurzgutachten und forderten im selben Atemzug Ministerien und weitere öffentliche Stellen auf, für datenschutzkonforme Zustände zu sorgen, sprich: die Nutzung von Facebook-Fanpages einzustellen. Passiert ist seitdem: nichts. Und es ist fraglich, ob sich daran etwas ändert. Denn anders als Unternehmen und Bürger müssen Behörden Vorgaben der Aufsichtsbehörden faktisch nicht umsetzen. Juristisch ausgedrückt: § 20 Abs. 7 BDSG entzieht den Aufsichtsbehörden die Befugnis zur Anordnung der sofortigen Vollziehung nach § 80 Abs. 2 Nr. 4 VwGO ausdrücklich, und § 43 Abs. 3 BDSG schließt die Verhängung von Bußgeldern gegen öffentliche Stellen aus. Behörden sind, wie Meldungen aus den Aufsichtsbehörden zeigen, auch nicht gewillt, sich freiwillig zu unterwerfen.

Angesichts der Vorbildfunktion der öffentlichen Hand schwant einem nichts Gutes: Hier werden Ignoranz und Respektlosigkeit gegenüber hoheitlichem Handeln zum Schutz der Privatsphäre rechtlich gebilligt. Ein Staat, der seinen Behörden einen Freibrief bei datenschutzwidrigem Verhalten einräumt, verletzt nicht nur das Rechtsstaatsprinzip der Gesetzmäßigkeit der Verwaltung (Art. 20 GG), sondern setzt auch seine Autorität aufs Spiel, wenn er von Bürgern, Schulen und Unternehmen verlangt, wichtige Arbeitsmittel wie z. B. Teams oder Microsoft 365 durch Open-Source-Lösungen zu ersetzen und damit die eigene Arbeitsfähigkeit zu gefährden. Der Verweis auf den Klageweg ist da ein stumpfes Schwert – ein Griff in die Haushaltskasse der Behörde (auch mal in sechsstelliger Höhe, wie es in anderen EU-Ländern Gang und Gäbe ist) dürfte da schon wirkungsvoller sein, auch wenn das Bußgeld nur von der rechten in die linke Tasche wandert.

Inhalt

secorvo
security consulting

Security News

Don't Stop Top 10

Regelmäßig veröffentlichen Hersteller, Fachportale oder Behörden die fünf, sieben oder zehn häufigsten Risiken oder gefährlichsten Schwachstellen, wahlweise in IT-, Informations- oder Cybersicherheit. So auch am 17.05.2022 die CISA mit zehn Handlungsfeldern bezüglich schwacher Sicherheitsmaßnahmen und typischer Angriffswege auf IT-Systeme. Andere Zusammenstellungen wie die CWE Top 25 Most Dangerous Software Weaknesses oder die OWASP Top 10 listen verbreitete Schwachstellen in der Software-Entwicklung.

Solche Rankings unterstützen eine schnelle Risiko-Priorisierung der jeweiligen Bedrohungen und nennen teilweise, wie die CISA-Liste, Maßnahmen zur Abschwächung oder Abhilfe. Sie richten den Blick allerdings nur auf ausgewählte verbreitete Risiken und ersetzen daher keine umfassende Risikoanalyse, wie sie ein Informationssicherheitsmanagementsystem (ISMS) fordert. Ihren vollen Nutzen entfalten sie auch erst im Kontext eines ISMS (bspw. nach ISO 27001 oder BSI IT-Grundschutz), das sicherstellt, dass die Umsetzung der Maßnahmen zur Reduktion der ermittelten Risiken regelmäßig und systematisch überprüft werden.

Cloud Computing Threats

Die Cloud Security Alliance (CSA) veröffentlichte am 06.06.2022 die elf Top Threats to Cloud Computing. Dazu waren zuvor über 700 Experten befragt worden. In der Auflistung finden sich zahlreiche Bekannte wie „Insufficient Identity" oder „Insecure Interfaces and APIs". Dennoch ist der Bericht lesenswert, denn er beschreibt die einzelnen Bedrohungen im Detail und vergleicht die Ergebnisse mit denen des Berichts aus dem Jahr 2019. So kann er helfen, die eigenen Risikoabschätzungen und Maßnahmenlisten für Cloud-Dienste zu überprüfen.

Drittstaatenübermittlung

Anlässlich des Beginns des fünften Geltungsjahrs der Datenschutzgrundverordnung (DSGVO) forderte der IT-Verband Bitkom am 25.05.2022, dass sich der „Datenschutz an realen Gefahren orientieren" müsse, nicht an „theoretischen Risiken", wie beispielsweise bei der Frage der Zulässigkeit des Einsatzes von Videokonferenzsystemen von US-Unternehmen in deutschen Schulen.

Dabei kommt es bei der Feststellung der Zulässigkeit einer Übermittlung von personenbezogenen Daten in Drittstaaten (Art. 44 ff. DSGVO) auf das Risiko gar nicht an. Entscheidend ist einzig, ob „das betreffende Drittland [...] ein angemessenes Schutzniveau" für die personenbezogenen Daten bietet. Dies hat Auswirkungen auf die Bewertung von Rechtsakten der Drittstaaten, die die Rechte (insbesondere ausländischer) Betroffener beschränken, wie der CLOUD-Act der USA. Und der EuGH stellte 2020 im Schrems II-Urteil klar, dass personenbezogene Daten nur dann in ein Drittland übermittelt werden dürfen, wenn das vom Anbieter garantierte Schutzniveau dem in der Union garantierten gleichwertig ist.

Das stellt viele Unternehmen bei der Nutzung von Cloud-Diensten vor Herausforderungen, denn die Verantwortung für die in ihrem Auftrag durch Dritte verarbeiteten Daten und die Pflicht zur Einholung von Einwilligungen liegt bei ihnen – auch dann, wenn ein Unter-Unter-Unterauftragnehmer eines Dienstleisters die Daten in ein Drittland übermittelt.

Schmerzensgeld für Google Fonts

Am 20.01.2022 sprach das Landgericht München I einem Kläger 100 € Schmerzensgeld zu, da auf einer von diesem besuchten Webseite Google Fonts eingebunden waren und damit seine IP-Adresse ohne Einwilligung an Google-Server übermittelt worden war. Da half auch nicht, dass Google (nach eigenen Angaben) die IP-Adresse nicht speichert.

Mit Verweis auf dieses Urteil wird derzeit versucht, Schadensersatzansprüche in Höhe von 100 € bei Webseitenbetreibern geltend zu machen, die Google Fonts in ähnlicher Weise nutzen – leicht feststellbar mit einem Browser-Plugin zur Tracking-Analyse. Das kann lukrativ sein, denn Google Fonts wurden bereits mehr als 63 Billionen Mal abgerufen.

Wir empfehlen, die Einbindung von Google Fonts zu überprüfen und gegebenenfalls zu korrigieren. Gleiches gilt für die Einbindung anderer Dienste von Anbietern in Drittstaaten wie Karten, Videos oder Social Media Share Buttons: Auch hier wird die IP-Adresse an den Anbieter übermittelt, was nur mit expliziter Einwilligung des Besuchers in die Übermittlung an und die Datenverarbeitung in dem jeweiligen Drittstaat zulässig ist.

Zoom in der Schule

Der hessische Beauftragte für Datenschutz und Informationsfreiheit teilte am 21.06.2022 mit, dass nun der Einsatz von Zoom für Lehrveranstaltungen nach dem „Hessischen Modell" erlaubt sei. Das setzt voraus, dass ein von Zoom unabhängiger Auftragsverarbeiter mit Servern und Sitz in der EU beauftragt wird und die Inhalte Ende-zu-Ende verschlüsselt werden. Ein Abfluss von personenbezogenen Daten in die USA wird durch diese Maßnahmen verhindert.

Tracking durch ID-Provider

Am 14.01.2020 hatte Google angekündigt, die Unterstützung von Third-Party-Cookies im Chrome-Browser im Jahr 2022 auslaufen zu lassen, und Apple hatte bereits am 26.04.2021 mit iOS 14.5 das Tracking durch Apps als Voreinstellung deaktiviert. Diese Entwicklung bedeutet keineswegs das Ende des Tracking (da Google und Apple über ausreichend selbst erhobene Verhaltensdaten verfügen) – wohl aber das Ende der Datenbasis heutiger Werbenetzwerke (siehe Editorial SSN 5/2022).

Die suchen bereits fieberhaft nach Alternativen, um auch zukünftig Verhaltensdaten zu gewinnen – idealerweise mit Bezug zu möglichst invarianten IDs wie der Mobilfunknummer oder der E-Mail-Adresse von Seitenbesuchern und App-Nutzern. Was liegt da näher, als die Nutzer-Identifikation gleich mit dem Login zu koppeln? Google, Apple und Facebook machen es seit Jahren vor: Sie bieten Login-Schnittstellen an, die Webseitenanbieter einbinden können, um sich damit die Implementierung einer eigenen Nutzerverwaltung zu sparen. Zahlreiche weiterer Identitätsanbieter erblicken gerade das Licht der Welt: Sie verschenken den Dienst und verdienen an den gehashten ID-Daten (wie bspw. Zoetap), die sie an zahlende Werbeanbieter und -broker weiterleiten.

Ohne Einwilligung der Betroffenen ist die Nutzung von ID-Anbietern, die (pseudonymisierte) Daten an Dritte weitergeben, allerdings genauso rechtswidrig wie die Nutzung der ID-Services von Google & Co.

Erhalte das freie Internet

Mit diesem Claim begrüßt TrustPid – ein von Vodafone und der Deutschen Telekom entwickelter ID-Service, der als deutsche Alternative zum Cookie-Tracking gedacht ist – seine Seitenbesucher. Willigt der Nutzer ein, wird aus der Mobilfunknummer und der IP-Adresse des Besuchers eine TrustPid-ID abgeleitet. Alle auf diese bezogenen Tracking-Informationen einer Seite, die TrustPid nutzt, werden dann an den TrustPid-Server übermittelt.

Die vom Nutzer erteilte Einwilligung lässt sich (anders als bei Cookies, die man beim Schließen des Browsers löschen lassen kann) allerdings nicht so leicht widerrufen. Der Weg ist umständlich und intransparent: Ein Widerruf ist nur aus dem Mobilfunknetz im Datenschutzportal von TrustPid oder (gegebenenfalls) auf der die Daten erhebenden Webseite möglich.

