secorvo
security consulting

Secorvo Security News

Januar 2020

Clear View

Eigentlich nicht überraschend, und doch ist die Empörung groß: Kashmir Hill, eine Reporterin der New York Times, löste am 18.01.2020 mit einem Bericht über Clearview AI einen Shitstorm aus. Die KI-Gesichtserkennung des Startups eines Australiers wird von mehr als 600 amerikanischen Strafverfolgungsbehörden genutzt – Claim: "Technology to help solve the hardest crimes". Lädt man ein Personenfoto hoch, durchsucht Clearview seine Datenbank mit rund drei Milliarden Bildern aus öffentlichen Quellen nach solchen, auf denen dieselbe Person abgebildet ist, und liefert die Bildquelle sowie, falls bekannt, den Namen und die Adresse der erkannten Person.

Die Technik dahinter ist kein Hexenwerk, sondern ein übliches biometrisches Gesichtserkennungsverfahren mit neuronalem Netz für die Ähnlichkeitssuche. Auch Microsoft bietet in Azure einen vergleichbaren Dienst. Neu ist bestenfalls die offenbar hohe Erkennungsrate. Da ist es kein großer Schritt zu einer Datenbrille, die auch gleich alle im Internet verfügbaren Informationen zu jeder erkannten Person anzeigt. So etwas gibt es bereits, und auch Clearview hat eine solche Brille entwickelt – will sie aber angeblich nicht auf den Markt bringen.

Gesichtserkennung, wie sie Clearview einsetzt, ist als Authentifikationsmechanismus bereits weit verbreitet; Apple bietet sie unter der Bezeichnung „Face ID" als Passwortersatz an. Und da sollten unsere Alarmglocken noch lauter anschlagen. Denn Gesichtserkennungssysteme berechnen aus dem Bild ein 3D-Modell des Gesichts, das mit Referenzwerten verglichen wird. Wer aber dieses Modell kennt (das sich aus jedem Personenfoto berechnen lässt), kann daraus schon heute täuschend echte Bilder erzeugen. Im Unterschied zu Passwörtern ist bei Gesichtserkennungssystemen allerdings ein „Passwortwechsel" nicht so einfach. Angesichts der Niedrigzinsen könnte es daher eine gute Idee sein, in Kliniken der plastischen Chirurgie zu investieren. Oder, besser noch, in die Unsichtbarkeits-Forschung.

Inhalt

secorvo
security consulting

Security News

Fotos auf Facebook Fanpage

Mit Urteil vom 27.11.2019 hat das VG Hannover bestätigt, dass die niedersächsische Datenschutz-Aufsichtsbehörde (LfD Niedersachsen) zu Recht eine Verwarnung gegenüber einer Partei ausgesprochen hat, weil diese ohne Einwilligung Personenfotos auf ihrer Facebook Fanpage veröffentlicht hatte.

Demnach stellt die Veröffentlichung der Bilder einen Verstoß sowohl gegen Art. 6 Abs. 1 lit. e und f DSGVO als auch gegen §§ 22, 23 KUG dar. Für die Rechtmäßigkeit der Veröffentlichung fehlt die notwendige Einwilligung. Allein die Teilnahme an einer Veranstaltung stellt keine konkludente Einwilligungshandlung dar. Die Veröffentlichung auf einer Facebook Fanpage ist mit einer Veröffentlichung in Presseberichterstattungen nicht vergleichbar.

Soweit einzelne Personen aus Bildern hervortreten, ob nur als Beiwerk oder bei einer Bildberichterstattung über Menschenansammlungen wie Karnevalsumzüge o. ä., ist eine Interessenabwägung durchzuführen, um das Persönlichkeitsrecht der abgebildeten Personen zu wahren. Eine Veröffentlichung der Bilder auf Facebook steht diesem Interesse entgegen, da nicht kontrollierbar ist, wie die Bilder weiterverwendet werden. Damit hätte für eine rechtmäßige Veröffentlichung der Bilder eine Einwilligung der abgebildeten und hervortretenden Personen eingeholt werden müssen.

Vor der Veröffentlichung von Fotos auch öffentlicher Veranstaltungen in sozialen Netzwerken, bei denen einzelne Personen klar erkennbar sind, sollte demnach immer eine Einwilligung der Betroffenen eingeholt werden.

Überraschungsei WPA3

Am 06.01.2020 erschien das Linux-basierte Router-Betriebssystem OpenWRT in der neuen Hauptversion 19.07. Neben einer Vielzahl von Verbesserungen unterstützt OpenWRT auch erstmalig WPA3 (SSN 01/2018). Die im April 2019 entdeckten diversen Schwachstellen im Handshake-Protokoll von WPA3 Personal (SSN 04/2019) und die im August 2019 vorgestellten Seitenkanalangriffe, die bei Umsetzung der Sicherheitsempfehlungen der Wi-Fi Alliance gegen die vorherigen Angriffe möglich sind, wurden in der mit OpenWRT ausgelieferten Version von „hostapd“ alle bereits behoben.

Generell sollte vor dem Einsatz von WPA3 Personal überprüft werden, ob die bekannten Schwachstellen in der jeweiligen Implementierung bereits behoben sind. Wer WPA3 Enterprise nutzt, ist davon nicht betroffen, da hier SAE nicht zum Einsatz kommt.

Angesichts der bereits gefundenen Lücken sind weitere Nachbesserungen am WPA3-Standard nicht ganz unwahrscheinlich. Wer WPA3 nutzen möchte, sollte Firmware-Aktualisierungen im Auge behalten und einen Hersteller mit vertrauenswürdiger Update-Strategie wählen.

Querschnittsprüfung zur DSGVO

Die Landesbeauftragte für den Datenschutz Niedersachsen, Barbara Thiel, führte Ende Juni 2018 die bislang größte anlassunabhängige und branchenübergreifende Querschnittsprüfung zur Umsetzung der DSGVO durch. Die Überprüfung erfolgte anhand eines zehn Gliederungspunkte umfassenden Fragebogens zur Darstellung der Umsetzung der DSGVO, der nach rund 200 Einzelkriterien ausgewertet wurde. 50 ausgewählte mittelgroße und große Unternehmen hatten sich an der Befragung beteiligt.

Der 36seitige Abschlussbericht wurde am 05.11.2019 vorgestellt. Nur neun der Unternehmen erhielten die Bewertung grün („überwiegend zufriedenstellend“), 32 gelb („vereinzelter Handlungsbedarf“) und neun Unternehmen rot („erhebliche Defizite“). Vor allem der technisch-organisatorische Datenschutz und die Datenschutz-Folgenabschätzungen seien besorgniserregend.

Zwar ist die Verallgemeinerbarkeit der Ergebnisse angesichts der insgesamt rund 280.000 Unternehmen in Niedersachsen, davon knapp 21.000 mittlere und große (ab 2 Mio. € Umsatz), eher begrenzt. Dennoch dürfte nach wie vor ein sehr großer Teil der Unternehmen deutlichen Nachholbedarf beim Datenschutzmanagement haben.

Der Kriterienkatalog eignet sich als Leitfaden und sinnvolle Basis für interne Datenschutz-Audits zur Überprüfung des Reifegrads des Datenschutz-Managements, zumal Zertifizierungsmöglichkeiten aus Art. 42 DSGVO weiterhin nicht verfügbar sind.

Presenter-Lücke

Angriffe auf Funktastaturen und -mäuse sind lange bekannt (SSN 8/2016). Weniger bekannt ist, dass einige Hersteller die in den vergangenen Jahren u.a. von Matthias Deeg und Gerhard Klostermeier aufgedeckten Schwachstellen (siehe z. B. die Präsentation vom 24.10.2019) einfach ignorieren – und daher auch Nachfolgeprodukte anfällig sind.

Von den Sicherheitslücken sind auch Presenter betroffen. Zwar beherrscht der Sender nur wenige Tastencodes (Page Up, Page Down, F5, ...); der USB-Empfänger hingegen spielt Tastatur – und akzeptiert jeden Tastencode eines passenden Senders. Da

das Funkprotokoll weder Integritätsschutz noch Senderauthentifikation bietet, ist das Einspielen einer beliebigen Zeichenfolge (z. B. Öffnen der Commandozeile mit Windows+'R' und Start der PowerShell) mit einem 35 €-Dongle möglich. Gegen diesen bereits 2016 veröffentlichten Angriff sind (neben denen anderer Hersteller) auch die weit verbreiteten Presenter-Modelle R400, R700 und R800 von Logitech bis heute anfällig. Immerhin: Inzwischen bietet Logitech betroffenen Nutzern offenbar Ersatzempfänger über den Kundendienst.

Amerikanische Inseln

Seit dem 01.01.2020 gilt der California Consumer Privacy Act vom 23.09.2019, der für den Bundesstaat Kalifornien ein mit der DSGVO vergleichbares Datenschutzniveau schafft.

Das Gesetz fügt Datenschutzregeln in den US Civil Code ein (Sec. 1798.105 ff). Es ist anwendbar auf in Kalifornien niedergelassene oder tätige Unternehmen mit mehr als 25 Millionen US-Dollar Umsatz oder einer Datenverarbeitung, die mehr als 50.000 Verbraucher, Haushalte oder Geräte betrifft. Weiter sind Unternehmen umfasst, die ihren Umsatz mindestens zur Hälfte mit dem Verkauf personenbezogener Verbraucherdaten erzielen. Der Verbraucherbegriff ist dabei auf kalifornische Bürger beschränkt.

Das Gesetz hat ausdrücklich keine Schutzwirkung für die auf Europa gerichteten Geschäftsaktivitäten kalifornischer Unternehmen. Kern des Gesetzes ist ein Widerspruchsrecht gegen den Verkauf von Verbraucherdaten, eine umfangreiche aktive Informationspflicht und der DSGVO ähnliche Betroffenenrechte, v. a. ein Auskunftsrecht. Die Sanktionen betragen 2.500 USD für einfache und 7.500 USD für vorsätzliche Verstöße.

Im Vergleich zur DSGVO ist der Anwendungsbereich noch stark eingeschränkt und die Verarbeitung der Daten nicht auf rechtliche Erlaubnistatbestände limitiert. Dennoch stellt die Gesetzesanpassung eine deutliche Annäherung an europäische Datenschutzstandards dar. An der derzeitigen Rechtssituation bezüglich der Datenverarbeitung in den USA kann das Gesetz eines einzelnen Bundesstaates, zudem mit beschränktem Anwendungsbereich, nichts ändern. Aber es ist wenigstens ein derzeit seltener Grund für verhaltenen Optimismus.

Secorvo News

Wissen ist Macht

Im Jahr 2020 bieten wir Ihnen wieder mehrere Gelegenheiten, Ihre Kenntnisse in der Informationssicherheit auszubauen oder durch ein T.I.S.P.- oder T.P.S.S.E.-Zertifikat bestätigen zu lassen.

Den Anfang macht ein „Klassiker": Unser ständig weiterentwickeltes und aktualisiertes PKI-Seminar (**09.–12.03.2020**). „Für mich bildet das bei Ihnen angeeignete Wissen zusammen mit den aufwändig gestalteten Seminarunterlagen eine zentrale Arbeitsgrundlage im PKI Umfeld", urteilte jüngst ein Seminarteilnehmer. Es folgt der „TeleTrusT Professional for Secure Software Engineering" – ein „informatives und interaktives Seminar mit einem sehr guten Verhältnis von Theorie und Praxis", so eine Teilnehmerbewertung (**16.–19.03.2020**). Und mit der Vorbereitung auf das nächste T.I.S.P.-Seminar (**11.–15.05.2020**) können Sie bereits jetzt mit der aktuellen dritten Auflage des Begleitbuchs zum T.I.S.P. beginnen, das wir Ihnen unmittelbar nach Eingang Ihrer Anmeldung zusenden.

Alle Termine, Programme und die Möglichkeit zur Online-Anmeldung finden Sie hier.

… und noch nie zu fragen wagten.

Keine Novellierung des Datenschutzrechts hat eine solche Aufmerksamkeit bekommen wie die im Mai 2018 in Kraft getretene Datenschutz-Grundverordnung. Obwohl fast alles beim Alten geblieben ist, ist doch alles anders… und sind viele konkrete Fragen offen: Wann ist das Tracking von Webseitenbesuchern zulässig? Wie kann ein Unternehmen seine Informationspflichten angemessen erfüllen? Welche Datenschutzvorfälle sind meldepflichtig? Wie bestimmt sich die Höhe eines Bußgelds?

Zu diesen, weiteren und auch Ihren Fragen zur DSGVO und dem Datenschutz wird uns auf dem Jahresstartevent der KA-IT-Si am **13.02.2020** Dr. Stefan Brink, Landesbeauftragter für den Datenschutz und die Informationsfreiheit in Baden-Württemberg, Rede und Antwort stehen. Wir freuen uns sehr auf diesen Termin, denn Herr Dr. Brink ist für seine klaren Einschätzungen bekannt – und hoffen auf großes Interesse Ihrerseits.

Wir empfehlen eine frühzeitige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Januar 2020	
31.01.-02.02.	ShmooCon 2020 (The Shmooh Group, Washington/US)
Februar 2020	
13.02.	KA-IT-Si Event "... und noch nie zu fragen wagten." (KA-IT-Si, Karlsruhe)
19.-20.02.	30. ID:SMART Workshop (Fraunhofer Institut SIT, Darmstadt)
24.-25.02.	27. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg
März 2020	
09.-12.03.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
16.-19.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.03.	GI Sicherheit 2020 (Gesellschaft für Informatik e.V., Göttingen)
25.-26.03.	secIT 2020 (Heise Medien, Hannover)
25.-27.03.	DFRWS EU Conference (DFRWS, Oxford/UK)
31.03.-03.04.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)
31.03.-02.04.	IT-Sicherheit – praxisnah und aktuell (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Februar 2020

Von der IT lernen

Selten, dass der Mensch etwas von der Informationstechnik lernen kann. In der Regel ist es umgekehrt: Vom einfachen Algorithmus bis zur künstlichen Intelligenz versucht die IT, vom Menschen zu lernen.

Aber im Umgang mit Viren kennt sich die Informationstechnik inzwischen aus – seit dem ersten Computer-Virus aus dem Jahr 1984 sind sie eine ständige Bedrohung. Computer-Viren mutieren zudem weit schneller als Grippeviren, und die Infektionswege haben durch immer weitere Schnittstellen und die zunehmende Vernetzung der Systeme ständig zugenommen. Trotzdem ist bis heute ein „GAU“ ausgeblieben.

Das Erfolgskonzept der Virenabwehr in der Informationstechnik ist die Reaktion auf verschiedenen Ebenen. Am einfachsten lässt es sich in fünf Schritten beschreiben:

1. Expertenanalyse des Virus direkt nach erstem Auftreten
2. Unverzügliche und umfassende Information über Infektionswege, Schad-Funktion und wirksame erste Gegenmaßnahmen
3. Sensibilisierung der Nutzer für Symptome und Infektionswege
4. Blockade einzelner Infektionswege (z. B. durch Updates)
5. Isolation befallener Systeme

Tatsächlich eignen sich nicht alle Maßnahmen, die gegen Computerviren helfen, auch für Menschen, wie das Neuaufsetzen des Betriebssystems oder das Formatieren der Festplatte.