TrustPid befindet sich derzeit im Technik-Test beim Axel-Springer-Verlag und kommt beispielsweise auf bild.de zum Einsatz. Dort erfolgt der Widerruf über separate Einwilligungsverwaltungen: „Widerruf Nutzerkennungen“ (TrustPid) und „Widerruf Tracking“ (Cookies). Die Provider behalten sich vor, dass die Löschung der TrustPid-Daten bis zu 90 Tage dauern kann. Ein Widerruf ist damit deutlich umständlicher als die Einwilligung und zudem sowohl in TrustPid als auch auf bild.de für Nutzer kaum erkennbar, da er lediglich in der Datenschutzerklärung, nicht aber auf der „Cookie-Wall“ Erwähnung findet (obwohl in letzterer die Einwilligung eingeholt wird).

Die deutschen Aufsichtsbehörden haben noch keine abschließende Bewertung zu TrustPid abgegeben. Für die Verwendung einer ähnlichen Technik hatte Verizon in den USA am 07.03.2016 einen Bußgeldbescheid der Federal Communication Commission über 1,35 Millionen US-Dollar erhalten.

Secorvo News

Spätsommerbildung

Wer schon vor dem Sommerurlaub wissen möchte, was sie oder er anschließend lernen wird, sollte sich unseren Frühbucherrabatt sichern: z. B. für das T.I.S.P.-Seminar (19.-23.09.2022) mit anschließender Möglichkeit zur Zertifizierung oder das Seminar IT Security Insights (27.-29.09.2022). Wir freuen uns auf Ihre Anmeldung und Ihren Besuch in Karlsruhe!

13. Tag der IT-Sicherheit

Wir freuen uns sehr, Sie zum diesjährigen Karlsruher Tag der IT-Sicherheit am **14.07.2022** in den Saal Baden der IHK Karlsruhe einladen zu können. Die Kooperationsveranstaltung der Karlsruher IT-Sicherheitsinitiative (KA-IT-Si) mit der IHK Karlsruhe, dem Kompetenzzentrum für angewandte Sicherheitstechnologie am KIT (KASTEL) und dem CyberForum e.V. will den Erfahrungsaustausch unter IT-Sicherheitsverantwortlichen (nicht nur) in der TechnologieRegion Karlsruhe fördern.

Es erwarten Sie spannende Fachvorträge zu den Themen Digitale Souveränität, Sicherheit und Erklärbarkeit von KI, Quantencomputer und Cybersicherheit sowie sicheres Betriebssystem durch Asset-, Lifecycle- und Patch-Management – und ein intensives Buffet-Networking.

Das Programm und die Möglichkeit zur Anmeldung finden Sie hier.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2022	
11.-15.07.	PETS 2022 (University of Minnesota, Sydney/AUS)
11.-14.07.	DFRWS USA 2022 (DFRWS, virtuell)
14.07.	13. Tag der IT-Sicherheit (KA-IT-Si, IHK, Cyberforum, KASTEL, Karlsruhe)
August 2022	
06.-11.08.	Blackhat USA 2022 (Blackhat, Las Vegas/US)
07.-09.08.	SOUPS 2022 (usenix, Boston/US)
10.-12.08.	31st USENIX Security Symposium (usenix, Boston/US)
11.-14.08.	DEF CON 30 (DEFCON, Las Vegas/US)
13.-18.08.	Crypto 2022 (IACR, Santa Barbara/US)
September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)

Fundsache

Der beste Schutz gegen Cyberattacken sind sensibilisierte Mitarbeitende. Das ist das Zwischenergebnis einer Datenschutzprüfung zur Ransomware-Prävention des Bayerischen Landesamts für Datenschutz (BayLDA). Für Unternehmen werden Ransomware-Angriffe und wirksame Gegenmaßnahmen in einem Infoblatt und einer Handreichung checklistenartig erklärt.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Milan Burgdorf, Stefan Gora, Kai Jendrian, Friederike Schellhas-Mende (Editorial), 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

secorvo
security consulting

Secorvo Security News

Juli 2022

Moderne Abhängigkeiten

Lange schon sind die Produktlebenszyklen bei IT-Produkten – verglichen mit anderen Branchen – recht kurz. Das gilt besonders für Software. Solange die Produkte in Organisationen oder bei Privatpersonen betrieben wurden, erwuchs daraus selten ein Problem: Man nutzte ein Programm so lange, bis ein nicht behebbarer Fehler oder fehlende Features eine Migration erzwangen.

Inzwischen sind immer mehr Organisationen und Menschen von IT-Diensten abhängig, die sie nicht mehr selbst kontrollieren, wie bspw. Cloud-Dienste, Steuersysteme in Fahrzeugen oder auch Lösungen, die bedeutsam für die Gesundheit von Menschen sind.

Die Abgabe von Kontrolle und der Einsatz von fremdbetreuten Diensten sind verlockend, weil sie einige unmittelbare Vorteile bieten: Zeitersparnis und die Kompensation von fehlendem Know-How. Und häufig betreiben Anbieter die Lösungen zudem effizienter und professioneller als ihre Kunden das selbst könnten.

Manchmal geht aber auch etwas schief. So gibt es zahlreiche Beispiele für Störungen – u. a. bei Amazon, Microsoft, Google, Facebook und Atlassian. Auch werden Dienste eingestellt, siehe die umfangreiche Killed by Google-Liste. Und was passiert, wenn darunter ein kritischer Dienst ist? Das ist keine hypothetische Frage: Wegen wirtschaftlicher Schwierigkeiten stellte 2020 ein Unternehmen aus dem Medizinbereich seinen Support für ein Retina-Implantat ein. Bei ca. 350 Betroffenen, die temporär wieder sehen konnten, bleibt nun im Falle eines Defekts Medizinschrott ohne Funktion im Körper.

Daher ist es ratsam, sich nicht blind in die Cloud zu stürzen, sondern nüchtern mögliche Risiken zu betrachten und sich über kompensierende Maßnahmen Gedanken zu machen. Eine Hilfestellung können dabei Anleitungen sein wie der Grundschutzbaustein Cloud-Nutzung oder der Kriterienkatalog Cloud Computing C5 des BSI.

Inhalt

Security News

Dünne Luft für Google Analytics

Die am 17.08.2020 publizierten 101 Beschwerden der noyb zu EU-US-Datentransfers wirken weiter: Nach der österreichischen dsb (SSN 1/2022) und der französischen CNIL (SSN 2/2022) hat nun auch die italienische Datenschutzbehörde GPDP entschieden, dass die Verwendung von Google Analytics gegen die DSGVO verstößt.

Eine Risikobewertung, die annimmt, dass US-Behörden wahrscheinlich nicht nach den Daten fragen, lehnt sie ab. Vielmehr müssen Unternehmen garantieren, dass das Grundrecht auf informationelle Selbstbestimmung weiterbesteht, wenn die Daten den Europäischen Wirtschaftsraum verlassen. Gekürzte IP-Adressen sind für die GPDP personenbezogene Daten; die Kürzung sei keine ausreichende Anonymisierung. Angesichts dieser Entwicklung sollten Analytics-Kunden ihr Tracking zügig auf datenschutzkonforme Alternativen umstellen.

Post-Quantum-Kryptoverfahren

Quantencomputer bedrohen die Sicherheit aller heute eingesetzten asymmetrischen Kryptoverfahren, denn mit dem von Peter Shor 1994 entwickelten Quanten-Algorithmus ist eine effiziente Faktorisierung großer Zahlen und Berechnung diskreter Logarithmen möglich. Damit wären RSA und DSA gebrochen.

Zwar benötigen solche Quantencomputer mehr als 2000 Qubits – heutige erreichen gerade einmal 127 (IBM, 2021). Aber es ist nur eine Frage der Zeit, bis es so weit ist. Um rechtzeitig gut untersuchte neue Verfahren zu etablieren, schrieb das NIST daher 2016 einen Wettbewerb für Post-Quantum-Algorithmen aus. Aus ursprünglich 69 Vorschlägen wählte das NIST am 05.07.2022 einen Kandidaten für Verschlüsselung und Key Exchange (CRYSTALS-KYBER) und drei für digitale Signaturen (CRYSTALS-Dilithium, FALCON und SPHINCS+) zur Standardisierung aus, die 2024 abgeschlossen werden soll. Vier weitere Verfahren nahm das NIST in die vierte Evaluationsrunde auf (vollständiger Bericht). Kurz darauf wurde eines davon, SIKE, am 30.07.2022 von Forschern der Universität Leuven gebrochen.

Nach 45 Jahren mit sicheren asymmetrischen Verfahren bricht nun eine Phase der Unruhe an – mit bisher noch ungewissem Ausgang.

Cloud Encryption

Der stärkste Vorbehalt gegen die Nutzung von Cloud-Diensten ist die Zugriffsmöglichkeit des Anbieters auf die verarbeiteten Daten – die in einigen Drittstaaten auch Nachrichtendiensten einen Datenzugang eröffnet. Davor schützt auch keine Datenverschlüsselung – denn während der Verarbeitung liegen die Daten und der Entschlüsselungsschlüssel offen im Arbeitsspeicher (RAM) des Servers. Abhilfe soll das am 19.07.2022 von Corey Sanders im Microsoft-Blog vorgestellte „Azure Confidential Computing“ schaffen. Dabei kommen spezielle Eigenschaften neuerer Prozessoren von AMD und Intel zum Einsatz (SME/SEV bzw. SGX): die Verschlüsselung aller vom Prozessor als Cache genutzten RAM-Bereiche. Damit liegen auch in einem Memory Dump Daten, Passwörter oder Schlüssel, die der Prozessor genutzt hat, nur verschlüsselt vor.

Sofern die Passwörter und Schlüssel für diese RAM-Verschlüsselung selbst in einem zugriffsgesicherten Bereich (Hardware Security Module, HSM) gehalten werden und die Verfahren keine Hintertür für behördlichen Zugriff haben, könnte eine solche Lösung den „zusätzlichen Garantien“ entsprechen, die der EuGH im Schrems-II-Urteil bei Verarbeitungen in datenschutzrechtlich unsicheren Drittstaaten fordert (SSN 10/2020).

Rechtswidrige Wächter-Modi

Am 19.07.2022 hat der Verbraucherzentrale Bundesverband (vzbv) bekanntgegeben, dass er Tesla wegen des (in den SSN 9+10/2021 vorgestellten) „Wächter-Modus“ im Model 3 verklagen wird. Dabei filmt das geparkte Fahrzeug mit den eingebauten Kameras die Umgebung; auf die Livebilder kann mit der Tesla Mobile App zugegriffen werden. Bei nahenden Passanten wird der Warnzustand aktiviert, in dem die Videobilder zusätzlich im Fahrzeug gespeichert werden.

Nach Ansicht des vzbv ist eine datenschutzkonforme Nutzung im öffentlichen Raum nicht möglich und die Datenverarbeitung damit unzulässig. Grundsätzlich bedürfe es dafür entweder einer Einwilligung der Passanten (praktisch nicht umsetzbar) oder eines überwiegenden Interesses des Fahrzeughalters oder -fahrers (bei anlassloser Überwachung nicht begründbar).

Auch bei dem anderen in den SSN 9+10/2021 vorgestellten „Wächter-Modus“ regt sich Widerstand: Am 13.07.2022 erklärte US-Senator Ed Markey nach einer Befragung von Amazon Ring das von über 2.100 US-Strafverfolgungsbehörden genutzte Angebot, direkten Zugriff auf die Geräte von Ring-Nutzern zu erhalten, für rechtswidrig. Zudem habe Amazon 2022 in elf Fällen Bildmaterial ohne Einwilligung der betroffenen Ring-Nutzer weitergegeben.

Nutzer solcher Wächter-Lösungen sollten sich nicht darauf verlassen, dass der Hersteller für die Einhal-

tung der datenschutzrechtlichen Anforderungen sorgt. Bußgeldbewehrt ist der rechtswidrige Betrieb – und verantwortlich der Betreiber. Das gilt nach der DSGVO auch für Privatpersonen.

Ampeln zur Klassifizierung

Die Forderung nach Informationsklassifizierung und angemessener Kennzeichnung sind seit jeher Bestandteil der Anforderungen der ISO 27002, wie schon des Vorgängers BS 7799-2. Bei der Umsetzung kann der Standard „Traffic Light Protocol (TLP)“ helfen, dessen Version 2.0 das Forum of Incident Response and Security Teams (FIRST) am 05.08.2022 veröffentlichte. Darin hat sich die CERT-Community auf eine einheitliche Nomenklatur für Vertraulichkeitsklassen geeinigt. Die Verwendung einheitlicher Bezeichnungen kann für die Kommunikation zwischen Organisationen hilfreich sein – z. B. indem Organisationen die FIRST-TLP adaptieren, ähnlich wie das BSI am 12.05.2022.

Big Brother Deutsche Bahn

Am 11.04.2022 veröffentlichten der Blogger Mike Kuketz und Peter Hense das vernichtende Ergebnis ihrer datenschutzrechtlichen Untersuchung der DB Navigator-App. So hält die Bahn 10 Dienstleister, darunter Adobe Analytics und Optimizely, für erforderliche Adressaten sämtlicher Daten, die im Rahmen einer Ticketbuchung erfasst werden.

Eine rechtliche Grundlage gebe es dafür nicht, denn um diese Verarbeitung zu vermeiden müssten Reisende ihr Ticket entweder am Automaten oder im Reisezentrum erwerben. Für den kurzfristigen Ticketkauf gebe es keine Alternative zur App, da Schaffner keine Tickets mehr im Zug verkaufen. Am 20.07.2022 teilte Kuketz mit, dass er jetzt gemeinsam mit digitalcourage die Bahn verklage, da die DB Navigator App erfasste Daten auch dann noch sendet, wenn in den Einstellungen „Nur erforderliche Cookies verwenden“ ausgewählt wurde. Die Klage kann man auf der Seite von digitalcourage unterstützen.

Leaky Forms

Auf dem diesjährigen 31. Usenix Security Forum (10.-12.08.2022) stellten vier Forscher aus Leuven, Nijmegen und Lausanne die Ergebnisse ihrer Mitte 2021 durchgeführten umfangreichen Studie zum rechtswidrigen Tracking von Daten in Web-Formularen vor. Dazu hatten sie mit eigens entwickelten Crawlern auf den 100.000 meistbesuchten europäischen und amerikanischen Webseiten je rund 50.000 Formularseiten identifiziert, auf denen E-Mail-Adressen abgefragt wurde. Trugen die Crawler dort eine Adresse ein, so wurde sie von 1.850 europäischen (3,7%) und 2.950 amerikanischen (5,9%) Servern ohne Einwilligung des Nutzers – d. h. vor der Betätigung des „Senden“-Knopfes – an den Tracker übertragen. Eine solche Übermittlung ist rechtswidrig – und kann obendrein Daten umfassen, deren Übermittlung gar nicht beabsichtigt war, wenn beispielsweise der „Autofill“-Mechanismus des Browsers verwendet wird. Ihre Datenbasis und die verwendete Software zur Identifikation der rechtswidrigen Tracker haben die Autoren auf Github veröffentlicht.

Secorvo News

Wenn nicht jetzt – wann dann?

1.700 Experten haben es schon – das T.I.S.P.-Zertifikat. Regelmäßig treffen sie sich zum Erfahrungsaustausch auf dem T.I.S.P.-Community-Meeting.

Falls Sie noch nicht dazu gehören: Vom **19.09. bis 23.09.2022** bieten wir Ihnen mit unserem T.I.S.P.-Seminar die nächste Gelegenheit, sich auf die Prüfung vorzubereiten. Mit Ihrer Anmeldung zum Seminar erhalten Sie vorab unser T.I.S.P.-Begleitbuch „Informationssicherheit und Datenschutz“. Wir freuen uns auf Sie!

Alle weiteren Seminarthemen und Termine unter https://www.secorvo.de/seminare.

Hokus Pokus Fidibus

Wie geht das – Entwicklung und Produktion von Hardware-Security-Modulen in Deutschland? Welche Herausforderungen sind damit verbunden – und wie werden die von einem der wenigen deutschen Hersteller von IT-Security Hardware gemeistert, der WIBU-SYSTEMS aus Karlsruhe? Das grenzt manchmal schon an Zauberei …

Erfahren Sie bei unserem kommenden KA-IT-Si-Event am **15.09.2022** aus erster Hand, welche Hürden bei der Entwicklung, den Multiplattform-Tests, der Beschaffung und der sicheren Produktion von Security Controllern „Made-in-Germany“ zu bewältigen sind. Wir erhalten die seltene Gelegenheit, die Fertigung zu besichtigen und Einblick in die automatisierten Prozesse des Downloads finaler Firmware, der Schlüsselerzeugung und optional individueller Schlüsselspeicherung für kundenspezifische Produkte zu bekommen. Die Spezialisten von WIBU-SYSTEMS und der Vorstand Oliver Winzenried stehen Ihnen dabei Rede und Antwort.

Im Anschluss haben Sie wie immer Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ – diesmal mit einem phänomenalen Blick auf den Schwarzwald (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)
27.-29.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
November 2022	
07.-11.11.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
07.-11.11.	ACM CCS 2022 (ACM/SIGSAC, Los Angeles/US)
09.-10.11.	T.I.S.P. Community Meeting (TeleTrusT e.V., Berlin)

Fundsache

TeleTrusT hat am 22.06.2022 einen Podcast zum "Stand der Technik in der IT-Sicherheit" veröffentlicht. Darin stellen Tomasz Lawicki (Leiter AK Stand der Technik) und Karsten U. Bartels (TeleTrusT Vorstand) die Methode zur Entwicklung der Handreichung "Stand der Technik", rechtliche Positionen und weitere Aspekte vor. Hörenswert.

Impressum

Secorvo Security News – ISSN 1613-4311

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

secorvo
security consulting

Secorvo Security News

August 2022

Deep Fake

Die technischen Möglichkeiten, Bilder, Videos und Sprache zu verfälschen, sind inzwischen gleichermaßen bekannt wie verbreitet. Mit ihrer Hilfe lassen sich biometrische Authentifikationsverfahren austricksen und „fake news“ erzeugen. Doch ist der Aufwand für praktisch nicht nachweisbare Fälschungen noch immer so hoch, dass sie zum Glück bisher isolierte Einzelerscheinungen sind – und bei ihrem Erscheinen schnell Zweifel an der Echtheit laut werden.

Ganz anders ist das bei Verfahren, die derzeit fast unbemerkt Einzug in unsere Lebenswirklichkeit halten: die KI-gesteuerte Erzeugung von Texten. Eine solche KI-Anwendung, die am 08.09.2020 durch einen Artikel des Guardian Furore machte, ist GPT-3 – eine KI der Firma OpenAI. Gefüttert wird sie mit Inhalten aus dem Internet und erzeugt zu einem vorgegebenen Thema kurze Notizen bis hin zu ganzen Büchern, die sogar an ausgewählte Schreibstile angepasst werden können. Sie sind stilistisch so elegant, dass sie mühelos als menschliche Werke durchgehen.

Die Wahrheit eines Sachverhalts kann GPT-3 allerdings nicht prüfen und ist daher auf eine Bewertung der Plausibilität angewiesen. Was aber könnte plausibler sein als eine sehr oft wiederholte Behauptung? GPT-3-Texte wiederholen also vor allem Verbreitetes – und verstärken damit selbst deren Plausibilität.

Wenn nun (was sicher bereits passiert) immer mehr Texte von solchen Automaten erzeugt werden, werden Plagiate, insbesondere bei wissenschaftlichen Arbeiten, zukünftig wohl kaum noch zu identifizieren sein. Vor allem aber werden Widerlegungen, die es heute schon schwer haben (wie z. B. der Mythos vom hohen Eisengehalt von Spinat), schon bald nicht mehr wahrgenommen werden – und Ähnliches könnte für neue Erkenntnisse gelten, denn die haben ja gerade die Eigenschaft, selten publiziert worden zu sein. KI-Fakes werden die Welt oberflächlicher machen. Und uns dümmer.