Allerdings gilt auch für „echte“ Viren: Keine Panik. Ausbreitung und Schäden lassen sich eindämmen. Ruhe bewahren – aber zugleich alle riskanten Tätigkeiten vermeiden. Und immer wieder gründlich die Hände scannen – pardon: waschen.

Inhalt

Security News

Gemeinsam verantwortlich

Bereits im Datenschutz-Tätigkeitsbericht 2019 legte der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI), Dr. Stefan Brink dar, dass angesichts der aktuellen Rechtslage insbesondere im Bereich Social Media Unklarheiten bei der Gemeinsamen Verantwortlichkeit bestehen. Am 06.02.2020 informierte der LfDI via Pressemitteilung über einen für öffentliche Stellen erstellten Anforderungskatalog der Aufsichtsbehörde. Danach riskiert die einen solchen Dienst einsetzende verantwortliche Stelle von der Aufsichtsbehörde in die Pflicht genommen zu werden, wenn die Anforderungen nach Art. 26 DSGVO vom Plattformbetreiber nicht angeboten und auch auf Anforderung des Nutzers nicht umgesetzt werden.

Der Anforderungskatalog sollte auch von Unternehmen geprüft werden, da die Anforderungen der Aufsichtsbehörde übertragbar sind. Wer in einem solchen Fall auf die Nutzung von Social-Media-Diensten nicht verzichtet, muss sich darüber im Klaren sein, dass er damit das Risiko eines Bußgeld bewehrten DSGVO-Verstoßes in Kauf nimmt.

Audit? Aber sicher!

Wie wichtig es ist, bei Security-Audits auf Qualität zu achten, haben im Februar die Audits zweier Wahl-Apps aus den USA gezeigt. So legte ein von Pro Publica in Auftrag gegebenes Security-Audit offen, dass die bei den Vorwahlen in Iowa verwendete Wahl-App von „elementaren Sicherheitsproblemen" betroffen ist, über die u. a. eine Manipulation der Anzahl der Stimmen möglich gewesen wäre. Der Hersteller behauptet, die App wäre zuvor „mehreren rigorosen Sicherheitstests durch eine Drittpartei" unterzogen worden. Auch die bereits mehrfach in den USA eingesetzte Wahl-App „Voatz" hat erhebliche Sicherheitsmängel, wie Forscher des MIT am 13.02.2020 mitteilten. Die Schwachstellen erlauben einem Angreifer Stimmen zu manipulieren, Stimmabgaben zu unterdrücken oder zu erkennen, für wen ein Wähler gestimmt hat. Auch für Voatz gab es laut Hersteller in der Vergangenheit diverse Sicherheitsaudits.

Security-Audits sollte man grundsätzlich von qualifizierten, idealerweise auch zertifizierten Auditoren nach anerkannten Prüfstandards durchführen lassen. Damit werden die Ergebnisse vergleichbar – und Vorfälle wie die oben genannten sollten seltene Ausnahmen sein.

Keep it simple

Am 28.01.2020 hat Linus Torvalds WireGuard in den Hauptzweig des Linux-Kernels aufgenommen. WireGuard realisiert ein neuartiges VPN-Protokoll, das einfacher, sicherer und performanter sein will als die VPN-Standards OpenVPN und IPsec.

Mit nur etwa 4.000 Zeilen Quellcode (loc) ist die Komplexität von WireGuard deutlich geringer als die von OpenVPN und OpenSSL (70.000 bis 600.000 loc) oder IPSec (400.000 loc). Damit sinkt die Fehleranfälligkeit und das Auditieren des Quelltextes wird erheblich erleichtert. Durch die Beschränkung auf das absolute Minimum – beispielsweise wird nur eine einzige Cipher Suite unterstützt und statt X.509-Zertifikaten kommen wie bei SSH Schlüsselpaare zum Einsatz – bietet WireGuard nicht denselben Funktionsumfang wie OpenVPN; das könnte eine Hürde bei der Durchsetzung sein. Aus Sicherheitssicht ist WireGuard jedoch ein Schritt in die richtige Richtung – denn Komplexität ist einer der großen Feinde der IT-Sicherheit.

Erpressung „on top"

Dass man Ransomware für die Betroffenen noch unangenehmer gestalten kann, haben die Macher der „MAZE"-Ransomware um den 05. und 09.12.2019 unter Beweis gestellt. Dafür kombinierten sie zwei schon lange von Cyberkriminellen genutzte „Geschäftsmodelle", um den Zahlungsdruck zu erhöhen: Zunächst werden die Daten gestohlen und wie üblich verschlüsselt. Kommt der Betroffene der Zahlungsaufforderung nicht nach, werden die gestohlenen Daten in kleinen Häppchen im Internet veröffentlicht. Besonders verheerend kann das angesichts hoher DSGVO-Bußgelder sowohl für Unternehmen als auch für Privatpersonen sein.

Wer bereits Maßnahmen zum Schutz vor Ransomware (SSN 02/2016 und SSN 04/2016) ergriffen hat und eine solide, getestete Disaster-Recovery-Strategie mit Backups umsetzt, sollte sich daher besser nicht zufrieden zurücklehnen und das Thema „Data Loss Prevention" aus den Augen verlieren...

IT-Grundschutz 2020

Das BSI hat – wie geplant – am 01.02.2020 die 2020er Edition des IT-Grundschutz-Kompendiums veröffentlicht. Mit der Umstellung der IT-Grundschutz-Kataloge auf das IT-Grundschutz-Kompendium verfolgte das BSI das Ziel, die Aufwände für die Konzepterstellung zu reduzieren und die Praktikabilität bei der Umsetzung zu erhöhen (SSN 8/2018) – aus der Praxis können wir bestätigen, dass das gelungen ist.

Neu in der Edition 2020 sind die Bausteine „CON.8 Software-Entwicklung" sowie „NF.5 Raum sowie

Schrank für technische Infrastruktur"; die weiteren Änderungen sind klar aufgeführt. Alte Zöpfe, wie die Anforderung, regelmäßig das Kennwort zu wechseln – „Die Passwörter SOLLTEN in angemessenen Zeitabständen geändert werden." (ORP.4.A8) – wurden bei der Gelegenheit auch abgeschnitten. Aus unserer Sicht ist die neue Fassung eine weitere Verbesserung dieses wichtigen Referenzwerkes der IT-Sicherheit.

Conditio sine qua non

In der Automobilbranche sind Anforderungen an die IT-Sicherheit wie eine TISAX-Zertifizierung mittlerweile Standard. Andere Branchen ziehen nach: So wurde in einer europaweiten Ausschreibung im Bereich Krankenkassen/Sozialdienste (Unterstützungsdienstleistungen Fallbearbeitung) von den Bietern ein ISMS-Zertifikat nach DIN EN ISO 27001 gefordert. Eine Bietergemeinschaft wurde ausgeschlossen, obwohl eines der Mitglieder zertifiziert war. Daraufhin hatte ein anderes, nicht zertifiziertes Mitglied den Ausschluss vor dem Bundeskartellamt angegriffen. Dieses wies den Nachprüfungsantrag jedoch bereits am 19.07.2019 zurück.

Das Beispiel zeigt, dass nach einer langen Phase der Zurückhaltung inzwischen auch in Deutschland ein ISMS zunehmend zum Stand der Technik gezählt und von Anbietern erwartet wird.

Mixed Content

Am 06.02.2020 kündigte Joe DeBlasio vom Chrome Security Team im Google Security Blog an, dass Chrome zukünftig Schritt für Schritt Mixed-Content-Downloads verhindern wird. Damit werden von verschlüsselten Seiten keine unverschlüsselten Downloads mehr möglich sein. Dies setzt die Ende 2019 angekündigten Bestrebung fort, Mixed Content in Chrome komplett zu blockieren. Dass dieses Vorgehen bei Herstellern problematische Umgehungsstrategien provozieren kann, hat 2018 der Sennheiser-Fall gezeigt (SSN 11/2018).

Entwickler sollten dennoch prüfen, ob ihre Anwendungen Mixed-Content-Downloads durchführen und diese auf HTTPS umstellen. In der Praxis beobachten wir insbesondere in Unternehmensnetzen noch vergleichsweise oft unverschlüsselte Kommunikation. Da diese in aktuellen Browsern zukünftig weiteren Beschränkungen unterliegen wird, erscheint auch hier der Umstieg auf HTTPS angebracht.

Secorvo News

Secorvo Seminare

Wenige Tage noch bis zum „TeleTrusT Professional for Secure Software Engineering" – einem interaktiven Seminar mit großem Praxisteil zur sicheren Softwareentwicklung (**16.–19.03.2020**). Und im Mai folgt das nächste T.I.S.P.-Seminar (**11.–15.05.2020**) – wer bereits jetzt mit der Vorbereitung anhand des jüngst aktualisierten Begleitbuchs zum T.I.S.P. beginnen möchte, sollte sich einfach anmelden – das Begleitbuch wird Ihnen umgehend zugesendet (Programme und Online-Anmeldung).

EaSy mit Microsoft-PKI

Unsere Zertifikatsmanagement-Lösung Certificates ready2go – EaSy erhält im nächsten Release (April 2020) die Möglichkeit zur Anbindung einer Active Directory Enterprise CA. Über das EaSy Enrollment-Gateway können ACME Clients wie der bekannte Certbot für interne Server öffentlich gültige Zertifikate bei Trustcentern wie Let's Encrypt & Co. beziehen und automatisch erneuern – und künftig auch intern gültige Zertifikate bei einer vorhandenen Microsoft-PKI. Für die internen Zertifikate entfällt die Beschränkung auf öffentlich registrierte Servernamen; die Enterprise CA kann Zertifikate auch für bspw. „intranet.local" erstellen (Kontakt).

„Ich seh' etwas, was Du nicht siehst…"

Das kommende KA-IT-Si-Event am 26.03.2020 dreht sich um die Sichtbarmachung des Unsichtbaren: Die Sicherheit eines Verfahrens oder Protokolls kann man nämlich nicht durch einfaches Hinsehen erkennen, wie Professor Dr. Jörn Müller-Quade (KIT) zeigen wird. Schlimmer noch: Sie ist keine funktionale Eigenschaft und kann daher auch nicht durch einfaches Testen festgestellt werden.

Dem begegnet die Kryptographie mit mathematischen Beweisen, mit denen nachgewiesen wird, dass ein Verfahren in einem bestimmten Modell unter präzise beschriebenen Voraussetzungen eine ebenso präzise definierte Sicherheitseigenschaft erfüllt. Unterschiede zwischen dem (vereinfachenden) Modell und der Wirklichkeit können dazu führen, dass auf die Implementierung eines als sicher bewiesenen Systems so genannte Seitenkanalangriffe möglich sind. Noch gravierender ist, dass nicht ohne weiteres nachprüfbar ist, ob ein reales technisches System auch wirklich die modellierte Sicherheitslösung umsetzt. Ein Ansatz, diesem Problem zu begegnen, ist *Auditable Security* – ein Konzept, das durch den modularen Aufbau von Systemen eine Überprüfung bestimmter Eigenschaften durch eingehende visuelle Inspektion zu ermöglichen versucht.

Im Anschluss haben Sie wie gewohnt Gelegenheit zum fachlichen und persönlichen Austausch beim „Buffet-Networking" (zur Anmeldung).

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

März 2020	
16.-19.03.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
17.-20.03.	GI Sicherheit 2020 (Gesellschaft für Informatik e.V., Göttingen)
25.-26.03.	secIT 2020 (Heise Medien, Hannover)
25.-27.03.	DFRWS EU Conference (DFRWS, Oxford/UK)
31.03.-03.04.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)
April 2020	
21.-22.04.	Datenschutztage 2020 (FFD, Wiesbaden)
21.-22.04.	Security Forum 2020 (Hagenberger Kreis, Hagenberg/AT)
Mai 2020	
06.-07.05.	BvD Verbandstag 2020 (BvD e.V., Berlin)
10.-14.05.	Eurocrypt 2020 (IACR, Zagreb/HRV)
11.-15.05.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
12.-15.05.	European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München)

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: André Domnick, Dirk Fox (Editorial), Stefan Gora, Hans-Joachim Knobloch, Sarah Niederer, Friederike Schellhas-Mende, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

März 2020

Panikresistenz

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

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

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

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

Inhalt

secorvo
security consulting

Security News

Datenschutz-Abmahnung

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

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

Kritische Leitsystem-Lücken

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

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

Wiederbelebungsversuch

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

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

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

Datenschutz und Social Media

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

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

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

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

Apple begrenzt Zertifikatsgültigkeit

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

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

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

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

Benachrichtigungspflicht

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

Secorvo News

Rezensenten gesucht

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

RaSy/DaSy mit LDAP-Anbindung

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

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

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

Impressum

Secorvo Security News – ISSN 1613-4311

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

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

Secorvo Security News

April 2020

Imagine

Stellen Sie sich einmal vor – rein hypothetisch – ein neuer Virus bräche aus. In China. Ein Computervirus, meine ich.

Und stellen Sie sich weiter vor, er besäße unschöne Eigenschaften: Er ist hochansteckend und besitzt eine Inkubationszeit von einigen Tagen, in denen er sich aber weiter verbreitet. Bricht er aus, dann richtet er bei 5-10 % der befallenen Geräte erhebliche Schäden an – von der Löschung des Datenbestands und der installierten Software bis hin zu irreparablen Hardware-Defekten. Jüngere Geräte sind offenbar weniger stark betroffen.

Dabei nutzt er alle Schwächungen des „Immunsystems" wie sicherheitskritische Fehler in veralteter Software oder unbedachte Konfigurationen. Offenbar verwendet er alle Arten von Kontakten mit anderen Rechnern zur Verbreitung: USB-Sticks, SD-Karten, Bluetooth-, WLAN- und Internetverbindungen. Befallene Rechner können bisher nur über die Symptome identifiziert werden; da der Virus sein Erscheinungsbild ändert, ist er für Virenscanner „unsichtbar".

Da sich der Virus nun auch in Deutschland ausbreitet, Sicherheitsexperten zur Schadensbegrenzung knapp sind und bisher keine wirksamen Schutzmaßnahmen zur Verfügung stehen, sperrt die Bundesregierung internationale Datenverbindungen. Rechner dürfen Räume nur noch in unvermeidlichen Fällen verlassen und nur innerhalb des Unternehmens oder der eigenen Wohnung miteinander verbunden werden (LAN). Sie müssen einen Mindestabstand von 1,5 m zu anderen Rechnern einhalten und außerhalb geschlossener Räume in Metallbehältern transportiert werden...