Inhalt

secorvo
security consulting

Security News

Video-Fake-Ident

Der Chaos Computer Club meldete am 10.08.2022, dass es ihm gelungen sei, mehrere videobasierte Online-Identifizierungsverfahren zu täuschen. Schon am Vortag hatte die Gematik den Vorgang zum Anlass genommen, die Nutzung von VideoIdent bis auf Weiteres zu untersagen.

Nach dem Untersuchungsbericht von Martin Tschirsich bedurfte es für die Angriffe keiner kostenintensiven Hard- oder Software. Es genügte, vor der Kamera ein manipuliertes Video abzuspielen, in dem das Passfoto auf dem Ausweis ersetzt worden war. Die Manipulationen wurden von keiner der sieben getesteten Lösungen erkannt. Zwar nennt der Bericht keine Hersteller, es ist aber zu befürchten, dass die Angriffe bei den weitaus meisten Video-Ident-Lösungen funktionieren.

Ursache ist, dass viele optische Sicherheitsmerkmale des Personalausweises am übertragenen Bild nicht geprüft werden können. Ein Hologramm ist beispielsweise nur zweidimensional zu sehen, und dem übertragenen Bild kann man nicht trauen, da das Equipment unter der Kontrolle eines Angreifers betrieben werden kann. Somit können das Video-Bild der Person oder die auf dem Ausweis angezeigten Daten „on the fly" verändert werden. Das bietet bestenfalls für einfache Anwendungen ein angemessenes Sicherheitsniveau.

Unverständlich ist, warum die eID-Funktion des vor 12 Jahren eingeführten „neuen Personalausweises" nicht selbstverständlich für derartige Anwendungen genutzt wird, obwohl die Zertifikatsinfrastruktur von den Bürgern mit der Personalausweisgebühr bereits teuer bezahlt wurde.

Pimp my Tesla

Die Anzahl von Kameras auf und an den Straßen Deutschlands hat sich, Tesla sei Dank (SSN 07/2022), in den letzten Jahren vervielfacht. Jetzt sind an einem Erprobungsfahrzeug montierte Kameras VW zum Verhängnis geworden: Der Landesbeauftragte für den Datenschutz Niedersachsens verhängte am 26.07.2022 ein Bußgeld in Höhe von 1,1 Mio. €, da die Kameras nicht gekennzeichnet waren.

Wird das Verkehrsgeschehen um das Fahrzeug herum aufgezeichnet, unterliegen auch Kameras an und in Fahrzeugen der Kennzeichnungspflicht nach Art. 13 DSGVO. Das gilt auch für Rückfahrkameras, Kameras von Einparkassistenten und teilautonomen Fahrzeugen. Eine interessante Vorstellung, dass Tesla-Fahrer zukünftig ihre acht Außenkameras einzeln kennzeichnen müssen – inklusive Angabe der für die Verarbeitung verantwortlichen Stelle…

Kein Konzernprivileg

Für einen Gehaltsvergleich übermittelte ein Unternehmen Arbeitsvertrag, Name, Einstellungsdatum, Gehalt und weitere Angaben zu einer Mitarbeiterin an eine Tochtergesellschaft. Eine Einwilligung der Mitarbeiterin wurde nicht eingeholt und ihr Widerspruch nicht beachtet. Ein teurer Fehler, denn die DSGVO kennt kein Konzernprivileg: Das LG Bochum widersprach nicht nur dem geltend gemachten überwiegenden Interesse des Unternehmens, sondern bezweifelte auch die Erforderlichkeit der Übermittlung, da die Vergleichswerte auch mit pseudonymisierten Daten hätten erstellt werden können.

Mit dem Ziel einer abschreckenden Wirkung sprach das LG Bochum der Mitarbeiterin 8.000 € Schadensersatz für den durch die rechtswidrige Verarbeitung erlittenen immateriellen Schaden zu; das OLG Hamm reduzierte diesen auf 4.000 €.

Ob ein Schadensersatz überhaupt eine abschreckende, d. h. sanktionierende Wirkung haben oder vielmehr nur zum Schadensausgleich dienen darf, ist Gegenstand von Vorlagefragen des AG München vom 03.03.2022 an den EuGH.

Viele Daten sind besonders

Am 01.08.2022 hat der Europäische Gerichtshof entschieden, dass die Definition der besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO weit auszulegen ist.

Anlass war die Beurteilung des litauischen Gesetzes zur Korruptionsbekämpfung über den Ausgleich öffentlicher und privater Interessen im öffentlichen Dienst. Danach müssen bestimmte Personen eine Erklärung über private Interessen abgeben – mit Angabe sowohl des eigenen als auch des Namens des Ehepartners. Laut EuGH lässt sich daraus mittels „gedanklicher Kombination oder Ableitung" ohne Weiteres auf die sexuelle Orientierung von Ehepaaren schließen. Demnach liegt eine Verarbeitung besonderer Kategorien personenbezogener Daten bereits dann vor, wenn diese Daten „geeignet sind, die sexuelle Orientierung einer natürlichen Person indirekt zu offenbaren." Deren Verarbeitung ist grundsätzlich untersagt und nur in Ausnahmefällen zulässig.

Die Argumentation des EuGH ist in zahlreichen weiteren Fällen anwendbar, da personenbezogene Daten häufig erlauben, indirekt Rückschlüsse auf besondere Kategorien personenbezogener Daten zu ziehen, wie z. B. die Bestellung koscheren Essens im Flugzeug oder der Schlüsseleintrag auf dem Führerschein (Brille, Hörgerät oder Prothese).

Wegen des hohen Schutzniveaus dieser Daten können von der weiten Interpretation des EuGH zahlreiche Datenverarbeitungen betroffen sein, bei denen die Verantwortlichen bisher davon ausgehen, lediglich „normale“ personenbezogene Daten zu verarbeiten. Das kann bedeuten, dass eine Datenschutz-Folgenabschätzung durchgeführt und ergänzende Maßnahmen zum Schutz dieser Daten ergriffen werden müssen.

Jagd auf Cookie-Banner

Die Initiative „My Privacy is None of Your Business“ (noyb) hat am 09.08.2022 angekündigt, erneut tausende Webseiten zu scannen, die Consent Management Platforms (CMP) wie OneTrust, TrustArc, Cookiebot, Usercentrics oder Quantcast verwenden.

Bereits am 31.05.2021 (SSN 6/2021) hatte noyb an 560 Unternehmen, die auf ihren Webseiten das CMP „OneTrust“ einsetzen, einen Beschwerdeentwurf samt Schritt-für-Schritt Anleitung zur rechtskonformen Anpassung ihrer Cookie-Banner versandt und eine 60-tägige Schonfrist zur Nachbesserung gewährt. 24 % aller angemahnten Verstöße wurden innerhalb dieser 60 Tage behoben, die meisten Unternehmen kamen der Aufforderung jedoch nicht oder nicht vollständig nach. Daraufhin reichte noyb 226 Beschwerden bei 18 Aufsichtsbehörden ein. Daraufhin wurden 42 % der verbleibenden Verstöße innerhalb von 30 Tagen korrigiert.

Webseitenbetreiber, die ihre Cookie-Banner auf Rechtskonformität prüfen möchten, finden u. a. beim Landesbeauftragten für Datenschutz und Informationssicherheit Baden-Württemberg hilfreiche Hinweise und Beispiele.

Verhältnismäßig

Die Frage der Erforderlichkeit einer Ende-zu-Ende-Verschlüsselung wird auch zwischen den Aufsichtsbehörden für den Datenschutz kontrovers diskutiert. Am 15.07.2022 hat nun das VG Frankfurt in der Frage, wann eine Ende-zu-Ende-Verschlüsselung elektronischer Kommunikation notwendig ist und wann eine Transportverschlüsselung ausreicht, einen Beschluss gefasst.

Sollen personenbezogene Daten übermittelt werden, müssen gemäß Art. 32 DSGVO und Erwägungsgrund 83 zur Gewährleistung von Sicherheit und Vertraulichkeit der Stand der Technik, die Implementierungskosten, Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die (je nach Fall ggf. unterschiedliche) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geprüft werden.

Das VG Frankfurt hat nun den Stand der Technik als das ausschlaggebende Kriterium für die Anforderungen an die angemessene Verschlüsselung gesetzt und entschieden, dass auch eine Transportverschlüsselung ausreichend sein kann, wenn es keine strengeren gesetzlichen Vorgaben gibt und die Sensibilität der verarbeiteten Daten dies zulässt. Damit geht es weiter als die bereits differenzierende Orientierungshilfe des AK Technik zu „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ vom 13.03.2020.

Secorvo News

T.I.S.P. und IT Security Insights

In der Woche **19.–23.09.2022** bieten wir Ihnen mit dem T.I.S.P.-Seminar die nächste Gelegenheit zur Zertifizierung Ihrer Kenntnisse in der IT-Sicherheit.

In der darauffolgenden Woche können Sie Ihre Kenntnisse in aktuellen Themen der Informationssicherheit und des Datenschutzes auf dem Seminar IT Security Insights auffrischen (**27.–29.09.2022**). Wir freuen uns auf Ihre Anmeldung!

Hokus Pokus Fidibus

Wie geht das – Entwicklung und Produktion von Hardware-Security-Modulen in Deutschland? Welche Herausforderungen sind damit verbunden – und wie werden die von einem der wenigen deutschen Hersteller von IT-Security Hardware gemeistert, der WIBU-SYSTEMS aus Karlsruhe? Das grenzt manchmal schon an Zauberei …

Erfahren Sie bei unserem kommenden KA-IT-Si-Event am **15.09.2022** aus erster Hand, welche Hürden bei der Entwicklung, den Multiplattform-Tests, der Beschaffung und der sicheren Produktion von Security Controllern „Made-in-Germany“ zu bewältigen sind.

Wir erhalten die seltene Gelegenheit, die Fertigung zu besichtigen und Einblick in die automatisierten Prozesse des Downloads finaler Firmware, der Schlüsselerzeugung und optional individueller Schlüsselspeicherung für kundenspezifische Produkte zu bekommen. Die Spezialisten von WIBU-SYSTEMS und der Vorstand Oliver Winzenried stehen Ihnen dabei Rede und Antwort.

Im Anschluss haben Sie Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking“ mit einem phänomenalen Blick auf den Schwarzwald (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2022	
19.-23.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
26.-30.09.	Informatik 2022 (GI, Hamburg)
27.-29.09.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
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)

Fundsache

Der Beirat Digitaler Verbraucherschutz des BSI hat Empfehlungen zur Kommunikation über Passwörter veröffentlicht. Danach sollen Unternehmen ihre Online-Dienste mit 2FA-Authentizierung absichern und Nutzern verständliche Passwort-Regeln vermitteln; Nutzer wiederum sollen angehalten werden, Passwörter in Passwort-Managern zu speichern und nicht mehrfach zu verwenden.

Impressum

Secorvo Security News – ISSN 1613-4311

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

secorvo
security consulting

Secorvo Security News

September 2022

Androide Gegner

Noch sind sie nicht die Regel, aber vereinzelt dürften sie bereits vorkommen: mit künstlicher Intelligenz optimierte Angreifer.

Das wachsende Angebot Cloud-basierter – also schnell und kostengünstig skalierbarer – KI-Systeme bietet immer mehr leistungsfähige Möglichkeiten, Angriffe auf IT-Systeme mit maschinellem Lernen zu verbessern.

Dass Angreifer die Suche nach bekannten Schwachstellen mit Crawlern automatisieren, ist lange bekannt. Auch die mühsame manuelle Suche nach Schwächen in der Eingabe-Validierung von Web-Anwendungen wird seit vielen Jahren mit Fuzzy-Systemen maschinell unterstützt.

Doch inzwischen könnten KI-Systeme auch gänzlich neue Schwachstellen identifizieren – vorausgesetzt, man würde sie mit geeigneten Samples „füttern". Ist der Source Code (wie z. B. bei Open-Source-Lösungen) zugänglich, funktioniert das zumindest im Labor.

Aber auch herkömmliche Angriffsmethoden lassen sich mit KI-Systemen perfektionieren. So können „Textgenerierungs-KIs" bereits heute beispielsweise an den Stil eines bestimmten Absenders adaptierte E-Mails formulieren, die von dessen eigenen nicht zu unterscheiden sind (siehe SSN 8/2022). Ein ideales Hilfsmittel für Spear-Phishing-E-Mails – und eine perfekte Methode, um CEO-Fraud zu optimieren. Schlimmer noch: Mit Stimm-Samples eines CEO trainiert kann ein KI-gesteuerter Sprachgenerator (siehe SSN 10/2020) einen täuschend echten Anruf des CEO vorspielen, sodass selbst engste Mitarbeiter die Falle nicht erkennen. Ganz ähnlichen Angriffen sehen sich heute biometrische Authentifikationsverfahren ausgesetzt. KI-Systeme können Bilder, Videos oder auch Fingerabdrücke erzeugen, die sich von echten nicht unterscheiden lassen.

Auch wenn KI-Systeme den Turing-Test noch nicht bestehen – in der Hand von Angreifern sind sie bereits ein gefährlicher Gegner.

Inhalt

secorvo
security consulting

Security News

Bug-Bounty-Marketing

Finden Forscher Schwachstellen in Software-Produkten, so erfolgt oft eine „responsible disclosure", sprich: eine Vorab-Benachrichtigung des Herstellers, die diesem Zeit einräumt, die Schwachstelle vor der Veröffentlichung zu beheben. Nach Ablauf dieser Karenzzeit werden Ursache und Auswirkungen der Schwachstelle meist als CVE (Common Vulnerabilities and Exposures) veröffentlicht. Um Nutzer der Software vor der Schwachstelle zu warnen, erfolgt die Veröffentlichung auch dann, wenn der betroffene Hersteller nicht reagiert hat. Inzwischen wird die Suche nach Schwachstellen von einigen Unternehmen durch Bug-Bounty-Programme gefördert: Wer eine Schwachstelle meldet, erhält eine kleine oder auch etwas größere Prämie. Das ist erstmal alles nicht neu (siehe SSN 12/2019).

Findet man zu einem Produkt wenige oder sogar keine CVEs, so kann das bedeuten, dass sich noch niemand die Mühe gemacht, es zu untersuchen. Bei verbreiteten Produkten ist es aber wahrscheinlicher, dass keine (oder nur wenige) Schwachstellen gefunden werden konnten – und das spricht für die Qualität des Produkts.

Wie die Forscher von modzero am 22.08.2022 veröffentlichten, gibt es allerdings noch eine dritte Möglichkeit: Jemand hat das Produkt untersucht, Schwachstellen festgestellt, sie dem Hersteller gemeldet, eine Prämie erhalten – sich aber über die Bestimmungen des Bug-Bounty-Programms verpflichtet, keine CVE zu veröffentlichen. Das Fehlen von CVEs sagt daher inzwischen leider wenig über die Sicherheit eines Produktes aus – Bug-Bounty-Programme als irreführendes Marketing…

Nmap-Jubiläum

Unglaublich, aber wahr: Nmap, der wohl bekannteste Netzwerk-Portscanner („Network Mapper"), wird 25 Jahre alt. Damit ist Nmap eines der (wenn nicht das) am längsten fortlaufend gepflegte Werkzeug für IT-Sicherheitsfachkräfte, Netzwerker und Administratoren. Die Entwicklung vom einfachen Portscanner über die Erkennung von Diensten und Betriebssystemen bis zur Bedienung über eine grafische Oberfläche – die Liste der Erweiterungen im Changelog ist lang. Nach wie vor kann man performant komplette Netzbereiche durchforsten und so bekannte und ggf. auch nicht zuzuordnende IT-Systeme und Netzwerk-Dienste finden.

Mit Nmap gelingt das genauso zuverlässig (und kostenlos) auch in der OT (Operational Technology) – zur Identifikation von im Netz erreichbaren Systemen muss man auch heute keine komplexen und kostspieligen Werkzeuge beschaffen. Wer wissen will, welche Systeme und Dienste in den eigenen Netzen – seien es Leittechnik oder Bürokommunikation, die DMZ oder der „Blick" vom Internet auf das eigene Netz – dem empfehlen wir der Einsatz von Nmap. Wir gratulieren, Fyodor!

Missbräuchliche Abmahnungen

Seit August erfasst eine Abmahnwelle Unternehmen und Privatpersonen in Österreich und Deutschland, die auf ihren Webseiten bei Google gehostete Fonts eingebunden haben. Darin werden – mit Bezug auf das Urteil des LG München (siehe SSN 6/2022) – Schadensersatzforderungen in Höhe von 100-200 € nach Art. 82 DSGVO geltend gemacht.

Tatsächlich sind die Schadensersatzansprüche in den meisten Fällen unbegründet, da der Anspruchsteller zur Ermittlung des Einsatzes von Google Fonts einen WebCrawler nutzt und die Abmahnungen automatisiert verschickt. Der Anspruchsteller war demnach nie persönlich auf den Webseiten, womit der Tatbestand des Art. 82 Abs. 1 DSGVO nicht erfüllt ist, da er nicht als natürliche Person betroffen war; die Schadensersatzforderung selbst erfolgt rechtsmissbräuchlich. In Österreich erstatteten daher Anwälte von Betroffenen Anzeige wegen gewerbsmäßigen Betrugs.

Der Fall zeigt, dass man beim Erhalt von Abmahnungen nicht vorschnell einen geforderten Schadensersatz direkt begleichen sollte. Wir empfehlen in einem solchen Fall Ruhe zu bewahren, zunächst die Begründetheit des Anspruchs genau zu prüfen und ihn gegebenenfalls zurückzuweisen.

Davon unbenommen sollte man allerdings auf der eigenen Webseite verwendete Google Fonts tatsächlich nicht einbinden, sondern auf dem eigenen Server hosten – Anleitungen dafür und hilfreiche Tools finden sich zahlreich im Internet.

Déjà-vu

Am 12.09.2022 stellte Martin Rost auf der Sommerakademie des ULD Schleswig-Holstein Neuerungen beim Standard Datenschutzmodell (SDM) sowie die Ergebnisse einer Umfrage zur Nutzung des SDM vor. Die wichtigste (und begrüßenswerte) Neuerung: Im Baustein 41 wurde eine aus dem IT-Grundschutz stammende Soll-Ist-Prüfung aufgenommen. Die in der Umfrage geäußerten Erfahrungen der Nutzer des SDM decken sich allerdings mit unseren Praxiserfahrungen: Es ist sehr aufwändig, die beschriebenen Maßnahmen zu prüfen und umzusetzen.

Das klingt nach einem déjà-vu. Im Jahr 2018 hatte das Bundesamt für Sicherheit in der Informations-

technik (BSI) aus denselben Gründen nach 15 Jahren die umfänglichen Maßnahmenvorschriften im IT-Grundschutz-Katalog auf Anforderungen an die Informationssicherheit in Form des IT-Grundschutz-Kompendiums umgestellt. Das BSI hatte (endlich) erkannt, dass Betreiber von Managementsystemen die operative (und unternehmerische) Freiheit benötigen, risikobezogen über Maßnahmen und deren Umsetzung zu entscheiden.

Im CON.2-Baustein des IT-Grundschutz-Kompendiums referenziert das BSI auf das SDM, aber es hat wohl geahnt, dass man Unternehmen besser nicht zur Umsetzung zwingt. Ein weiser Schritt, denn es gibt auch andere, kostengünstigere Wege, ein wirksames Datenschutz-Managementsystem (DSMS) aufzubauen, als alle Gewährleistungsziele mit Maßnahmenbergen zu erschlagen. Die Vorgehensweise nach dem SDM ist grundsätzlich gut, allerdings sollten die Bausteine wie beim „neuen" Grundschutz praxistauglicher gestaltet werden.

Falsch verstandene Transparenz

Seit dem 01.08.2022 sind die Inhalte des „Gemeinsamen Registerportals der Länder" kostenfrei abrufbar. Das ist das Ergebnis der unmittelbaren Anwendung der „Digitalisierungsrichtlinie" der EU (Richtlinie 2019/1151) vom 20.06.2019 durch das Gesetz zur Umsetzung der Digitalisierungsrichtlinie (DiRUG). Dem Inkrafttreten folgte ein „Aufschrei", weil nun über das Registerportal auch Dokumente eingesehen werden können, die zuvor nicht ohne weiteres zugänglich waren – wie die Privatadressen von Unternehmern, Geschäftsführern und Aufsichtsräten oder deren gescannte Unterschriften. Frei verfügbare Daten, die geradezu zum Missbrauch einladen.