Das klingt ein wenig wie Selbstmord aus Angst vor dem Tod. Und selbst wenn der Vergleich mit der aktuellen Situation hinkt (denn schließlich geht es dort um den Schutz von Leib und Leben): Ein wenig mehr Paranoia hier und etwas mehr Augenmaß dort könnten keinesfalls schaden.

Inhalt

secorvo
security consulting

Security News

MASVS 1.2

Nach zahlreichen Überarbeitungen wurde am 17.03.2020 Version 1.2 des Mobile Application Security Verification Standard (MASVS) von OWASP gleich in acht Sprachen veröffentlicht. Analog zum etablierten ASVS für Web-Anwendungen definiert der MASVS einen Sicherheitsstandard aus verschiedenen Anforderungen an mobile Apps. In Anbetracht der häufigen Berichterstattung über verwundbare Apps war ein solcher Standard überfällig.

Der MASVS unterscheidet drei aufeinander aufbauende Prüf-Niveaus/Level: Der Basis-Level 1 wird in Level 2 um Defense-in-Depth-Anforderungen und in Level „R" um Maßnahmen gegen Reverse Engineering erweitert. Je nach Schutzbedarf der App sollte der gewünschte Level entsprechend festgelegt werden. In acht Bereichen wird im Standard beschrieben, welche Anforderungen beispielsweise an Architektur, Datenschutz und sichere Kommunikation gestellt werden.

Ergänzt wird der MASVS zukünftig um die Version 1.2 des Mobile Security Testing Guide (MSTG). Der MSTG beschreibt Prüfpunkte für die Sicherheitsanforderungen des MASVS und kann somit im Rahmen eines Pentests eingesetzt werden. Da Apps meist mit Web-Services im Backend kommunizieren und deren Sicherheit im Rahmen des MASVS nicht betrachtet wird, sollte die Prüfung des Gesamtsystems auch die Web-Services umfassen. Hierbei empfiehlt sich eine Vorgehensweise auf Basis des OWASP Testing Guide und Prüfung der API Security Top 10.

CWE für Hardware-Schwächen

Bisher war die Common Weakness Enumeration (CWE) eine Sammlung und Kategorisierung häufiger Fehler in Software, die zu Sicherheitsschwachstellen führen können (SSN 12/2019). Am 24.02.2020 sind mit Version 4.0 häufige Fehler im Hardware-Design neu hinzugekommen; zusätzlich gibt es eine für die sichere Softwareentwicklung wertvolle „Software Development"-Sicht auf die Schwächen, welche die vorherigen Architektur- und Entwicklungs-Sichten kombiniert.

Aus Sicherheitssicht besonders zu begrüßen ist die Integration von Hardware-Schwächen in die CWE. Dieser Schritt unterstreicht eine Entwicklung, die wir in der vergangenen Zeit vermehrt beobachten konnten: Nachdem Software-Sicherheit sich inzwischen als ein wichtiges und zunehmend höher priorisiertes Qualitätsmerkmal etabliert hat, wird der Allgemeinheit die Fehlbarkeit von Hardware immer bewusster – nicht zuletzt aufgrund von medial wirksamen Schwachstellen wie Meltdown und Spectre (SSN 02/2018). Bisher spielte die Sicherheit bei der Entwicklung von Hardware eher eine untergeordnete Rolle. Wichtigere Parameter waren Performance, Effizienz und Kosten. Dass Hardware-Fehler unter Umständen alle anderen Sicherheitsmaßnahmen kompromittieren können, haben verschiedene Schwachstellen eindrucksvoll demonstriert. Beispielsweise war ein Fehler im Nvidia Tegra Prozessor in frühen Nintendo Switch Konsolen dafür verantwortlich, dass diese ohne eine Möglichkeit zur Behebung mit Homebrew-Firmware bespielt werden konnten. Auch Apple hat in jüngster Vergangenheit Bekanntschaft mit Hardware-Schwachstellen gemacht: Der checkra1n-Exploit für iPhones wurde inzwischen auf den in Macs zu findenden T2-Chip „portiert". Und Intels „Converged Security and Management Engine" (CSME) ist ebenfalls von einer nicht behebbaren Schwachstelle betroffen. Wir empfehlen daher auch bei Hardware-Entwicklung die Nutzung der CWE und die Durchführung expliziter Risikobetrachtungen.

Gefährliche Browser-Helfer

Als kleine Alltagshelfer erleichtern „Browser Extensions" und andere Plugins vielerlei Aufgaben. Doch merke: Erweiterungen sind Computerprogramme und können Schaden anrichten. Sie dürfen zudem meist mit nur wenigen Klicks auch von niedrig privilegierten Nutzern installiert werden und stammen oft aus intransparenten Quellen.

Wie Brian Krebs am 03.03.2020 berichtete, war eine Browser Extension verantwortlich dafür, dass die Webseite des „Blue Shield of California" von verschiedenen Sicherheitsprodukten als bösartig eingestuft wurde. Ein Mitarbeiter, der die Webseite aktualisierte, hatte in seinem Webbrowser die Erweiterung „Page Ruler" installiert. Als einst nützliches Tool mit über 400.000 Installationen wurde sie vor wenigen Jahren vom Entwickler verkauft und injiziert seitdem im Hintergrund bösartigen JavaScript-Code in Webseiten, während diese über ein CMS wie WordPress oder Joomla gepflegt werden.

Wie häufig das Problem bösartiger Erweiterungen ist, zeigt ein Blick auf Googles Chrome Web Store: Im Februar 2020 wurden 500 bösartige Erweiterungen entfernt, im April 2020 nochmals fast 50 – und das ist wahrscheinlich nur die Spitze des Eisbergs. Wie schon beim Umgang mit Docker-Images und Programmbibliotheken (SSN 03/2019) empfehlen wir auch bei Plugins einen minimalistischen Ansatz: Installieren Sie nur solche Plugins, die Sie unbedingt benötigen und die von vertrauenswürdigen Entwicklern aus offiziellen Quellen stammen. In größe-

ren Umgebungen empfiehlt sich ein Whitelisting-Ansatz: Konfigurieren Sie Webbrowser so, dass nur erlaubte Plugins installierbar sind. Eine vollständige Deaktivierung von Plugins sollte hingegen gut abgewogen werden, da viele Plugins Ihre Sicherheit und Privatheit im Web verbessern.

Neu im Telemediengesetz

Am 03.04.2020 hat die Bundesregierung mit dem Gesetzesentwurf zur Umsetzung der 2018 überarbeiteten Richtlinie über audiovisuelle Mediendienste (AVMD-RL) im Telemediengesetz das Gesetzgebungsverfahren eröffnet; jetzt ist der Bundesrat am Zug. Der Entwurf verankert neben dem bisherigen Telemedienrecht neue Pflichten für Anbieter von Webseiten zum Abruf von Video-Sendungen und Videosharing-Plattformen in den neuen §§ 10a ff TMG. Dazu gehören ein Beschwerdeverfahren, das Videosharing-Plattform-Anbieter ihren Nutzern bereitstellen müssen, und ein entsprechendes Abhilfeverfahren bezüglich rechtswidriger Inhalte. Weiter werden eine Verpflichtung zum Einsatz von Nutzungsbedingungen und eine Datenschutzregelung für den Umgang u. a. mit Altersverifikationsdaten eingeführt.

Auch wenn Ziel des Gesetzes die Richtlinienumsetzung ist, überrascht doch, dass trotz wiederholter TMG-Änderungen seit Geltung der DSGVO noch immer keine Anpassung der §§ 13 ff TMG erfolgt, obwohl diese schon lange von Aufsichtsbehörden und Lehre als unzureichend angesehen werden.

Dauerbrenner DS-Erklärung

Das Spannungsverhältnis zwischen Transparenz und Verständlichkeit von Datenschutzerklärungen erhält weiteres Futter. Der Erwägungsgrund 39 der DSGVO verlangt Verständlichkeit in einer klaren und einfachen Sprache. Aufsichtsbehörden und Gerichte scheinen sich jedoch derzeit eher in Richtung Detaillierung zu bewegen. So wandte sich die dänische Datenschutzaufsichtsbehörde am 11.02.2020 in einer Entscheidung gegen das Dänische Meteorologische Institut gegen gängige Cookie-Banner: Die Einwilligung über ein einheitliches „Akzeptieren“ oder „Ok“ sei nicht ausreichend für eine freiwillige Einwilligung. Vielmehr müsse in unterschiedliche Verarbeitungszwecke granular und einzeln eingewilligt werden. Das Angebot einer detaillierten Auswahl nach einem weiteren Klick sei intransparent. Auch müsse eine Gesamtablehnung mit einem Klick möglich und genauso schnell auffindbar sein. Mit anderem Bezug, aber möglicherweise richtungsweisend urteilte das OLG Köln am 19.02.2020, dass allein der 80seitige Umfang der AGB bei einem komplexen Geschäftsmodell wie PayPal nicht zur Intransparenz und mangelnder Einbeziehung führe. Bei Internetgeschäften sei es dem Nutzer überlassen, wie lange er sich mit den Bedingungen befasse.

Für Datenschutzerklärungen (56 Seiten von Samsung) wurde dies auch schon umgekehrt bewertet (SSN 06/2016). Die „Wahrheit“ dürfte wohl in der Mitte liegen.

Corona-Orientierungshilfe

Der Europäische Datenschutzausschuss (EDSA) hat in seiner 24. Sitzung am 24.04.2020 seine bisherigen Empfehlungen zum Umgang mit Gesundheitsdaten während einer Pandemie ergänzt und Orientierungshilfen zur Verarbeitung von Gesundheitsdaten zu Forschungszwecken im Kontext des Covid-19 Ausbruchs angenommen.

Eine erste Ergänzung betrifft die Erleichterung internationaler Datentransfers zu Forschungszwecken in Drittstaaten. Hier soll auf die Ausnahmen des Art. 49 DSGVO zurückgegriffen werden, wenn andere Garantien des Datenschutzniveaus nicht zur Verfügung stehen.

Bezüglich der Tracking-Tools zur Ausbreitungsüberwachung verweist der EDSA auf die Flexibilität der DSGVO, die den Datenbedarf zur Epidemie-Bekämpfung bereits vorsehe. Die Orientierungshilfe setzt sich intensiv mit der Gestaltung erforderlicher Einwilligungen auseinander. Weitere Anforderungen betreffen Anonymisierung und Löschfristen sowie den angemessenen Schutz der Daten, wenigstens durch Pseudonymisierung oder Verschlüsselung.

Insgesamt betont der EDSA, dass trotz der Ausnahmesituation die Datenschutzbestimmungen der DSGVO umgesetzt werden können und müssen.

Secorvo News

Wiederaufnahme des Seminarbetriebs

Den aufgrund der Pandemie-Verordnungen des Landes Baden-Württemberg bis Ende Mai eingestellten Seminarbetrieb werden wir nach der Sommerpause wieder aufnehmen. Da viele Teilnehmer ihre Anmeldung verschoben haben, ist die Mindestteilnehmerzahl schon jetzt bei einigen Seminaren erreicht – wir empfehlen daher eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Hinweis: Wegen der derzeitigen Pandemie-Einschränkung finden einige der genannten Veranstaltungen möglicherweise nicht oder in anderer Form statt.

Mai 2020	
06.-07.05.	BvD Verbandstag 2020 (BvD e.V., Berlin)
12.-15.05.	European Identity & Cloud Conference 2020 (KuppingerCole Ltd., München)
13.-14.05.	21. Datenschutzkongress (EUROFORUM, Berlin)
Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)

Fundsache

Privacy Captcha gibt es zwar schon seit 2014, aber seit Spätsommer 2019 in neuem Gewand und gerade derzeit für einen sicheren Versand schützenswerter Daten bei unsicheren Kommunikationskanälen zu empfehlen.

Impressum

Secorvo Security News – ISSN 1613-4311

Autoren: Dirk Fox (Editorial), André Domnick, Michael Knopp, Sarah Niederer, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Mai 2020

Unterirdisch

Die Londoner „Tube“, benannt nach den Röhren, durch die die Untergrundbahnen fahren, ist die älteste U-Bahn und mit mehr als 270 Stationen an über 400 km Schienenstrecke noch heute das drittgrößte U-Bahn-Netz der Welt.

Der Eröffnung am 09.01.1863 ging jedoch ein erbittertes Ringen voraus. 17 Jahre hatte der Jurist *Charles Pearson* für den Bau gekämpft. Zwar erstickte London damals im Pferdedroschkenverkehr, aber Eisenbahnen waren noch eine junge Technik – erst 1838 hatte *Isambard Kingdom Brunel* die erste Eisenbahnstrecke erbaut. Doch der nur 6,5 km lange erste U-Bahn-Abschnitt wurde allen Widrigkeiten zum Trotz ein riesiger Erfolg: Im ersten Betriebsjahr beförderte die Tube bereits 9,5 Mio. Fahrgäste. Daher folgten bald weitere Linien; heute nutzen über 3 Mio. Menschen die Tube am Tag – fast 1,2 Milliarden im Jahr.

Drei Jahre Bauzeit und 1,3 Mio. Pfund kostete der Bau; für die damalige Zeit ein gigantisches Projekt. Aber es wurde rechtzeitig begonnen, bevor Bebauungsdichte und Kanalisation ein solches Querschnittsprojekt unmöglich gemacht hätten. Der erste Abschnitt konnte fast komplett in offener Bauweise errichtet werden. Wer heute eine U-Bahn plant, muss trotz aller technischen Errungenschaften wie Tunnelbohrmaschinen mit ganz anderen Hindernissen und Kosten kalkulieren. 320 Mio. Euro kostete das nach 14 Jahren Bauzeit am 08.08.2009 eröffnete, 1,8 km lange U-Bahn-Sackgässchen (U55) ins Berliner Regierungsviertel (177 Mio. €/km), und mehr als eine Milliarde Euro wird der knapp 3,4 km lange Stadtbahn-Tunnel in Karlsruhe bei der Fertigstellung 2021 nach 11jähriger Bauzeit voraussichtlich verschlungen haben (294 Mio. €/km).

Mit U-Bahnen verhält es sich offenbar wie mit dem Datenschutz: Auch der benötigt engagierte, idealistische Vorkämpfer, die nicht so leicht aufgeben – und je später man mit der Umsetzung beginnt, desto aufwändiger und teurer wird es am Ende.

Inhalt

secorvo
security consulting

Security News

Präventive Kontaktdaten

Seit dem 04.05.2020 atmet die Republik auf: Viele Dienstleistungen wie Friseur- oder Restaurantbesuche, die wochenlang verboten waren, sind zumindest eingeschränkt wieder zugelassen. Diese Einschränkungen haben es allerdings aus datenschutzrechtlicher Sicht in sich: Je nach Bundesland muss man nun seine Kontaktdaten (Name, Anschrift und Telefonnummer) hinterlassen bzw. werden diese von den Anbietern erfasst. Es sei denn, man wechselt in das „richtige" Bundesland: Nicht überall ist die Kontaktdatendokumentation vorgeschrieben, da es keine bundeseinheitliche Regelung gibt. Auch die Vorgaben zur Art und Weise der Erfassung und Verarbeitung, der Dauer der Aufbewahrung (vier bis sechs Wochen) und der Löschung der Daten sind uneinheitlich. In einem Bundesland muss der Besucher sogar (zwingend) sein Einverständnis zur Erhebung der Kontaktdaten erteilen – hier hat der Verordnungsgeber offenbar das Prinzip der datenschutzrechtlichen Einwilligung nicht verstanden. Einig ist man sich immerhin darin, dass das Aushängen oder Auslegen von Listen keine probate Form der Datenerfassung ist.

In manchen Bundesländern sind die Regelungen zur Kontaktnachverfolgung in einer einheitlichen Corona-Verordnung niedergelegt, in anderen gibt es für jedes Gewerbe getrennte Verordnungen. So wird beispielsweise in der ab dem 02.06.2020 gültigen Fassung der Verordnung des Baden-Württembergischen Kultus- und des Sozialministeriums über Sportstätten der nun wieder zulässige Betrieb von Schwimm- und Hallenbädern sowie Thermal- und Spaßbädern geregelt. Neben der Bereitstellung einer Aufsichtskraft für das Einhalten der Grundsätze des Infektionsschutzes muss der Betreiber solcher Einrichtungen dem Gesundheitsamt oder der Ortspolizeibehörde über die Besucher Auskunft geben können. Diese Angaben umfassen Namen und Vornamen, Datum und Uhrzeit (Beginn und Ende) des Besuchs, eine Telefonnummer oder Adresse. Die Daten sind vier Wochen nach der Erhebung zu löschen. Betriebe, die sich einen Onlineshop leisten können, werden mit der Erfüllung der Anforderungen an die Datenerhebung weniger Probleme haben; alle anderen haben mit Besucherschlangen und Papierbergen zu rechnen. Mit dem Grundsatz der Datensparsamkeit haben die Anforderungen wenig gemein.

Bleibt die (vage) Hoffnung, dass damit anonyme Schwimmbad- und Restaurantbesuche nicht der Vergangenheit angehören – und die Listen nicht zum Standard werden. Schließlich könnte ja eine zweite Infektionswelle kommen – und da wäre es doch praktisch, auf diese Daten zurückgreifen zu können...

Corona-App und Datenschutz

Nach vielen Warnungen hat die Bundesregierung am 26.04.2020 den Schwenk auf eine freiwillige, dezentrale App-Lösung zur Kontaktverfolgung und Infektionseindämmung vollzogen. SAP und die Deutsche Telekom sollen die App nun bis Mitte Juni fertigstellen. Viele Politiker möchten weitere Lockerungen der Kontaktbeschränkungen mit der Einführung einer solchen App verknüpfen, um bei Neuinfektionen mögliche weitere Betroffene zukünftig schneller und mit weniger Aufwand informieren zu können.

Mit der Hinwendung zu einem datenschutz-freundlicheren, dezentralen Konzept sind die Herausforderungen jedoch noch nicht gelöst. Es bleibt eine pseudonyme Datenverarbeitung durch den Anbieter, zu der Rechtsgrundlage, Verantwortlichkeit und Sicherheit zu bestimmen sind. An der Einwilligung des Nutzers als Rechtsgrundlage hat bereits der EDSA Zweifel geäußert. Kritisch wird diesbezüglich die Freiwilligkeit sein. Diese besteht nur, wenn Eingriffslockerungen wie Restaurantbesuche auch von privater Seite nicht von der App-Nutzung abhängig gemacht werden.

Ungeklärt sind zudem die Folgen von Kontaktwarnungen. Ist der Nutzer dadurch zur Quarantäne verpflichtet, hat er einen sofortigen Testanspruch oder besteht sogar eine Testpflicht? Gilt der Nutzer nach einer Warnung als „in Kontakt mit einem Infizierten" und werden die App-Daten damit zum Beweismittel gegen den Nutzer?

Diese Fragen erfordern ein Begleitgesetz, denn für eine diesbezügliche Verordnung gibt das Infektionsschutzgesetz selbst bei weitester Dehnung keine Ermächtigung her. Einen sehr bedenkenswerten Gesetzentwurf hat eine Privatinitiative bereits vorgelegt. Die Verfügbarkeit der App wird dadurch jedoch weiter verzögert, denn im Unterschied zu einer Verordnung unterliegen Gesetze demokratischen Entscheidungsprozessen.

Zuverlässige Corona-App?

Unabhängig von der datenschutz-konformen Gestaltung der Corona-App stellt sich die grundlegendere Frage, ob eine derartige App die in sie gesetzten Erwartungen auch technisch erfüllen kann. Die vorgeschlagenen Lösungen basieren überwiegend auf der Signalstärkemessung mittels *Bluetooth Low Energy Beacons*, beispielsweise mit den Google und Apple APIs. Leider sind derartige Messungen physikalisch bedingt trotz Kalibrierungen sehr ungenau und werden durch Faktoren wie die Antennenform,

den Gerätetyp und die Umgebung stark beeinflusst. Nicht ohne Grund werden bei der Entfernungsmessung (z. B. mit GPS) nicht die Signalstärken, sondern die sehr viel präziseren Zeitdifferenzen zwischen dem Senden und Empfangen verwendet.

Tatsächlich kann auch die Exposition nicht verlässlich festgestellt werden, da sich Smartphones in der Regel nur beim Telefonieren in Gesichtsnähe befinden und sonst meist in einer Hosen-, Hand- oder Jackentasche stecken oder irgendwo herumliegen. Bluetooth-Signale werden zudem von Vorhängen, Plexiglasscheiben und dünnen Wänden nicht abgeschwächt. Daher sind häufige Fehlerkennungen zu erwarten – sowohl *false positives* (Kontakteinträge, auch wenn die Personen wirksam voreinander geschützt waren) als auch *false negatives* (keine Kontakteinträge, weil z. B. die Smartphones weiter voneinander entfernt waren als die Personen oder das Signal abgeschirmt wurde).

Die Messungen sind daher prinzipiell unzuverlässig und können nur Hinweise geben. Zudem könnten Angreifer mittels starker Signale die App täuschen und einer großen Zahl von Personen einen Kontakt mit einem Corona-Infizierten vorspielen. So ließe sich beispielsweise ein ganzes Unternehmen vorsätzlich in Quarantäne schicken. Weitere Angriffsmöglichkeiten sind das Kopieren fremder Identitäten oder Falschmeldungen zu positiven Tests.

Zwar ist die Forderung nach staatlichem Schutz vor der Corona-App zu begrüßen, aber auch darüber lassen sich die technisch bedingten Unzulänglichkeiten und die genannten Angriffsvektoren nicht ausräumen. So deutet alles darauf hin, dass der praktische Nutzen der App im besten Fall eher gering sein dürfte – und im schlimmsten sogar die negativen Folgen überwiegen.

Corona-Patientendatenschutz

Einige Gesundheitsämter haben sich in den vergangenen Wochen offenbar „vorsorglich“ mit Schreiben an die Kliniken ihrer Region gewandt und diese zur unverzüglichen Fax-Übermittlung aller Entlassungsberichte von mit Corona-Viren infizierten Patienten aufgefordert. Tatsächlich lässt sich aus dem Infektionsschutzgesetz jedoch keine solche Ermächtigung ableiten. Die Gesundheitsämter müssen sich, wenn sie diagnostische Daten benötigen, direkt an die betroffenen Patienten wenden. Denn auch eine Pandemie entbindet Kliniken nicht von der ärztlichen Schweigepflicht, und sie entzieht den Betroffenen auch nicht ihre Persönlichkeitsrechte.

Eine Übermittlung von Patientendaten an die Gesundheitsämter ist damit regelmäßig nicht nur ein Verstoß gegen geltendes Datenschutzrecht, sondern nach § 203 Strafgesetzbuch eine Verletzung von Privatgeheimnissen – und damit eine Straftat. Werden die Patientendaten dann auch noch per Fax übermittelt, kann dies zudem als ein mindestens fahrlässiger Verstoß gegen Sicherungspflichten gewertet werden.

Videokonferenzen & Datenschutz

Die Berliner Beauftragte für Datenschutz hatte am 08.04.2020 auf der Webseite ihrer Behörde eine „Checkliste zur Durchführung von Videokonferenzen während der Kontaktbeschränkungen“ bereitgestellt. Darin wies sie darauf hin, dass die Dienste Microsoft Teams, Skype Communications und Zoom Video Communications „die aufgeführten Bedingungen nicht erfüllen.“

Microsoft veröffentlichte daraufhin am 06.05.2020 eine Stellungnahme, in der sich das Unternehmen gegen diese Einschätzung von Teams und Skype wehrt. Unterschiedliche Medien berichten in diesem Zusammenhang von einer Abmahnung von Microsoft gegenüber der Berliner Beauftragten für Datenschutz. Kurz darauf war das Dokument der Datenschutzaufsicht nicht mehr abrufbar.

Dabei ist nicht etwa der Inhalt des Dokuments unzutreffend. Vielmehr wurde von der Aufsichtsbehörde nicht begründet, warum genau die genannten Produkte die Anforderungen nicht erfüllen. Seit dem 22.05.2020 ist eine überarbeitete Version 1.3 der Checkliste verfügbar, in der die Behörde weiterhin fordert, kurzfristig eingesetzte „nicht datenschutzgerechte Lösungen“ so bald wie möglich abzulösen, aber auch ankündigt, „in Kürze eine ausführlichere Übersicht mit detaillierteren Angaben zu verschiedenen gängigen Anbietern von Videokonferenz-Diensten zu erstellen.“

Doch wie findet man bis dahin geeignete datenschutzrechtlich zulässige Produkte? Auf die Tests von Institutionen wie der Stiftung Warentest kann man sich dabei wohl eher nicht stützen – Testsieger waren am 13.05.2020 Microsoft Teams und Skype, trotz eines „befriedigend“ beim „Basisschutz persönlicher Daten“.

Secorvo News

Herbstseminare

Den aufgrund der Pandemie-Verordnungen des Landes Baden-Württemberg eingestellten Seminarbetrieb werden wir wie geplant nach der Sommerpause wieder aufnehmen. Da viele Teilnehmer ihre Anmeldung verschoben haben, ist die Mindestteilnehmerzahl schon jetzt bei einigen Seminaren erreicht – wir empfehlen Ihnen daher eine baldige Anmeldung.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juni 2020	
02.-03.06.	a-i3/BSI-Symposium 2020 (a-i3, Bochum)
15.-16.06.	DuD 2020 (COMPUTAS, Berlin)
Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)
August 2020	
01.-06.08.	Blackhat USA 2020 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
09.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
16.-20.08.	Crypto 2020 (IACR, Santa Barbara/US)

Fundsache

Im April 2020 veröffentlichte das CrypTool-Entwicklerteam Release 2020.1 der Version 2 des bewährten Kryptographie-Lerntools. Es enthält zahlreiche Verbesserungen, Ergänzungen und Korrekturen – darunter auch ein Tutorial für die Differentielle Kryptoanalyse. Die neue Version wird im Dezember bei unserem Adventsrätsel „Krypto im Advent“ zum Einsatz kommen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Fabian Ebner, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Juni 2020

Friendly Fire

Es ist nicht lange her, da galten Phishing-Angriffe als IT-Dilettanten-Test: Wer auf die holprigen, in schlechtem Englisch verfassten Aufforderungen hereinfiel und PIN und TAN für sein Konto preisgab, der konnte sich der Schadenfreude seiner Umgebung sicher sein. Die von solchen Angriffen verursachten Schäden blieben daher überschaubar, auch, weil die deutschen Banken technisch gegensteuerten: 2016 summierten sie sich auf gerade einmal 8,7 Mio. Euro.

Aber die Phisher lernten schnell, dass mit „digitalem Social Engineering" auch ganz andere Summen abgerufen werden können: Ob CEO Fraud, Verschlüsselungs-Trojaner oder Credential Phishing – alle diese Angriffsformen basieren im Kern darauf, den Empfänger mit einer halbwegs plausiblen Geschichte zu einer Schaden verursachenden Reaktion zu verleiten. Entscheidender Auslöser ist am Ende ein Klick – auf einen Link, einen Login-Knopf oder eine Online-Überweisung.

Zwar gibt es probate Mittel, um die Authentizität einer E-Mail oder eines Anrufs zu überprüfen, auf die auch ausgefuchste Angreifer keinen Einfluss haben: die interne Rückfrage, die Prüfung der Rufnummer oder E-Mail-Adresse, das Vier-Augen-Prinzip. Eine solche Aufdeckung digitaler „Enkel-Tricks" fordert jedoch Aufmerksamkeit und gesundes Misstrauen von den IT-Nutzern. Leider sind wir seit Jahren (SSN 01/2012) dabei, ihnen gerade dies abzugewöhnen.

E-Mail-Clients, die nur den vom Absender wählbaren Sendernamen statt der E-Mail-Adresse anzeigen, Online-Anbieter, die für den Rechnungsversand oder das User-Management beliebige Second-Level-Domains nutzen und Marketing-Abteilungen, die Klickraten durch HTML-formatierte E-Mails mit verdeckten Links in die Höhe zu treiben versuchen: All dies stumpft Aufmerksamkeit und Misstrauen ab. Schutz vor Täuschungsangriffen werden wir daher nicht allein durch Mitarbeiter-Sensibilisierung erreichen – auch Hersteller, Marketingabteilungen und die interne Kommunikation müssen ihren Teil der Verantwortung erkennen.

Inhalt

secorvo
security consulting

Security News

IT-Sicherheit 2.0

Mitte Mai wurde ein Referentenentwurf des Innenministeriums für das „IT-Sicherheitsgesetz 2.0“ mit Stand vom 07.05.2020 öffentlich. Zwar kann sich bis zur Gesetzesverabschiedung noch sehr viel ändern, doch verdient der Entwurf aufgrund seiner zahlreichen Neuerungen Aufmerksamkeit. So erhält das BSI neue Aufgaben, u. a. die Förderung des Verbraucherschutzes und die Entwicklung eines „Stands der Technik“ bzgl. der sicherheitstechnischen Anforderungen an IT-Produkte. Es soll zur allgemeinen Meldestelle für Sicherheitsrisiken in der Informationstechnik werden und selbst aktiv nach Sicherheitslücken von öffentlich erreichbaren IT-Systemen suchen dürfen, auch mittels simulierter Angriffe.

Den Betreibern kritischer Infrastrukturen auferlegte Pflichten werden ausgeweitet auf „Unternehmen von besonderem öffentlichen Interesse“, die durch Rechtsverordnung noch genauer zu bestimmen sind. Im Telemediengesetz (TMG) soll u. a. eine Anzeigepflicht bei Angriffen und Datenverlusten gegenüber dem Bundeskriminalamt ergänzt werden. Ein interessantes Detail ist auch die Verlängerung der Speicherdauer für Protokolldaten der Systeme des Bundes auf bis zu 18 Monate. Und nicht zuletzt werden die Sanktionen bei Verstößen auf DSGVO-Niveau angehoben.