Ziel der Digitalisierungsrichtlinie ist es, digitale Unternehmensgründungen zu vereinfachen und durch Transparenz Missbrauch und Betrug vorzubeugen. Klare Vorgabe des Gesetzgebers ist es, dass dabei die Grundsätze des Datenschutzes nach der DSGVO zu berücksichtigen sind. Bei der deutschen Umsetzung ist das zumindest teilweise schiefgegangen, da die beteiligten Registergerichte offensichtlich keine Interessenabwägung zwischen den schutzwürdigen Interessen der Unternehmer und der Sicherstellung von Vertrauenswürdigkeit durch Transparenz vorgenommen haben.

Fein raus sind lediglich Unternehmen, die ihre Dokumente vor dem 01.01.2007 eingereicht haben – die liegen nicht digital vor und sind daher auch nicht online abrufbar. Es ist zu hoffen, dass die Regelung einer Überprüfung unterzogen wird.

Secorvo News

Teamverstärkung

Seit dem 01.09.2022 verstärkt uns Oliver Oettinger in den Sicherheitsthemen Public Key-Infrastrukturen und Forensik. Herzlich willkommen im Secorvo-Team!

T.I.S.P. und BSI Vorfall-Experte

In der Woche **14.–18.11.2022** bieten wir Ihnen mit dem T.I.S.P.-Seminar die letzte Gelegenheit in diesem Jahr zur Zertifizierung Ihrer Kenntnisse in der IT-Sicherheit. Nach Eingang Ihrer Anmeldung erhalten Sie das von Secorvo verfasste Begleitbuch zum T.I.S.P. zur Vorbereitung auf das Seminar und die anschließende Prüfung. Wir empfehlen eine baldige Anmeldung.

Unser letztes Seminarangebot in diesem Jahr ist die Vorbereitung auf die Zertifizierung zum BSI Vorfall-Experten nach dem Curriculum des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in der Kalenderwoche 48 (**29.11.–01.12.2022**). Wir freuen uns auf Ihre Anmeldung!

Die Seminar-Programme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Webseite unter https://www.secorvo.de/seminare.

Gotcha.

Das Nachverfolgen oder das Erstellen von Profilen zu Besuchern von Webseiten mittels Cookies ist bekannt und bekommt öffentliche Aufmerksamkeit – bei E-Mails haben Tracking und Profiling hingegen bisher kaum Aufmerksamkeit erfahren, obwohl diese bei Newslettern und deren Inhalten regelmäßig angewendet werden.

Auf dem kommenden Online-Event der KA-IT-Si am 03.11.2022 stellen Milan Burgdorf und Christian Blaicher (Secorvo) exemplarisch die technischen Möglichkeiten und Umsetzungen für Tracking und Profiling in E-Mails vor und beleuchten die rechtlichen Rahmenbedingungen für deren Verwendung. Wir freuen uns auf Ihre Teilnahme.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Oktober 2022	
04.-06.10.	heise devSec 2022 (dpunkt verlag, heise, Karlsruhe)
17.-19.10.	IDACON 2022 (WEKA-Akademie, München)
24.-26.10.	ISSE 2022 (IEEE, Wien/A)
25.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH)
25.-27.10.	it-sa 2022 (NürnbergMesse GmbH, Nürnberg)
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)

Fundsache

Die Landesdatenschutzbeauftragte für den Datenschutz Niedersachsen hat im August 2022 FAQ zur Auftragsverarbeitung nach Art. 28 DSGVO veröffentlicht, die auf 15 Seiten lebensnahe Antworten zu Fragen rund um AV-Verträge geben.

Impressum

Secorvo Security News – ISSN 1613-4311

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

secorvo
security consulting

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.

Inhalt

secorvo
security consulting

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

secorvo
security consulting

Secorvo Security News

November 2022

Festgebissen

Was die Animosität ausgelöst hat, wird sich kaum mehr feststellen lassen. Sicher ist: Die deutschen Aufsichtsbehörden haben sich auf Microsoft eingeschossen, wie die aktuelle Entscheidung der Datenschutzkonferenz (DSK) zu MS 365 vom 24.11.2022 belegt. Wie berechtigt die Kritik auch einmal gewesen sein mag: Sie bewirkte schon vor 20 Jahren einen Strategiewechsel bei Microsoft. Nicht nur, dass Microsoft sich bereits 2007 (!) beim ULD mit dem „Update Service 6.0“ und „WSUS 2.0“ für ein Datenschutz-Gütesiegel qualifizierte. Microsoft war auch der erste amerikanische Software-Riese, der 2014 mit auf das EU-Recht abgestimmten Verträgen für Office 365 auf Servern in Irland warb – lange bevor Cisco, Amazon oder Google auch nur das Problem verstanden hatten. Secorvo war seitdem bei vielen Unternehmen an der Abstimmung von MS 365-Verträgen gutachterlich oder mit einer DSFA beteiligt, und ich erinnere mich gut an meine eigene Überraschung über die hohe Qualität und Transparenz der Unterlagen von Microsoft. Seitdem hat Microsoft wiederholt nachgelegt, z. B. mit der Reaktion auf das Schrems-II-Urteil (New steps to defend your data und Initiative Tech fit 4 Europe) oder der Ankündigung einer „EU Data Boundary“ für die MS-Cloud am 06.05.2021. Auch zum CLOUD Act hat Microsoft Position bezogen und bemüht sich um möglichste Transparenz, z. B. durch Veröffentlichung aller Law Enforcement Requests.

Man mag argwöhnen, dass das substanzloses Marketing-Geklapper ist. Aber ist das plausibel? Anders als die US-Internet-Giganten lebt Microsoft nicht von Nutzerdaten. Im Gegenteil: Ein einziger begründeter Verdacht, dass Microsoft trotz seiner Zusicherungen Kundendaten missbraucht, würde den gesamten europäischen Markt zusammenbrechen lassen. Dem Datenschutz wäre mehr gedient, wenn die DSK sich endlich die erklärten Feinde des Datenschutzes vornehmen würde, anstatt das erkennbare Bemühen Microsofts mit fadenscheinigen Einwänden zu entmutigen.

Inhalt

secorvo
security consulting

Security News

Abgelaufen

Eine Möglichkeit, die Übermittlung personenbezogener Daten in Drittländer (also Ländern außerhalb des europäischen Wirtschaftsraums) ohne ein anerkannt gleichwertiges Datenschutzniveau rechtskonform zu gestalten ist der Abschluss eines Vertrags nach den von der EU Kommission vorgegebenen Standardvertragsklauseln. Die „alten" Standardvertragsklauseln aus dem Jahr 2001 wurden als Folge des Schrems-II-Urteil des EuGH mit Durchführungsbeschluss 2021/914 vom 04.06.2021 abgelöst (siehe SSN 6/2021). Bis zum 27.12.2022 müssen alle bestehenden Verträge auf die neuen Standardvertragsklauseln für internationalen Datentransfer umgestellt werden. Altverträge werden nach dem zweiten Weihnachtstag automatisch unwirksam – und damit die betroffene Datenübermittlung rechtswidrig.

Abgesichert

Die wachsende Bedeutung des Schutzes von Software Supply Chains wurde erst kürzlich durch die Veröffentlichung des Enduring Security Frameworks der NSA vom 24.08.2022 deutlich. Dabei spielen Code-Signaturen zum Schutz der Authentizität und Integrität von Software eine zentrale Rolle. Doch bis vor kurzem galten für Code-Signing noch Bedingungen, die denen der „Prä-LetsEncrypt-Ära" für Web-Zertifikate entsprachen: kompliziert, aufwändig, teuer. Besonders Open-Source-Entwickler scheuten den Aufwand zur Schlüsselverwaltung und Beschaffung von Zertifikaten. Das könnte sich nun ändern: Das am 17.11.2022 von Newman, Meyers und Torres-Arias veröffentlichte Open-Source-Projekt „Sigstore" – inspiriert durch Let's Encrypt – könnte die Hürden für Code-Signaturen deutlich senken. Dahinter steckt eine Sammlung von Werkzeugen, mit deren Hilfe Code(fragmente) extrem einfach signiert und zur Prüfung in Transparency Logs veröffentlicht werden können. Unter der etwas irreführenden Bezeichnung „keyless signing" arbeitet Sigstore mit Einmalschlüsseln, für die nach einer Bestätigung der Identität des Entwicklers über OpenID-Connect ein kurzlebiges Zertifikat ausgestellt wird. Mit diesem kann ein Codefragment signiert, im Log veröffentlicht und von jedermann auf Gültigkeit überprüft werden. Sigstore übernimmt das Schlüsselmanagement für den Entwickler. Dieser muss sich lediglich um den Schutz seiner OpenID kümmern.

Abgemeldet

Der Messenger-Dienst WhatsApp bedient sich bekanntlich (SSN 4/2016) am Adressbuch des Smartphones und lädt auch die Namen und Telefonnummern von Personen hoch, die weder bei WhatsApp noch bei Instagram oder Facebook ein Benutzerkonto haben. Zu diesen Personen erstellt Meta ein sogenanntes Schattenprofil.

Bisher waren die Möglichkeiten begrenzt, das zu verhindern. Verwehrt man WhatsApp den Adressbuchzugriff, wird bei jeder Nachricht nur noch die Telefonnummer des Absenders angezeigt – eine erhebliche Komforteinbuße.

Zwar steht Betroffenen nach der DSGVO ein Recht auf Löschung zu, jedoch werden die Daten nach einer Löschung beim nächsten Adressbuchabgleich erneut an Meta übermittelt. Und der Versand von Unterlassungserklärungen an alle eigenen Telefonbuchkontakte ist keine besonders freundschaftserhaltende Option.