Die Rolle des BSI wird durch den Gesetzesentwurf deutlich erweitert. Der Entwurf enthält zahlreiche Regelungen, die erhebliche Auswirkungen auf IT-Vorhaben zahlreicher Unternehmen haben werden. Die Umsetzungsfristen, soweit vorgesehen, liegen bei nur einem Jahr – ein wichtiger Grund, das Gesetzgebungsverfahren aufmerksam zu verfolgen.

Cookies - nur mit Einwilligung

Am 28.05.2020 hat der Bundesgerichtshof nach der Planet49-Entscheidung des EuGH (SSN 10/2019) nun auch ein Urteil in Sachen Cookies gefällt. Das Ergebnis ist wenig überraschend: Das Setzen von Cookies ist nur zulässig, wenn der Betroffene zuvor eingewilligt hat. Die Auffassung, dass hiervon technisch erforderliche Cookies nicht betroffen sind, teilt der BGH mit dem EuGH. Am meisten Aufsehen erregt der BGH mit seiner Auslegung des § 15 Abs. 3 Satz 1 TMG: Obwohl darin dem Wortlaut nach von einem Widerspruch die Rede ist, hat nach Überzeugung des BGH auch hier eine Einwilligung vorzuliegen.

Damit steht unzweifelhaft fest: Möchte ein Webseitenbetreiber neben technisch notwendigen Cookies und ähnlichen Technologien auch solche einsetzen, die z. B. dem Marketing dienen, benötigt er die Einwilligung des Seitenbesuchers. Klarheit darüber, wie solche Einwilligungen in der Praxis auszusehen haben, gibt es jedoch weiter nicht.

Ungewolltes Phishing-Training

Am 02.04.2020 sperrte Linksys die Konten aller „Smart-Wi-Fi“-Nutzer, nachdem bekannt geworden war, dass Angreifer über so genannte Credential-Stuffing-Attacken die Kontrolle über eine Vielzahl von Benutzerkonten erlangt hatten. Dazu probieren Angreifer aus früheren Leaks bekannte Benutzernamen und Passwörter in anderen Anwendungen aus.

Die – an sich begrüßenswerte – proaktive E-Mail von Linksys, in der die Kunden zur Rücksetzung des Passworts aufgefordert wurden, wurde jedoch nicht von einer bekannten Linksys-Domäne, sondern von subscribermanagement@linksys-email.com verschickt – typisches Merkmal einer Phishing-E-Mail. Ein vermeidbarer sicherheitskritischer Fehler: Misstrauische Nutzer werden nicht auf diese E-Mail reagiert haben, andere wurden verunsichert und einige werden wieder einmal gelernt haben, dass es doch nicht weh tut, auf zweifelhafte E-Mail-Links zu klicken.

Kein Einzelfall, wie unsere Praxiserfahrung zeigt. E-Mails mit anhängenden Bestellungen im PDF-Format ohne Begleittext, Faxe mit anderer Ortsvorwahl als die des Absenders, kryptische Servernamen und Aufforderungen, ein Benutzerkonto zu aktivieren, die von unternehmensfremden Domains verschickt werden. Vermeintliche Kleinigkeiten, die mittelfristig jedoch große Schäden verursachen können. Denn der nächste Phishing-Angriff kommt bestimmt.

Aus für Google Analytics

Die Datenschutzkonferenz hat am 12.05.2020 ihre Hinweise zum Einsatz von Google Analytics aktualisiert und die Orientierungshilfe für Anbieter von Telemedien ergänzt. In der ausdrücklich nicht abschließenden Beurteilung werden der Widerrufs-Button von Google und die Einordnung als Auftragsverarbeitung „beerdigt“. Zudem wird klargestellt, dass Google unabhängig von anonymize_IP regelmäßig mit personenbezogenen Daten arbeitet. Die Datenschutzkonferenz betrachtet die Nutzung von Analytics daher als Fall der gemeinsamen Verantwortung (Art. 26 DSGVO).

Die Nutzung von Analytics könne in der Regel nicht aus einem berechtigten Interesse abgeleitet werden, sodass eine Einwilligung der Nutzer erforderlich ist. Die Information der Betroffenen muss beinhalten, dass Google die gesammelten Daten zu „beliebigen eigenen Zwecken“ verwendet, die Daten unter Zugriff staatlicher Stellen in den USA verarbeitet und darlegen, welche Zwecke damit von Google verfolgt werden. Dazu wird auf die Leitlinien für Transparenz des EDSA vom 11.04.2018 verwiesen.

Keine dieser Anforderungen erfüllt Analytics derzeit: Es gibt kein Vertragsangebot von Google zur gemeinsamen Verantwortung, und auch technisch genügt Analytics den Anforderungen der DSK nicht. Eine informierte Einwilligung kann auch der Seitenanbieter nicht beisteuern. In aller Klarheit und Kürze: Die Nutzung von Google Analytics ist in Europa derzeit nicht rechtskonform möglich.

Thunderspy

Intels Thunderbolt-Technologie setzt sich immer weiter durch; viele Notebooks bringen bereits entsprechende Ports mit. Technisch werden dabei der DisplayPort für die Bildübertragung und PCI Express (PCIe) für eine performante Datenübertragung kombiniert. Zurzeit wird Version Thunderbolt 3 verbreitet, die die Funktionen von USB 3.1 umfasst, also den Anschluss von USB-Geräten und Ladefunktionen bietet. So eignet es sich ausgezeichnet als Docking-Port. Da PCIe auf der Basis von Direct Memory Access (DMA) arbeitet, kann darüber auf den Hauptspeicher des Computers zugegriffen werden. Um das unberechtigte Auslesen sensibler Daten und Manipulationen des Systems zu verhindern, haben Hersteller DMA Remapping und Thunderbolt Security entwickelt; darüber kann man einzelne Geräte (z. B. Docks) für PCIe autorisieren.

Nach unserer Erfahrung wird Thunderbolt Security in vielen Unternehmen jedoch deaktiviert, weil der Verwaltungsaufwand hoch ist. Der Sicherheitsforscher Björn Ruytenberg hat am 17.04.2020 in einem Paper mehrere Schwachstellen des Protokolls veröffentlicht, die es erlauben, die Sicherheitsfunktionen zu umgehen. Nach Einschätzung des Autors lassen sich die Schwachstellen kaum in Software beheben. Wer den Thunderbolt Port nutzt, sollte daher auf die Vertrauenswürdigkeit des Geräts achten.

DSGVO-konforme Auskünfte

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, Dr. Stefan Brink, hat aufgrund zahlreicher Beschwerden die Berechnungsmethoden von Wirtschaftsauskunfteien zur Einstufung der Kreditwürdigkeit von Unternehmen und Privatpersonen überprüft. Die Pressemitteilung vom 05.06.2020 lässt aufhorchen: Nach den Grundsätzen für die Verarbeitung personenbezogener Daten gemäß DSGVO müssen die Daten u. a. „sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein“, Art. 5 Abs. 1 lit. d DSGVO. Gegen diesen Grundsatz haben Wirtschaftsauskunfteien offenbar teilweise verstoßen: So wurden Bonitätsbeurteilungen bei nicht vorliegenden Informationen z. B. auf Basis von Annahmen getroffen. Dies führte dazu, dass Kreditrahmen niedriger eingestuft wurden. Bewertungen sind jedoch nur dann rechtmäßig, wenn die Richtigkeit der genutzten Daten (und damit der Bewertung selbst) sichergestellt ist.

Universalität der Grundrechte

Am 19.05.2020 hat das Bundesverfassungsgericht über die Auslandsfernaufklärung des Bundesnachrichtendienstes im Ausland geurteilt und Teile des BND-Gesetzes für verfassungswidrig erklärt. Im Urteil stellt das BVerfG klar, dass sich deutsche Staatsgewalt auch an die Grundrechte (im Verständnis von Abwehrrechten, z. B. zum Schutz vor staatlichen Abhörmaßnahmen) halten muss, wenn sie Wirkungen außerhalb des deutschen Staatsgebietes erzeugt, und auch dann, wenn keine deutschen Bürger betroffen sind.

Dieses Urteil wird bei der Gesetzgebung zu generell grenzüberschreitenden Sachverhalten wie Datenschutz, Rechtsfragen des Internet, Medienrecht usw. künftig stets zu beachten sein. Damit steht es in eklatantem Kontrast zum amerikanischen Grundrechtsverständnis, wie es beispielsweise im US CLOUD Act (SSN 3/2019) zum Ausdruck kommt.

Secorvo News

T.P.S.S.E. und T.I.S.P.

Im September bieten wir Ihnen wieder die Möglichkeit, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren: für das Teilgebiet des sicheren Software-Engineerings (T.P.S.S.E., **14.–17.09.2020**) und das Zertifikat als Information Security Professional (T.I.S.P., **21.–25.09.2020**). Zur Vorbereitung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“, das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist.

Termine zum Vormerken

Am 08.07.2020 bietet KA-IT-Si-Partner Connecting Media die zweite SecurityCruise – diesmal auf der „MS Digital“. Spannende Vorträge, Workshops und spezielle Talkrunden mit den größten IT-Security-Anbietern im deutschsprachigen Raum erwarten Sie. Für KA-IT-Si-Partner und –Unterstützer gibt es das Steuermannpaket zum Vorteilspreis von 45 €. Schicken Sie bei Interesse eine kurze E-Mail an info@ka-it-si.de und wir senden Ihnen den Rabattlink zu.

Derweil freuen wir uns darauf, unsere KA-IT-Si-Veranstaltungen im zweiten Halbjahr 2020 wieder aufzunehmen. Notieren Sie sich gerne schon einmal die geplanten Termine in Ihrem Kalender: 24.09.2020 | 22.10.2020 | 12.11.2020 | 10.12.2020. Wir beginnen im September mit einem spannenden Vortrag zum „Mythos der Enigma“ von Johann Grathwohl, IT-Security-Architekt bei CONITAS.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Juli 2020	
08.07.	Security Cruise (Connecting Media, Karlsruhe)
14.-18.07.	PETS 2020 (University of Minnesota, Montréal/CAN)
19.-21.07.	DFRWS USA 2020 (DFRWS, Memphis/US)
August 2020	
01.-06.08.	Blackhat USA 2020 (Blackhat, Las Vegas/US)
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
07.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
17.-21.08.	Crypto 2020 (IACR, Santa Barbara/US)
September 2020	
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)

Fundsache

Das *Border Gateway Protocol* (BGP) ist ein zentraler Bestandteil des Internet-Routings. Wie unsicher BGP ist, haben in den letzten Jahren verschiedene „Fehlkonfigurationen" z. B. von chinesischen, pakistanischen oder russischen Internet Service Providern gezeigt. Cloudflare hat mit der Website „Is BGP Safe Yet?" am 17.04.2020 eine Art „digitalen Pranger" eingerichtet, der ISPs animieren soll, Sicherheitsmechanismen wie die kryptographische Validierung von Routing-Informationen zu nutzen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze.

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Juli 2020

Menschenrecht Anonymität

Menschen urteilen täglich. Vieltausendfach. Über Menschen. Wir müssen das tun, um angemessen auf unser Umfeld zu reagieren. Aber diese Urteile sind nie zutreffend und nur selten gerecht, denn es sind verkürzende, vereinfachende Bewertungen, die wir auf der Grundlage sehr begrenzter Detailkenntnis vornehmen. Das ist jedoch unvermeidlich – schließlich sind wir begrenzte Wesen: Kein Mensch, kein Richter könnte von sich behaupten, alle für ein Urteil relevanten Fakten und Hintergründe zu kennen. Doch da wir handeln müssen, müssen wir auch mit Halbwissen urteilen.

Und genau hier beginnt das Dilemma. Je mehr wir wissen, desto schwerer fällt es uns, ein Urteil zu fällen. Entgegenstehende Fakten trüben den Blick, lassen die Konturen von schwarz und weiß, von richtig und falsch unscharf werden. Das mag einer der Gründe sein, warum Vorurteile und generalisierte Bewertungen etwas bestechend Verlockendes an sich haben: Sie sind klar, rein, einfach – leider aber (fast) immer falsch. Denn sie zeichnen ein überscharfes (Zerr-) Bild der Wirklichkeit, das die komplexe, vielschichtige „Wahrheit" bestenfalls in einer ganz bestimmten Perspektive widerspiegelt.

Können wir einen Menschen mit irgendeiner Information in Verbindung bringen, fällen wir also unvermeidlich ein (wahrscheinlich ungerechtes) Urteil – sogar dann, wenn die Information unzuverlässig, sachfremd oder in diesem Kontext irrelevant ist. Genau deshalb brauchen wir Anonymität: Sie allein schafft einen urteilsarmen Raum, in dem neutraler Respekt und unvoreingenommener Umgang zwischen Menschen möglich wird. Und damit freie Entfaltung.

Am 10.07.2020 machte ein Beitrag auf netzpolitik.org das polnische Startup PimEyes bekannt, das aus im Internet verfügbaren Bildern biometrische Daten von mehr als 900 Mio. Gesichtern gewonnen haben will. Es bietet Gesichtsidentifikation für jedermann – der Anfang vom Ende der Anonymität. Wer aber anonyme Räume zerstört, schafft freie Entfaltung ab.

Inhalt

secorvo
security consulting

Security News

Ende des Privacy Shields

Der Europäische Gerichtshof hat am 16.07.2020 – wie von europäischen Datenschutzexperten erwartet – den Kommissionsbeschluss zum EU-US-Privacy Shield für ungültig erklärt. Auch die Standardvertragsklauseln werden im Urteil sehr kritisch beurteilt und dürften als Rechtsgrundlage für viele der bisher über das Privacy Shield legitimierten Verarbeitungen in den USA ausscheiden: Mit Rechtsvorschriften wie dem CLOUD Act (SSN 3/2019) garantiere das amerikanische Recht nach Auffassung des EuGH keinen dem EU-Recht äquivalenten Schutz personenbezogener Daten.

Damit hat der EuGH der Verarbeitung europäischer personenbezogener Daten in den USA, aber auch durch Töchter amerikanischer Unternehmen in Europa eine deutliche Absage erteilt – wer es dennoch tut, ist in der Nachweispflicht. Das wird auch aus den FAQ des europäischen Datenschutzausschusses zum Urteil deutlich, die dieser am 23.07.2020 veröffentlichte. Sollten die Aufsichtsbehörden nun gezielt Verarbeitungen personenbezogener Daten europäischer Bürger durch amerikanische Unternehmen mit Bußgeldern ahnden, dürfte eine Schockwelle durch Online-Marketing-Abteilungen schwappen.