Am 31.10.2022 berichtete Shona Ghosh bei Businessinsider, dass Meta offenbar seit Mai 2022 „Nicht-Kunden" eine Möglichkeit bietet, im globalen Meta-Adressbuch nach der eigenen Telefonnummer oder E-Mail-Adresse zu suchen – und sie auf Wunsch löschen und in eine „Blacklist" aufnehmen zu lassen. Der Link ist in den „Informationen für Personen, die keine Meta-Produkte nutzen" versteckt – im Absatz „Klicke hier, wenn du eine Frage zu den Rechten hast, die dir möglicherweise zustehen." Irreführender geht es kaum.

Abgemahnt

Die systematischen und automatisierten Abmahnungen von Webseitenbetreibern wegen der Einbindung von Google Fonts (SSN 8/2022) reißen nicht ab. Neuerdings enthalten einige Abmahnschreiben neben Schmerzensgeldanspruch und Gebührenrechnung auch noch ein Auskunftsersuchen.

Zwar sind Zweifel angebracht, dass die Erheblichkeitsschwelle für die Geltendmachung eines Schadensersatzanspruchs überschritten ist (vgl. OLG Frankfurt/Main, Urteil v. 30.06.2022, 16 U 229/20). Einem Auskunftsersuchen hingegen ist unabhängig davon nachzukommen. Allerdings muss der Betroffene dafür seine Identität nachweisen. Stellt sich jedoch heraus, dass die Berufung auf die Betroffenenrechte missbräuchlich erfolgt, besteht auch keine Auskunftspflicht.

Abgelehnt

Am 24.11.2022 veröffentlichte die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) eine Zusammenfassung des Berichts zum datenschutzkonformen Einsatz von Microsoft 365 und stellt fest, „dass der Nachweis von Verantwortlichen, Microsoft 365 da-

tenschutzrechtskonform zu betreiben, (...) nicht geführt werden kann." Kernpunkt der Kritik ist weiterhin die Datenverarbeitung von Microsoft für legitime Geschäftszwecke und die angebliche Unmöglichkeit, der Rechenschaftspflicht als Auftragsverarbeiter beim Einsatz von Microsoft 365 wegen intransparenter Datenverarbeitungen durch Microsoft nachzukommen.

Hier verliert die DSK völlig aus dem Blick, welche Anforderungen vernünftigerweise an eine Auftragsverarbeitung zu stellen sind. Dass ein Unternehmen zur Erfüllung der Rechenschaftspflicht seines Auftraggebers sämtliche Datenverarbeitungen und damit auch gegebenenfalls Geschäftsgeheimnisse offenlegen soll, ist nicht nachvollziehbar. Unberücksichtigt bleibt auch, dass Microsoft eine bestimmte Menge an Diagnose- und Telemetriedaten verarbeiten muss, um die angebotenen Dienste überhaupt vertragsgemäß erbringen zu können. Warum die DSK zudem nicht die angekündigten Neuerungen in Sachen EU Data Boundary abgewartet hat, ist nicht zu verstehen.

Microsoft hat in einer Stellungnahme bereits auf die Verlautbarung reagiert und die Kritik (erwartungsgemäß) zurückgewiesen. Für Verantwortliche aus dem öffentlichen Sektor bringt das DSK-Papier viel Arbeit mit sich, wenn sie Microsoft 365 dennoch datenschutzkonform einsetzen möchten – möglich bleibt das jedoch, aller Kritik zum Trotze.

Abgestraft

Im Jahr 2018 hatten 40 (!) US-amerikanische Bundesstaaten Google wegen der heimlichen Sammlung von Standortdaten verklagt. Auslöser war ein Bericht von Keith Collins vom 21.11.2017, in dem er aufdeckte, dass Android seit Anfang 2017 auch bei abgeschalteten Location Services und sogar ohne eingelegte SIM-Karte Standortinformationen in Gestalt der Cell ID der Mobilfunkzellen in Reichweite sammelt und an Google übermittelt, sobald das Smartphone wieder online ist.

Nach vier Jahren wurde Google nun am 14.11.2022 zur Zahlung einer Geldstrafe von 391,5 Mio. US$ verurteilt – ein historisches Urteil, nicht nur wegen der Höhe der Strafe, sondern weil es zeigt, dass sich auch in den USA langsam eine Sensibilität für die Schutzwürdigkeit der Privatsphäre entwickelt.

Secorvo News

E-Mail-Tracking

Das Nachverfolgen (Tracking) von Webseitenbesuchen und die Erstellung von Besucherprofilen stehen schon lange im Fokus des Datenschutzes und müssen von Anbietern via Cookie-Banner transparent gemacht werden. Tracking und Profiling bei E-Mails sind hingegen bisher der Aufmerksamkeit von Aufsichtsbehörden entgangen – obwohl sie bei E-Mail-Newslettern inzwischen üblich sind. Meist erfolgt das heimlich – und verstößt somit gegen geltendes Datenschutzrecht.

Am 03.11.2022 gaben Christian Blaicher und Milan Burgdorf beim KA-IT-Si-Event „Gotcha. E-Mail-Tracking und -Profiling" einige vertiefte technische und rechtliche Einblicke in das Thema. Dabei ging es einerseits darum, wie Unternehmen E-Mail Tracking und Profiling innerhalb der Grenzen der DSGVO und des TTDSG rechtskonform gestalten können. Andererseits wurde erläutert, wie sich Empfänger solcher E-Mails sowohl rechtlich als auch technisch davor schützen können. Die Referenten haben das Wichtigste in einem Handout zusammengefasst.

Sollten Sie den Vortrag verpasst haben: Christian Blaicher wird zu dem Thema auf der DFN-Konferenz „Sicherheit in vernetzten Systemen" am 09.02.2023 um 14 Uhr in Hamburg vortragen.

Seminarprogramm 2023

Seit Ende November ist der Secorvo-Seminarkalender 2023 online – just in time für Ihre frühzeitige Weiterbildungsplanung im kommenden Jahr.

Lernen wird überbewertet

Vor rund einem Jahr sorgte die Schwachstelle log4j für erhebliche Aufregung. Der Auslöser ist mittlerweile beseitigt, und viele der betroffenen Softwareprodukte wurden 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 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 Vortrag „Log4j und was wir (nicht) daraus gelernt haben" zeigen wird. Wir freuen uns auf einen kurzweiligen und interessanten Abend mit Ihnen (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Dezember 2022	
05.-08.12.	Black Hat Europe 2022 (Blackhat, London/UK)
08.12.	Lernen wird überbewertet (KA-IT-Si, virtuell)
Januar 2023	
20.-22.01.	ShmooCon 2023 (The Shmoo Group, Washington/US)
Februar 2023	
08.-10.02.	30. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
21.-22.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)

Fundsache

Am 11.11.2022 veröffentlichte die ENISA die TOP 10 aufkommenden Cybersicherheitsbedrohungen bis 2030. Neben aktuell diskutierten Bedrohungen wie gefährdeten Lieferketten oder Desinformationskampagnen werden darin auch der Missbrauch intelligenter Geräte oder künstlicher Intelligenz und Lösungen für die erwarteten Herausforderungen in der Cybersicherheit beschrieben.

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

secorvo
security consulting

Secorvo Security News

Dezember 2022

Runder Kopf

Der Kopf ist rund, damit das Denken die Richtung wechseln kann.
Francis Picabia

Verfolgt man, welche Standpunkte in jüngster Zeit zum Thema Datenschutz eingenommen werden, lassen sich nur zwei Positionen finden: Die derjenigen, die jegliche Risiken für die Betroffenen vermeiden, und die derjenigen, die den Datenschutz am liebsten ganz abschaffen möchten.

So fordert Alena Buyx, Vorsitzende des deutschen Ethikrats, am 08.12.2022 im Interview mit der Süddeutschen Zeitung, nicht über Risiken von Daten zu sprechen, sondern über deren Nutzen. Zu viel Datenschutz gefährde Patienten. Liest man hingegen beispielsweise die FAQ zu MS365 des LfDI Rheinland-Pfalz, so scheint nach Auffassung der Aufsichtsbehörden eine Verarbeitung nur noch zulässig zu sein, wenn keinerlei Risiken für den Betroffenen verbleiben.

Beide Positionen gehen am Kern der DSGVO vorbei. Denn dort geht es in erster Linie um den Umgang mit möglichen Risiken: So dürfen personenbezogene Daten im lebenswichtigen Interesse der Betroffenen immer verarbeitet werden (Art. 6 Abs. 1 d)), während sich in anderen Fällen die Zulässigkeit einer Verarbeitung nach der Frage richtet, welche konkreten Risiken es gibt, wie wahrscheinlich deren Eintritt ist und welche Maßnahmen dagegen ergriffen werden (können). Schließlich soll nach dem Grundsatz „Privacy by Design" der Datenschutz schon bei der Konzeption und Entwicklung innovativer Lösungen mitberücksichtigt werden.

Auch die datenschutzrechtlich Verantwortlichen sind Grundrechtsträger und verfolgen berechtigte Interessen. Die sind abzuwägen gegen die schutzwürdigen Interessen der Betroffenen. Das gelingt nur mit einem unverstellten Blick auf die tatsächlichen Risiken und die Umstände des Einzelfalls. Das ist mühsamer als ein pauschales „so nicht" – wird aber zu besseren Entscheidungen führen.

Inhalt

secorvo
security consulting

Security News

Spy Kit

Die Firma Pushwoosh vertreibt Software Development Kits (SDK) zur Auswertung von Nutzeraktivitäten in Apps (Tracking, Profiling), die Entwickler in ihre Programme integrieren können. Nach der Webseite des Herstellers nutzen bereits über 80.000 Firmen ein Pushwoosh-SDK.

Am 14.11.2022 wurde das vorgeblich in den USA ansässige Unternehmen nach Reuters-Recherchen in Novosibirsk verortet: Es hat 40 Mitarbeiter und einen Jahresumsatz von (umgerechnet) 2,4 Mio. €. „Mailand oder Madrid, Hauptsache Italien!" möchte man da fast sagen… Am selben Tag veröffentlichte Internet Safety Labs eine Liste einiger tausend Apps, die vorgeblich Pushwoosh-Code verwenden – darunter auch Training-Apps der US Army. Offenbar hatte man angenommen, das Unternehmen käme aus Washington D.C.

Tatsächlich bietet die Webseite von Pushwoosh Anlass für Skepsis: Eine Firmenanschrift sucht man dort vergeblich. Wer fremde Software in seine „Supply Chain" integriert, sollte daher schon genau hinsehen – vor allem, wenn der Code Nutzerdaten auf externe Server überträgt.

Domain-Trickserei

Schon immer konnte man den Kartendienst Google Maps sowohl über maps.google.com als auch über google.com/maps erreichen. Wie Rutger Roffel am 02.12.2022 auffiel, ersetzt Google jedoch neuerdings die URL maps.google.com beim Aufruf durch google.com/maps. Kleiner Schritt – große Wirkung:

Bisher waren alle Dienste von Google (wie news.google.com oder mail.google.com) durch eine eigene Sub-Domain logisch von der Top-Level-Domain google.com getrennt – mit der Folge, dass Browser-Freigaben nur für den jeweils aktiven Dienst gelten. Diese Trennung hat Google nun bei Maps aufgehoben und den Kartendienst damit zu einem Teil der Top-Level-Domain google.com gemacht. Gibt ein Nutzer für den Kartendienst die Übermittlung seines Standorts durch den Browser frei, gilt diese Freigabe für die gesamte Domain google.com – der Standort wird also auch bei der Google-Suche übermittelt. Ein Schelm, wer…

Datenschutzrechtlich ist das ein Verstoß gegen das Transparenzgebot (Art. 12 DSGVO), denn Google täuscht Nutzerinnen und Nutzern vor, dass sich die Standortfreigabe lediglich auf Maps bezieht. Da sich Google bei der Verarbeitung zudem auf „berechtigtes Interesse" beruft, wird der Standort auch dann verarbeitet, wenn im Consent-Banner „alles" abgelehnt wird. Die Zustimmung zur Standort-Übermittlung durch den Browser ist jedoch keine rechtskonforme Datenschutz-Einwilligung.

Immerhin: Firefox-User sind nicht betroffen, da Firefox ausschließlich temporäre Standortfreigaben erteilt.

Threema-Verschlüsselung

Am 09.01.2023 veröffentlichten Forscher der ETH Zürich eine kryptografische Analyse der Threema-Verschlüsselung. Darin beschreiben sie sieben Angriffsmöglichkeiten auf das Protokoll des verbreiteten Messengers. Laut Threema ist das im Dezember 2022 eingeführte neue Protokoll Ibex für die dargestellten Angriffe nicht anfällig; soweit bekannt wurde auch keiner der beschriebenen Angriffe in der Praxis eingesetzt.

Doch der Fall ist ein Paradebeispiel für mehrere Lektionen, die bei der Entwicklung kryptografischer Protokolle beachtet werden sollten. So war nicht eine fehlerhafte Implementierung kryptografischer Verfahren das Problem, sondern deren Zusammenstellung zu miteinander verwobenen Protokollen. Zusätzlich zum bekannten Mantra „don´t roll your own crypto" lautet die generelle Empfehlung der ETH-Forscher, wann immer möglich auf bekannte und bewährte Protokolle wie beispielsweise TLS zurückzugreifen – spätestens seit dem Desaster des WEP-Protokolls (SSN 3/2002) sollte das eigentlich das „übliche Vorgehen" sein.

Auch Schneier´s Law haben die Threema-Entwickler missachtet: Danach kann ein kryptografisches Protokoll (genau wie ein kryptografischer Algorithmus) nur durch unabhängige Analysen seine Sicherheit unter Beweis stellen. Für die Einordnung solcher Sicherheitsanalysen muss zudem definiert sein, gegen welche Angriffsmodelle das Protokoll schützen soll; erst daraus können Sicherheitsaussagen abgeleitet werden. Die Definition von Standard-Angriffsmodellen, gegen die ein kryptografisches Protokoll für einen Messenger schützen soll, wäre daher für Entwickler und Sicherheitsexperten hilfreich.

Um Protokoll-Analysen zu erleichtern ist der derzeitigen Darstellung des Threema-Protokolls eine höhere Detailtiefe zu wünschen – vergleichbar der der Dokumentation des Signal Protokolls.

Bußgeld-Krimi

Seit dem 20.08.2018 hatte sich die für ihre laxe Haltung in Datenschutzfragen bekannte irische Datenschutzaufsichtsbehörde (DPC) mit offensichtlichen Datenschutzverstößen von Meta beschäftigt – nicht auf eigene Initiative, sondern ausgelöst

durch eine Beschwerde der von Max Schrems gegründeten Non-Profit-Organisation NOYB bei der belgischen Datenschutzaufsicht vom 25.05.2018.

Um die strengen datenschutzrechtlichen Anforderungen an eine Einwilligung zu umgehen hat Meta die Verarbeitung von Nutzerdaten für personalisierte Werbung als Klausel in die AGB von Facebook und Instagram aufgenommen, da diese für die Bereitstellung der Dienste erforderlich sei. Ein Umgehen der Einwilligung durch die Aufnahme in einen Vertrag ist jedoch durch das Kopplungsverbot (Art. 6 Abs. 4 DSGVO) untersagt. Der Verstoß hat zusätzliches Gewicht durch die Monopolstellung von Meta.

Gegen den vorläufigen Entscheidungsentwurf der DPC legten neun europäische Aufsichtsbehörden Beschwerde ein, sodass eine Streitbeilegung nach Art. 65 durch die europäische Datenschutzaufsicht (EDPB) erforderlich wurde. Derweil verhängte die DPC am 15.03.2022 ein 17 Mio. €-Bußgeld gegen Facebook und am 28.11.2022 ein 265 Mio. €-Bußgeld gegen Instragram. Wenige Tage später veröffentlichte der EDPB am 05.12.2022 die verbindlichen Anordnungen zu Facebook und zu Instagram, in denen Meta die Praxis untersagt und von der DPC die Verhängung eines höheren Bußgelds verlangt wird. Die reagierte am 31.12.2022 mit einem weiteren Bußgeldbescheid über 390 Mio. €. Darin ist allerdings die Abschöpfung der von Meta mit den unrechtmäßig verarbeiteten Daten erwirtschafteten (Milliarden-) Gewinne nicht enthalten – das letzte Wort ist also wohl noch nicht gesprochen.

Vor diesem Hintergrund wirkt die Stellungnahme von Meta gegenüber der DPA geradezu hämisch: „Wir glauben zutiefst, dass unser Ansatz die EU-Datenschutzverordnung respektiert […].“

Garantien von Microsoft

Am 15.12.2022 hat Microsoft bekannt gegeben, dass das lange angekündigte EU Data Boundary für Microsoft 365 (SSN 11/2022) zum 01.01.2023 in Betrieb geht. Automatisch kommt man aber nicht in den Genuss der Vorteile dieser Regelung: Nur wer das Data Protection Addendum auf die Fassung vom 01.01.2023 aktualisiert, kann sicher sein, dass seine Daten in dem von Microsoft beschriebenen Rahmen innerhalb der EU gespeichert und verarbeitet werden. Die Verantwortung dafür liegt beim Kunden. Das Angebot richtet sich nicht nur an Kunden mit Volumenlizenzvertrag, sondern an alle, die mit Microsoft Vereinbarungen im Zusammenhang mit deren Cloud-Produkten und –Dienstleistungen abgeschlossen haben.

Mit Daten bezahlen

Am 29.11.2022 hat die Datenschutzkonferenz (DSK) einen Beschluss zu den „Auswirkungen der neuen Verbrauchervorschriften über digitale Produkte im BGB auf das Datenschutzrecht“ veröffentlicht – dem „Bezahlen mit Daten“, das durch die Änderung des § 312 BGB zur Umsetzung der EU-Richtlinie zu digitalen Inhalten und Dienstleistungen nun zulässig ist. Die DSK beschränkt sich allerdings darauf festzustellen, dass die neuen Regelungen nur auf Verträge über digitale Produkte anwendbar sind, und nicht, wenn Betroffene lediglich ihre Einwilligung bei Consent Bannern erteilen. Bei Consent Walls wird man hingegen davon ausgehen dürfen, dass es zu einem Vertragsabschluss kommt.

Die Frage nach dem angemessenen Preis, wenn sich Betroffene dafür entscheiden, statt mit Geld mit ihren Daten zu bezahlen, wird auch von der DSK nicht beantwortet.

Secorvo News

Seminare

Ins Jahr 2023 startet unser Seminarbereich mit dem Seminar BSI Vorfall-Experte. Vom **07.03.** bis **09.03.2023** haben Sie die Möglichkeit, sich bei uns auf die Zertifizierung zum BSI-Experten nach dem Curriculum des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorzubereiten.

Im Seminar IT Security Insights – T.I.S.P. Update vom **21.03.** bis **22.03.2023** können Sie Ihren Wissenstand rund um die Themen Informationssicherheit und Datenschutz auffrischen. Kurz vor Ostern (**27.03.–31.03.2023**) bieten wir Ihnen mit dem T.I.S.P.-Seminar die Möglichkeit, Ihre IT-Security-Kenntnisse nicht nur zu vertiefen, sondern auch zertifizieren zu lassen – zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser T.I.S.P.-Buch „Informationssicherheit und Datenschutz“ (erschienen im dpunkt-Verlag).

Die Seminarprogramme und weitere Informationen zu unseren Seminaren finden Sie auf unserer Website. Wir freuen uns auf Ihre Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2023	
20.-22.01.	ShmooCon 2023 (The Shmoo Group, Washington/US)
Februar 2023	
08.-10.02.	30. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
13.-16.02.	OWASP 2023 Global AppSec (OWASP Foundation, Dublin/IRL)
März 2023	
07.-09.03.	BSI Vorfall-Experte (Secorvo, Karlsruhe)
14.-16.03.	secIT 2023 (Heise Medien, Hannover)
21.-22.03.	IT Security Insights - T.I.S.P. Update (Secorvo, Karlsruhe)
21.-24.03.	DFRWS EU 2023 (DFRWS, hybrid)
27.-31.03.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
April 2023	
23.-27.04.	Eurocrypt 2023 (IACR, Lyon/FR)
24.-27.04.	PKI - Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
25.-27.04.	Datenschutztage 2023 (WEKA, virtuell)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox, Christian Blaicher, Stefan Gora, Kai Jendrian, Oliver Oettinger, Friederike Schellhas-Mende (Editorial), 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