Bußgeld für die AOK

Am 30.06.2020 teilte der Baden-Württembergische Beauftragte für Datenschutz und Informationssicherheit mit, dass seine Behörde gegen die AOK Baden-Württemberg ein Bußgeld in Höhe von 1,24 Mio. € verhängt hat. Im Zusammenhang mit Gewinnspielen hatte die AOK personenbezogene Daten erhoben und zu Werbezwecken verwendet; in mehr als 500 Fällen lag die dafür notwendige Einwilligung jedoch nicht vor. Bei der Bußgeldbemessung (SSN 10/2019) wurden das kooperative Verhalten der Krankenkasse, ihre Bedeutung für das Gesundheitssystem sowie die Belastung durch die Corona-Pandemie berücksichtigt. Wie hoch wäre es wohl ausgefallen, wenn diese begünstigenden Faktoren nicht vorgelegen hätten?

Angesichts unzureichender, aber immerhin vorhandener Maßnahmen und eines vergleichsweise geringen Anteils an rechtswidriger Werbeverwendung erscheint die Bußgeldhöhe kaum verhältnismäßig. Doch steigt damit der Druck auf Unternehmen, ihre Datenschutzumsetzung in der Praxis wirksamer zu überwachen.

Lunchgate

Die Sicherheitsfirma modzero veröffentlichte am 07.07.2020 eine Schwachstelle in der um eine Kontaktdatenfunktion erweiterte Tisch-Reservierungs-App des Schweizer Startups Lunchgate. Dem Bericht „Mit Webapps gegen COVID-19“ zufolge handelt es sich dabei um eine sogenannte Insecure Direct Object Reference, durch die alle erfassten Daten öffentlich einsehbar waren. Dabei fiel auf, dass Lunchgate die Kontaktdaten mindestens 21 statt der maximal zulässigen 14 Tage speichert. Lesen bildet: Ein Blick in die OWASP Cheat Sheets, hier konkret in das Insecure Direct Object Reference Prevention Cheat Sheet, hätte den Entwicklern geholfen, diese Lunchgate-Affäre zu vermeiden.

DSFA für CWA

Als die Corona-Warn-App (CWA) am 16.06.2020 zur Nutzung bereitgestellt wurde, hatte das Robert-Koch-Institut (RKI) erst vier Tage zuvor die zugehörige Datenschutz-Folgenabschätzung (DSFA) abgeschlossen. Der 117 Seiten lange Bericht dürfte eine der bislang meistdiskutierten und am besten durchleuchteten DSFA seit dem Inkrafttreten von Art. 35 DSGVO sein. Er orientiert sich am Standard-Datenschutzmodell (SDM) und berücksichtigt sämtliche in Art. 35 Abs. 7 DSGVO vorgegebenen Inhaltsbestandteile. So sind der Ablauf aus Nutzersicht, die Systemarchitektur, die Funktionsweise, die rechtliche Bewertung, die Analyse der Risiken für die Betroffenen und die getroffenen Maßnahmen ausführlich dokumentiert.

Dennoch werden dem Bericht datenschutzrechtliche Unerfahrenheit, Zielverfehlung (Legitimation statt Risikominimierung) und erhebliche Lücken attestiert, bspw. bei der Betrachtung der verwendeten Serverkomponenten und der möglichen Verknüpfung der Positivschlüssel mit den IP-Adressen bei der Übermittlung. Weitere Kritikpunkte sind das Ausklammern der Risiken durch das nicht kontrollierbare *Exposure Notifikation Framework* (ENF) von Apple und Google, durch das bestimmte Verarbeitungsschritte fremddiktiert werden, oder die Methodik der Risikobetrachtung. Die teilweise berechtigten Kritikpunkte erscheinen jedoch angesichts der Umstände (politischer Druck, Zeitdruck, vermeintliche Bedeutung der App) entschuldbar – zumal die öffentliche Diskussion über die Datenschutzkonformität der CWA zweifelsfrei dem Datenschutz gedient hat.

Bundesgenossen

Das Bundeskartellamt hat am 01.07.2020 den Abschlussbericht zur bereits im Dezember 2017 begonnenen Sektoruntersuchung zu Smart-TVs vorgelegt. Anlass der Untersuchung war der Verdacht auf erhebliche, dauerhafte Verstöße gegen verbrau-

cherrechtliche Vorschriften - mit einem Schwerpunkt beim Datenschutz.

Der Bericht dokumentiert erhebliche Datenschutzmängel wie zu pauschal bezeichnete Rechtsgrundlagen und Zwecke (bspw. „Verbesserung der angebotenen Dienste“), zu komplexe, unverständliche und zugleich undifferenzierte Datenschutzerklärungen, fehlende Angaben zu den verarbeiteten Daten, mangelnde Datensicherheit oder unerlaubte Werbung.

Dank des 9. Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) hat das Kartellamt seit dem 08.07.2017 mit § 32e Abs. 5 GWB die Befugnis zur Prüfung von Wirtschaftszweigen auf die Einhaltung von Verbraucherschutzrecht. Zuletzt hatte sich das Bundeskartellamt im Februar 2019 bereits mit dem Datenschutz bei Facebook beschäftigt (SSN 2/2019). Sollten weitere derartige Berichte folgen, könnte das Bundeskartellamt zu einem relevanten Player im Datenschutz werden.

Nun sind die Datenschutzaufsichtsbehörden aufgerufen, die im Bericht festgestellten Mängel aufzugreifen, dessen Untersuchungstiefe über viele Betrachtungen der Aufsichtsbehörden deutlich hinausgeht.

Videokonferenzsysteme – revisited

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit hat am 03.07.2020 vier einander ergänzende Dokumente zu Videokonferenzsystemen, darunter eine ausführliche Bewertung führender Angebote (u. a. GoToMeeting, Jitsi, Google Meet, Teams, Skype, WebEx und Zoom) samt Handlungsempfehlungen für Unternehmen und Behörden vorgelegt und damit ihre erste Stellungnahme vom 08.04.2020 (SSN 5/2020) ergänzt.

Der Checkliste zufolge soll vor jeder Videokonferenz geprüft werden, ob nicht eine Telefonkonferenz ausreicht. Weiter sollen selbst betriebene Dienste vorgezogen werden, da die vorhandenen Angebote überwiegend als „nicht rechtskonform einsetzbar“ eingestuft werden. Dabei wird zum einen auf das (derzeit für solche Telemediendienste noch nicht anwendbare) Telekommunikationsgeheimnis verwiesen; zum anderen geht die Prüfung davon aus, dass das organisierende Unternehmen grundsätzlich Auftragsverarbeitungsverträge schließen müsse – und diese würden für Teams, Google Meet und Co. nicht ausreichend angeboten.

Nicht näher analysiert wird allerdings, ob die Voraussetzungen für eine Auftragsverarbeitung überhaupt regelmäßig vorliegen. Hieran bestehen Zweifel, denn nicht jedes der Angebote muss als Dienst mit fester Nutzeranmeldung betrieben werden. Und selbst dann ist fraglich, warum die damit verbundene Übermittlung dienstnotwendiger Daten nicht zu rechtfertigen sein soll. Die Untersuchung reiht sich damit leider in eine Reihe durch die Corona-Krise ausgelöster, überhasteter Stellungnahmen zu Videokonferenzsystemen ein, auch wenn die mit deren Einsatz verbundene grundsätzliche Problematik nicht in Abrede zu stellen ist.

Wieder einmal Störerhaftung

Seit dem 3. Gesetz zur Änderung des Telemediengesetzes (TMG), das die Störerhaftung von WLAN-Betreibern durch die Neufassung von § 8 TMG begrenzen sollte, ist es um Filesharing-Urteile ruhig geworden. Daher sorgte die (noch nicht rechtskräftige) Verurteilung einer älteren Dame, die nach eigenen Angaben einen offenen WLAN-Knoten betrieben aber selbst nicht genutzt hatte, durch das Amtsgericht Köln vom 08.06.2020 für Aufsehen. Um den Erstattungsanspruch abzuwehren hätte sie nach Auffassung des Gerichts konkrete Nutzer im fraglichen Zeitpunkt benennen müssen.

Eine Rückkehr zur Störerhaftung ist trotz dieses Urteils zum Glück nicht zu fürchten. Allerdings ist es keine gute Entwicklung, dass durch subtile Differenzierungen des Klägers unkundige WLAN-Betreiber ohne anwaltliche Vertretung – wie in diesem Fall – Gefahr laufen, verurteilt zu werden.

Secorvo News

Endlich wieder... Seminare

Nach langer Pause können wir Ihnen im September wieder die Möglichkeit bieten, Ihre Kenntnisse und Kompetenzen in der IT-Sicherheit zu aktualisieren – und zu zertifizieren: für das Teilgebiet des sicheren Software-Engineerings (T.P.S.S.E., **14.–17.09.2020**) und das Zertifikat als TeleTrust Information Security Professional (T.I.S.P., **21.–25. 09.2020**).

Zur Vorbereitung auf das Seminar und die T.I.S.P.-Prüfung erhalten Sie nach Ihrer Anmeldung unser Begleitbuch „Informationssicherheit und Datenschutz“, das im vergangenen Herbst in dritter Auflage im dpunkt-Verlag erschienen ist – und sich inzwischen zahlreicher positiver bis begeisterter Kritiken erfreut. Wer also noch eine Sommerlektüre sucht...

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

August 2020	
06.-09.08.	DEF CON 28 (Defcon, Las Vegas/US)
07.-11.08.	SOUPS 2020 (usenix, Boston/US)
12.-14.08.	29th USENIX Security Symposium (usenix, Boston/US)
17.-21.08.	Crypto 2020 (IACR, Santa Barbara/US)
September 2020	
07.-11.09.	IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/IT)
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-22.09.	Security of Things World (we.CONECT Global Leaders GmbH, Berlin)
21.-25.09.	T.I.S.P. – TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)
24.09.	IT-Sicherheitsrechtstag (TeleTrusT e.V., Berlin)
29.09.-01.10.	IT-Sicherheit - praxisnah und aktuell (Secorvo, Karlsruhe)
29.09.-02.10.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)

Fundsache

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe hat am 16.06.2020 den Umsetzungsbericht 10 Jahre „KRITIS-Strategie“ veröffentlicht. Der bietet vertiefte Einblicke in die Risikobewertung und den Schutz der verschiedenen Sektoren kritischer Infrastrukturen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

August 2020

Vermintes Terrain

Bei manchen Gelegenheiten sollte man zurückhaltend sein, Kenntnisse in der IT-Sicherheit oder dem Datenschutz durchblicken zu lassen. Zum Beispiel beim Abendessen mit Freunden. Eine der sich nach einem solchen „Coming Out" geradezu schicksalhaft ergebenden Fragen, die jeden noch so zauberhaften Abend irreparabel pulverisieren kann, ist – pars pro toto – diese hier: „Ist Whatsapp eigentlich sicher?"

Wo soll man da anfangen – und was lieber verschweigen? Dass die Kontaktdaten des Smartphones an Whatsapp übertragen werden? Dass eine solche Übermittlung von Daten Dritter in die USA rechtswidrig ist? Dass Whatsapp sich die Rechte an allen Inhalten übertragen lässt? Dass Whatsapp nach eigenen Angaben Ende-zu-Ende-Verschlüsselung realisiert? Dass man diese Behauptung nicht sicher bestätigen kann – schließlich könnte es ja eine „Hintertür" geben? Dass verlinkte Inhalte nicht in die Verschlüsselung eingeschlossen sind? Dass Whatsapp-Videochats ohnehin unverschlüsselt übertragen werden? Dass das vielleicht gar nicht die wichtigste Frage ist, da die Verbindungsdaten ein „digitales Bewegungsbild" liefern? Dass Whatsapp zum Facebook-Konzern gehört – und dass für diesen Verbindungsdaten ohnehin wertvoller sind als Kommunikationsinhalte? Dass „ich hab' ja nichts zu verbergen" das denkbar ignoranteste Argument gegen Datenschutz ist? Dass „Soziale Netzwerke" keine Sozialkontakte ersetzen sollten? Dass Bewegung für die Entwicklung der Sprösslinge besonders wichtig ist – und zwar nicht nur für die Daumen? Und – spätestens hier werden Sie mit hoher Wahrscheinlichkeit enthauptet – dass die Vermittlung von Digitalkompetenz und der damit einhergehenden „digitalen Souveränität" wichtiger sein sollte als die Befürchtung sozialer Ausgrenzung, und es sich daher lohnt, sich dem Anpassungsdruck entgegenzustellen?

Wissen kann manchmal einsam machen.

Inhalt

secorvo
security consulting

Security News

Folgen von „Schrems II“

Nach dem Urteil des EuGH zur Ungültigkeit des EU/US Privacy-Shield (C-311/18) vom 16.07.2020 hat Google mit ersten Hinweisen zur Neugestaltung seiner Datenübermittlungen in die USA reagiert und erweitert seine Vertragsbedingungen für Werbeprodukte und Google Analytics um Standardvertragsklauseln. Zudem kann der Anwender bei Beauftragung aktuell entweder die Variante "Auftragsverarbeitung" für verschiedene Dienste, darunter Analytics, oder unabhängige Verantwortung ankreuzen. Die Einordnung als gemeinsame Verantwortung der DSK vom 12.05.2020 wird damit nicht umgesetzt. Google hält seine Anwender zudem zum Einholen von Einwilligungen der Nutzer an, stellt hierzu auch Hilfen zur Verfügung und verweist auf seine Informationen zur Datennutzung.

Diese Reaktion wird von Max Schrems und der neu gegründeten Initiative „My Privacy is None of Your Business“ als unzureichend angesehen. Um die Aufsichtsbehörden zur Urteilsdurchsetzung zu zwingen hat die Initiative daher Seiten großer Unternehmen gescannt und Beschwerden über die fortgesetzte Nutzung eingereicht; inzwischen liegen Beschwerden gegen 101 Unternehmen in 30 EU-Staaten vor.

Auch die Haltung der deutschen Aufsichtsbehörden ist eindeutig, wie u. a. die Stellungnahme des LfDI Baden-Württemberg vom 25.08.2020 belegt. „Retten“ lässt sich die Situation wohl allein durch eine technische Beschränkung der Datenverarbeitung auf Europa und eine aufklärende Erneuerung der Informationen zur Datennutzung seitens Google – oder den konsequenten Verzicht auf die Nutzung dieser Dienste.

Alt und anfällig...

E-Mails dominieren weltweit sowohl die private als auch die Unternehmenskommunikation. Das dabei verwendete „Simple Mail Transfer Protocol“ (SMTP) feierte in diesem Monat seinen 38. Geburtstag – und stammt aus einer Zeit, in der Sicherheitsmechanismen noch nicht zu den Kernfunktionen eines Protokolls zählten. Passenderweise stellten drei Forscher am 06.08.2020 auf der Blackhat USA 18 Angriffe auf E-Mail-Sender-Authentisierung vor und zeigten, wie anfällig E-Mail-Infrastrukturen auch mit nachträglich eingebauten Sicherheitsmechanismen wie SPF, DKIM und DMARC sind. Sicherheitsaufsätze stoßen auch hier an ihre Grenzen.

Angriffe mit gefälschten Absendern zählen derzeit zu den erfolgreichsten Wegen, Schadsoftware zu verbreiten, wie der unlängst wiederbelebte Emotet demonstriert. Aufgrund der veralteten Architektur wird E-Mail auch mit Sicherheitsaufsätzen auf lange Zeit unsicher bleiben. Daher müssen neben technischen Schutzmaßnahmen vor allem auch die Menschen über die Fallstricke von E-Mail aufgeklärt werden.

Qualifikation des DSB

Das Landesarbeitsgericht (LAG) Mecklenburg-Vorpommern hat am 25.02.2020 über die Abberufungsvoraussetzungen eines Datenschutzbeauftragten (DSB) entschieden. Dabei traf es eine Reihe von Feststellungen zu den erforderlichen Qualifikationen und zum Pflichtumfang des DSB. Zur Qualifikation stellt das LAG fest, dass ein Volljurist mit Rückgriff auf technisches Personal zur Klärung von Fragen ohne weiteres über die erforderliche Fachkenntnis verfügt bzw. Datenschutzrecht korrekt anwenden kann.

Bezüglich der Pflichten war streitig, ob der DSB durch eine unterbliebene Verarbeitungsbeanstandung und einen Hinweis im Januar 2018, die DSGVO könne erst mit Geltung umgesetzt werden, seine Pflichten verletzt habe. Hierzu führt das LAG aus, dass ein DSB bei mehreren Betrieben und umfangreicher Datenverarbeitung zwangsläufig Prioritäten setzen muss. Durch Schulungen, Bearbeitungen von Anfragen und Mitwirkung in entsprechenden Unternehmensgremien hat er seine Pflichten erfüllt. Für die Einhaltung des Datenschutzes ist letztlich das Unternehmen verantwortlich. Dies galt auch für die Vorbereitungen zur Umsetzung der DSGVO.

Die Position des DSB wird durch das Urteil gestärkt, gleichzeitig werden die Anforderungen an seine Tätigkeit auf eine realistische Erwartung beschränkt. Als Orientierung für die Aufgabenbeschreibung bietet das Urteil hilfreiche Bezüge.

Listen to the Key

In ihrem am 24.08.2020 als Videoaufzeichnung erschienenen Vortrag von der HotMobile 2020 stellten Sicherheitsforscher der National University of Singapore einen neuen Angriff auf physische Schließsysteme vor. Die Forscher konnten zeigen, dass Angreifer neben dem bekannten Lockpicking auch das Geräusch eines ins Schloss geschobenen Schlüssels analysieren können. Denn aus dem z. B. mittels Smartphone-Mikro aufgezeichneten Geräusch der Pins beim Einschieben lässt sich das Profil des Schlüssels errechnen und ein passender Nachschlüssel fräsen – vorausgesetzt, der Angreifer kennt den Typ von Schloss und Schlüssel und der Schlüssel wird mit gleichmäßiger Geschwindigkeit eingeschoben. Eine App, die aus einer Audio-Aufnahme automatisch Nachschlüssel erzeugt, liegt also immerhin noch in einiger Ferne.

Bei dem Angriff handelt es sich um einen typischen Seitenkanalangriff. Darüber lassen sich häufig auch gute „primäre“ Schutzmechanismen umgehen: So kann beispielsweise ein grundsätzlich sicheres Kryptoverfahren einem Angreifer über Laufzeit- oder Spannungsunterschiede bei der Berechnung die Rekonstruktion des Schlüssels oder Klartextes ermöglichen. Solche Angriffe wurden u. a. bei der Mifare DESFire-Karte gezeigt. Andere Seitenkanalangriffe sind ein Passwortdiebstahl durch Aufzeichnung der Tippgeräusche oder Wärmebildaufnahmen der Tastatur. Die Härtung gegen Seitenkanalangriffe ist allerdings eine herausfordernde Angelegenheit.

Out of Scope

Dass beauftragte Einbrüche – ob digital als Penetrationstest oder physikalisch beispielsweise als Bestandteil eines Red-Team-Assessments – immer auch mit Risiken verbunden sind, hat der Fall zweier amerikanischer Penetrationstester eindrucksvoll gezeigt. Als diese am Abend des 11.09.2019 im Rahmen eines größeren, vom Staat Iowa beauftragten Assessments zum Testen des Alarmsystems durch eine offene Tür in das Dallas County Courthouse in Iowa eingedrungen waren, verließen sie das Gebäude in Handschellen – obwohl sie die schriftliche Freigabe für das Assessment mit sich führten und sich gegenüber den Beamten identifizieren konnten. Nach mehr als fünf Monaten rechtlichen Trubels wurden die Pentester Ende Januar 2020 freigesprochen. Eine Zusammenfassung der gesamten Geschichte mitsamt „Lessons learned“ gaben die beiden nun auf der Blackhat 2020.

Hilfreich war, dass ihr Arbeitgeber Coalfire sich unermüdlich für die beiden Mitarbeiter einsetzte. Um ähnliche Vorfälle zu vermeiden, rät Coalfire Auftraggebern und Pentestern, Vereinbarungen zum Ablauf eines Assessments immer schriftlich zu dokumentieren und die zugehörigen Vertragsunterlagen im Vorfeld von Juristen überprüfen zu lassen.

Auch klassische Penetrationstests können mit ähnlichen Risiken verbunden sein, wie der Fall von Rob Fuller zeigt: Durch einen winzigen Schreibfehler im vom Kunden genannten IP-Adressblock wurde das falsche Unternehmen angegriffen. Obwohl es in diesem konkreten Fall ohne negative Folgen blieb (und sogar zu einem neuen Kunden führte), hätten auch hier rechtliche Konsequenzen drohen können. Die eindeutige Klärung des Auftragsumfangs und der Zielobjekte („In Scope“/„Out of Scope“) muss deshalb zentraler Bestandteil einer jeden Vereinbarung zu einem Security Assessment sein.

Vergissmein(nicht)?

Der Bundesgerichtshof (BGH) entschied am 27.07.2020 bezüglich zweier Verfahren, wann Suchergebnisse durch Google zu löschen sind. Im ersten Fall konnte der Betroffene nicht erreichen, dass direkt auf ihn beziehbare Daten entfernt werden, da die Grundrechtsabwägung keinen Vorrang seines Schutzinteresses ergab. Das zweite Verfahren wurde ausgesetzt und mit weiteren Fragen an den Europäischen Gerichtshof (EuGH) für eine Vorabentscheidung eingereicht. Darin muss die Frage beurteilt werden, ob Google – nach Auffassung der Kläger – inhaltlich falsche Artikel eines Unternehmens über die Betroffenen löschen muss.

Im Urteil C-507/17 vom 24.09.2019 beschied der EuGH, dass Betreiber nicht verpflichtet sind, Auslistungen in sämtlichen Versionen ihrer Suchmaschinen vorzunehmen, sondern diese auf alle mitgliedstaatlichen Versionen beschränkt werden können. Aufgrund nationaler Datenschutzstandards können die Behörden eines Mitgliedsstaates jedoch eine Löschung in allen Versionen verlangen. Auch daraus wird deutlich, dass das in Art. 17 der DSGVO verankerte Recht auf „Vergessenwerden“ immer für den konkreten Einzelfall betrachtet werden muss.

Secorvo News

KA-IT-Si-Stammtisch

Aufgrund der nach wie vor geltenden Auflagen im Veranstaltungsbereich können wir unsere KA-IT-Si-Events nicht wie gewohnt durchführen. Daher möchten wir mit unserem ersten „KA-IT-Si-Stammtisch“ am **Donnerstag, 24.09.2020**, ab 18 Uhr im Biergarten der „Ersten Fracht“ in Karlsruhe (direkt gegenüber dem Hauptbahnhof) eine Plattform für den Austausch bieten.

Dort erwarten Sie vier verschiedene Thementische mit Andreas Sperber von aramido (Penetrationstests – das Was und Wie), Dr. Ingmar Baumgart vom FZI (Vulnerability Disclosure), Dirk Fox von Secorvo (Phishing-Awareness) und Oliver Winzenried von WIBU-Systems (Karlsruher „House of IT-Security“ und die zukünftige IT-Security Coworking Area). Die Ansprechpartner werden die Diskussionen mit einer kurzen Einführung in das Thema anstoßen.

Bei Interesse reservieren wir Ihnen gerne einen Platz an Ihrem ausgewählten Thementisch. Bitte melden Sie sich dafür bis Dienstag, 22. September 2020 an (keine Teilnahmegebühr, Bewirtungskosten exklusive).

Secorvo Seminare

Eine Terminübersicht, ausführliche Programme und die Möglichkeit zur Online-Anmeldung finden Sie auf unserer Webseite.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

September 2020	
07.-11.09.	IEEE European Symposium on Security and Privacy (IEEE Computer Society, Genua/IT)
14.-17.09.	T.P.S.S.E. - TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)
21.-22.09.	Security of Things World (we.CONECT Global Leaders GmbH, Berlin)
21.-25.09.	T.I.S.P. (TeleTrusT Information Security Professional) (Secorvo, Karlsruhe)
22.09.	Datenschutztag 2020 (COMPUTAS. Köln)
24.09.	IT-Sicherheitsrechtstag (TeleTrusT e.V., Berlin)
29.09.-01.10.	Informatik 2020 (GI Gesellschaft für Informatik, Karlsruhe)
29.09.-02.10.	Blackhat Asia 2020 (Blackhat, Singapur/SIN)
Oktober 2020	
12.-14.10.	ISSE 2020 (IEEE, Wien/A)
13.10.	Swiss Cyber Storm (Swiss Cyber Storm Association, Bern/CH
22.-23.10.	heise devSec 2020 (dpunkt.verlag, heise Developer, heise Security, Heidelberg

Fundsache

Der Vortrag My Cloud is APT's Cloud: Investigating and Defending Office 365 zeigt bekannte und weniger bekannte Angriffe auf Microsofts Cloud-Lösungen auf, die in Zeiten von Covid-19 immer mehr an Bedeutung gewonnen haben.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news")

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

September 2020

Wehret den Anfängen

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

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

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

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

Inhalt

secorvo
security consulting

Security News

Keine Biometrie zur Zeiterfassung

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

Bereits das erstinstanzliche Gericht hatte die für den Fingerabdruckabgleich gespeicherten „Minuten" als biometrische Daten gemäß Art. 9 Abs. 1, 4 Nr. 14 DSGVO eingeordnet. Demzufolge sei nach der Eignung zunächst zu prüfen, ob kein gleich wirksames, das Persönlichkeitsrecht weniger beeinträchtigendes Mittel existiere. Trotz der vorgetragenen abstrakten Manipulationsgefahr hat das LArbG Chipkarten oder Tokensysteme als gleich wirksam angesehen und damit die Erforderlichkeit im Kontext der betrieblichen Zeiterfassung verneint. Erst wenn die Erforderlichkeit bejaht worden wäre, hätten die vorgetragenen Schutzmaßnahmen (Nichtauslesbarkeit, Pseudonymisierung u.a.) im Rahmen einer Abwägung berücksichtigt werden können.

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

Schlüsselkasten

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

KISS

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

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

Minimalismus als Grundprinzip für Container, Bibliotheken (SSN 03/2019) und (Browser-)Plugins (SSN 04/2020) hilft auch gegen LOL-Angriffe: Die Angriffsfläche wird reduziert, die Angriffsresilienz erhöht. Lassen Sie weg, was nicht unbedingt nötig ist.

Darf ich mal sehen?

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

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

Einwilligungs-Standards

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

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

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

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

Totgesagte leben ewig

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

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

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

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

Secorvo News

Seminarbetrieb wieder aufgenommen

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

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

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

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

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

https://www.secorvo.de/seminare

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

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

Fundsache

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

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Oktober 2020

Deep Fakes

Seit Jahrzehnten durchzieht eine zentrale Frage die IT-Sicherheit: Wie kann ein IT-System zuverlässig feststellen, ob eine natürliche Person, die sich am System anmeldet, tatsächlich diejenige ist, die sie zu sein behauptet? Dass Passwörter zwar die vielleicht einfachste, aber keineswegs ideale Lösung für dieses Problem sind, wissen wir seit Langem. Besser ist die Prüfung verschiedener Merkmale wie der Besitz eines Tokens (Smartcard, EC-Karte, ...) oder der Zugang zu einem E-Mail-Account bzw. einem Telefonanschluss. Auch die Analyse biometrischer Daten mittels Fingerabdruckscannern, Stimm- oder Gesichtserkennung verbreitet sich dank deren technischer Weiterentwicklung (und aller Kritik zum Trotz).

Während Authentifikationen dadurch zuverlässiger, aber auch immer (zeit-)aufwändiger werden, erzeugt die Weiterentwicklung der Verfahren zugleich ein ganz neues Problem. Denn von der Extraktion eindeutiger Erkennungsmerkmale ist der Weg zur Synthese oft nicht besonders weit. Bilder (Gesichter) und Filme (Bewegungen) lassen sich heute auf beeindruckende Weise digital nachbilden. Durch den Einsatz lernender Algorithmen wird inzwischen auch die Fälschung des gesprochenen Worts zum Kinderspiel. So lassen sich nicht nur Inhalt, Wortwahl und Satzbildung imitieren (eindrucksvoll demonstriert von „The New Yorker“ im Jahr 2017 mit einer synthetisch erzeugten Rede von Donald Trump). Mit „Voice-Cloning“-Systemen wie Replica oder Lyrebird kann man inzwischen auch das gesprochene Wort selbst täuschend echt technisch erzeugen.

Daher könnten uns in unserer immer stärker medial vermittelten Wirklichkeit, in der auch persönliche Kontakte zunehmend per Telefon, Chat oder Video gepflegt werden, schon bald die in der „analogen Welt“ bewährten Erkennungsmechanismen verloren gehen. Bevor wir glauben, dass wir einen Kommunikationspartner tatsächlich sehen oder hören, warten wir womöglich in nicht allzu ferner Zukunft lieber erstmal dessen Passworteingabe ab.

Inhalt

secorvo
security consulting

Security News

Microsoft und der Datenschutz

Heftige Kritik erntete Baden-Württemberg für seinen Plan, Microsoft Office 365 in Schulen einzuführen. Kultusministerin Eisenmann wurde dafür am 28.09.2020 mit dem Big Brother Award 2020 ausgezeichnet. Bei der Bewertung sind sich jedoch auch die Datenschutz-Aufsichtsbehörden uneins: Die Datenschutzkonferenz beschloss am 23.09.2020 mit knapper Mehrheit die vorläufige, auf Verträgen vom Januar 2020 beruhende Einschätzung, Microsoft Office 365 sei derzeit nicht datenschutzkonform einsetzbar. Darauf reagierten die Landesdatenschutzbeauftragten des Saarlandes, Hessens, Bayerns und Baden-Württembergs am 02.10.2020 mit einer abweichenden gemeinsamen Stellungnahme, nach der sie zwar im Hinblick auf das EuGH-Urteil Schrems II erhebliches Verbesserungspotenzial sehen, die Frage jedoch ohne Anhörung von Microsoft und die Berücksichtigung aktueller Vertragsanpassungen für nicht entscheidungsreif halten. Der LfDI Baden-Württemberg, Dr. Brink, kündigte am 30.10.2020 an, das Pilotprojekt des Landes zur Einführung von Microsoft Office 365 an Schulen zu begleiten.

So viel ist jedoch klar: Beim Abschluss von Microsoft-365-Verträgen sollten die folgenden Punkte unbedingt schriftlich fixiert werden:

- Daten werden nur auf Servern innerhalb der EU gespeichert.
- Microsoft ist Auftragsverarbeiter und nimmt keine Rechte in Anspruch, die zur Verantwortlichkeit des Auftraggebers zählen (wie die Kontrolle über Unterauftragsverarbeiter etc.).
- Die Konfiguration ist so zu wählen, dass Daten nur übertragen werden, wenn es (aus Sicht des Verantwortlichen) tatsächlich notwendig ist.
- Datenübermittlungen in Länder ohne geeignetes Datenschutzniveau sind nur bei Vorliegen geeigneter Garantien erlaubt – dafür genügen die Standardvertragsklauseln ohne zusätzliche Schutzmaßnahmen regelmäßig nicht.

Bei Verträgen mit US-Anbietern besteht weiterhin das bisher ungelöste Problem des Cloud Acts, der amerikanische Unternehmen verpflichtet, US-Behörden auch den Zugriff auf solche Daten zu ermöglichen, die in Rechenzentren außerhalb der USA verarbeitet werden.

Dark Pattern

Am 07.09.2020 veröffentlichte das Bundesministerium für Justiz und Verbraucherschutz die Studie „Innovatives Datenschutz-Einwilligungsmanagement“, die die Ausgestaltung, Nutzerfreundlichkeit und Rechtskonformität von Einwilligungsmanagement-Modellen und Verbesserungsmöglichkeiten bewertet. Danach zielen viele Modelle darauf ab, Verbraucherinnen und Verbraucher mittels so genannter Dark Pattern zu einer Einwilligung in Trackingmechanismen zu bewegen. Dieses Vorgehen kann strafrechtliche Relevanz besitzen: Nach § 42 Abs. 2 Nr. 2 BDSG ist mit bis zu zwei Jahren Freiheitsstrafe bedroht, wer sich personenbezogene Daten durch unrichtige Angaben erschleicht.

Unternehmen sollten daher genau prüfen, ob das auf der Webseite gewählte Verfahren zur Einwilligung Nutzern eine „echte“ Wahl lässt. Der Studie zufolge sind Nutzer durchaus bereit ihre Einwilligung zu erteilen – vorausgesetzt, sie wurden ordentlich informiert.

Täteropfer

Das US Treasury Department's Office of Foreign Assets Control (OFAC) warnte am 01.10.2020 in einem Advisory vor Zahlungen – auch durch Dritte – an Ransomware-Erpresser (SSN 06/2019) wegen möglicher Verstöße gegen Bestimmungen bestehender Handels- und Wirtschaftssanktionen. US-Bürgern sind bspw. nach dem International Emergency Economic Powers Act (IEEPA) oder dem Trading with the Enemy Act (TWEA) Zahlungen an Personen oder Institutionen untersagt, die sich auf der OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) befinden.

Entsprechende europäische Regelungen sind die EU-Verordnungen Nr. 2580/2001 und Nr. 881/2002. In Deutschland werden Verstöße nach den §§ 17 ff AWG geahndet, die auch „leichtfertiges Handeln“ einbeziehen: Eine Zahlung an den zunächst vermutlich unbekannten Erpresser kann dies erfüllen.

War ein Ransomware-Angriff erfolgreich, stehen Unternehmen (ohne aktuelles Backup) vor einem Dilemma: Die Chance auf ein schnelles, wenn auch nicht gesichertes Wiedererlangen der Daten und Unterbleiben der teilweise angedrohten Veröffentlichung (SSN 2/2020) gegen das mit einer Lösegeldzahlung verbundene Sanktionsrisiko. Lösbar erscheint dies nur durch Prävention: So hat z. B. die Cybersecurity and Infrastructure Security Agency (CISA) zusammen mit dem Multi-State Information Sharing & Analysis Center (MS-ISAC) am 30.09.2020 hierfür ein gemeinsames Dokument zum Umgang mit Ransomware veröffentlicht.

Sichere Online-Wahlen?

Am 30.09.2020 hat das BSI einen Entwurf der Technischen Richtlinie BSI TR-03162 vorgelegt, die

IT-sicherheitstechnische Anforderungen an eine Online-Wahl für Verwaltungsräte der Sozialversicherungen festlegt. Die Vorgaben sind schlüssig und definieren unter Rückgriff auf verschiedene BSI-Vorgaben wie das IT-Grundschutz-Kompendium und die IT-Grundschutz-Standards verpflichtende Anforderungen. Dabei werden die verschiedenen Phasen einer Wahl berücksichtigt und auch weitere Technische Richtlinien des BSI referenziert.

Nicht explizit betrachtet werden jedoch konkrete Anforderungen an die Absicherung von Anwendung und Anwendungskomponenten. Für das benannte Modellprojekt mag das ausreichen – die Einhaltung der für politische Online-Wahlen geltenden Wahlrechtsgrundsätze des Grundgesetzes (siehe die Ausarbeitung des Deutschen Bundestages zu Online-Wahlen vom 03.03.2014) kann die Richtlinie jedoch nicht garantieren.

Windows Open Source

Kurz vor dem 19. Geburtstag von Windows XP am 25.10.2020 postete ein anonymer Nutzer am 23.09.2020 auf 4chan unter /g/ eine Quellcode-Sammlung von Windows XP SP1, Windows Server 2003 RTM, Windows 2000 und weiteren älteren Windows-Betriebssystemen. Sie besteht aus früheren Quellcode-Leaks, die zum Teil seit Längerem in privaten Foren ausgetauscht wurden. Trotz einiger fehlender Komponenten konnten daraus funktionierende Windows-Versionen kompiliert werden.

Die mediale Aufmerksamkeit führte zu neuen Funden im Quellcode. So entdeckte ein Twitter-Nutzer die Root Signing Keys für Benutzerzertifikate in Microsofts NetMeeting. Und die für die EternalBlue-Schwachstelle (CVE-2017-0144) verantwortliche Funktion war schon zu Erscheinen von Windows XP mit einem Kommentar versehen, der vor dem gefährlichen Verhalten warnte.

Der Quellcode könnte ein gefundenes Fressen für White- und Blackhat-Hacker sein: So enthalten aktuelle Windows-Versionen zweifellos zahlreiche „alte“ Code-Fragmente oder ganze Komponenten. Der Sicherheitsforscher Tavis Ormandy demonstrierte im August 2019 sicherheitskritische Schwachstellen, die in fast allen Windows-Versionen der letzten Jahrzehnte enthalten waren. Zwar hatten zahlreiche Unternehmenskunden über Microsofts „Shared Source Initiative“ schon lange Zugriff auf den Code, aber die allgemeine Verbreitung könnte die Aufdeckung bisher versteckt gebliebener Schwachstellen kurzzeitig beflügeln.

Jäger und Sammler

Am 06.10.2020 hat der Europäische Gerichtshof zum dritten Mal zur Vorratsdatenspeicherung (diesmal in Großbritannien, Belgien und Frankreich) geurteilt. Darin bestätigt er erneut, dass eine anlasslose und undifferenzierte Speicherung von Verkehrs- und Standortdaten der Telekommunikation einen schweren Eingriff in die Grundrechte der Betroffenen darstellt. Dennoch wird die Anordnung einer Vorratsdatenspeicherung nicht vollständig ausgeschlossen; es bedarf allerdings einer tatsächlichen, gegenwärtigen oder vorhersehbaren Gefahrenlage, etwa eines unmittelbar bevorstehenden oder erfolgten Angriffs auf die nationale Sicherheit. Auch die Bekämpfung schwerer Kriminalität erfordert mindestens das Bestehen von Rechtsschutzmöglichkeiten für die Betroffenen. Die Urteile gründen auf der grundrechtskonformen Auslegung der Datenschutz-Richtlinie für elektronische Kommunikation (2002/58/EG) und legen den Spielraum für eine eventuelle Verordnung zur elektronischen Kommunikation (ePrivacy-Verordnung) fest. Ob die Regelungen der §§ 113b ff TKG dem standhalten darf bezweifelt werden: Das Urteil könnte also auch Folgen für die Rechtslage in Deutschland haben.

Secorvo News

Rätsel lösen und Preis gewinnen

Vor fünf Jahren ging „Krypto im Advent“ – eine Initiative von Secorvo in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe – mit über 1.000 Anmeldungen an den Start. Im vergangenen Jahr begeisterte der Online-Adventskalender, der Kinder und Jugendliche spielerisch an Verschlüsselungstechniken heranführt, bereits mehr als 3.500 Teilnehmer. Dabei gilt es, täglich spannende Verschlüsselungs-Rätsel zu lösen, um einen von über 200 Sachpreisen zu gewinnen.

Auch Schulklassen und Profis können miträtseln, letztere allerdings außer Konkurrenz. Anmeldungen sind ab sofort auf Krypto-im-Advent.de möglich – die Teilnahme ist wie immer kostenlos.

Seminarangebot 2021

Wir hoffen Ihnen im kommenden Jahr unsere Präsenzseminare wieder in der bekannten Qualität anbieten zu dürfen. Alle Seminarthemen, Termine und Programme finden Sie unter

https://www.secorvo.de/seminare

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

November 2020	
03.-04.11.	T.I.S.P. Community Meeting (TeleTrusT, Berlin)
09.-13.11.	ACM CCS 2020 (ACM/SIGSAC, Orlando/US)
09.-12.11.	Black Hat Europe 2020 (BlackHat, London/UK)
13.-15.11.	FIfFKon20 (FIfF, Berlin)
18.-20.11.	44. DAFTA (GDD, Köln)
19.-20.11.	DeepSec 2020 (DeepSec, Wien/AT)
30.11.-01.12.	Cybersecurity 2020 (Handelsblatt/EUROFORUM, Berlin)
Februar 2021	
01.-02.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)

Fundsache

Am 09.10.2020 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Bericht zur Lage der IT-Sicherheit in Deutschland vorgelegt. Dabei wird die wachsende Verbreitung und Zunahme von Schadprogrammvarianten als die auch zahlenmäßig größte Bedrohung für die Informationssicherheit deutlich.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

November 2020

Unter den Wolken

Luftaufnahmen haftet etwas Magisches an. Vielleicht, weil sie aus einer Perspektive aufgenommen werden, die wir Menschen aus eigener Kraft nicht einnehmen können – es grüßt der ewige Traum vom Fliegen. Diese Faszination ist es wohl auch, die Menschen auf Türme, Berge und zu Ballonfahrten und Fallschirmsprüngen treibt.

Doch diese bislang seltenen Bilder werden selbstverständlicher: Dank leistungsstarker Servo-Motoren, verbesserter Batterie-, Funk- und Kameratechnik sowie hochwertiger GPS-, Beschleunigungs- und Gyro-Sensoren liefern mit Videokameras bestückte Drohnen heute Aufnahmen, die zuvor bestenfalls aus Hubschraubern möglich waren.

Und das weckt Begehrlichkeiten. Drohnenflüge kosten nur einen mikroskopischen Teil eines Hubschrauberflugs, können fast überall gestartet werden und liefern Bilder in Echtzeit – perfekte Voraussetzungen für eine großflächige Überwachung des öffentlichen Raums. Im April wurden in Düsseldorf Drohnen zur Überwachung der Einhaltung der Corona-Kontaktbeschränkung eingesetzt.

Mitte November brachte die Firma DJI die Kamera-Drohne „mini 2“ auf den Markt: Mit nur 239 g darf sie von jedermann geflogen werden, überträgt Full-HD-Aufnahmen über eine Distanz von bis zu 10 km und erreicht eine Fluggeschwindigkeit von über 57 km/h. Bei einer Flugdauer von bis zu 30 Minuten und einer maximalen Flughöhe von 4.000 m ist der Wirkungskreis gewaltig. Die Motoren sind schon aus wenigen Metern Entfernung nicht mehr zu hören – und die nur 14 cm lange Drohne kaum noch zu erkennen.

Die Anschaffung eines Polizeihubschraubers kostet rund 5,8 Mio. €, Betriebs- und Flugkosten sowie die Pilotenausbildung nicht gerechnet. Für diesen Betrag erhält man – ohne Preisverhandlung – rund 13.000 Mini-Drohnen: für jeden vierten Bundespolizisten eine.

Schöne neue Überwachungswelt.

Inhalt

secorvo
security consulting

Security News

Vorsicht bei Gesundheits-Apps

Neben sogenannten „Medical Apps“ aus dem Lifestyle- und Wellness-Bereich wurden am 06.10.2020 die ersten „Gesundheits-Apps“ zugelassen, die es vom Arzt auf Rezept gibt und deren Kosten von den gesetzlichen Krankenversicherungen übernommen werden. In das DiGA-Verzeichnis aufgenommen werden die Apps ohne weitere sicherheits- und datenschutzrechtliche Prüfung durch die zuständigen Behörden nach einem an die CE-Kennzeichnung angelehnten „Fast-Track“-Verfahren: Die Hersteller geben eine Erklärung ab, in der sie versichern, dass sie die gesetzlichen Vorgaben einhalten. Dieses kursorische Verfahren bewertet der Landesbeauftragte für Datenschutz und Informationsfreiheit Rheinland-Pfalz kritisch – bei den ersten angebotenen „Apps auf Rezept“ wurden bereits erhebliche Sicherheits- und Datenschutzlücken festgestellt. Eine Überprüfung durch die zuständige Aufsichtsbehörde, das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM), fand erst im Nachgang statt. Wer solche Apps verschrieben bekommt oder freiwillig nutzen möchte, sollte sich zuvor genauer mit den Einstellungen beschäftigen. Blindes Vertrauen in solche Anwendungen ist jedenfalls nicht zu empfehlen.

Spurenarm Surfen

Wer im Internet „surft“ hinterlässt Spuren – unvermeidlich beim Anbieter der aufgerufenen Seite und fast immer zusätzlich bei eingebundenen Trackern, Werbeseitenanbietern, Diensten, Icons von Social Networks oder Schriftarten. Zwar dürfen IP-Adresse und Zugriffszeitpunkt nur mit Einwilligung der Betroffenen übermittelt und von den Empfängern zu eigenen Zwecken wie der Gewinnung von Werbe-Profilen genutzt werden – aber darum kümmern sich viele Anbieter wenig.

Schutz gegen solcherart unerwünschtes Tracking bieten nicht nur die Datenschutz-Grundverordnung, sondern auch Browser-Einstellungen und die Nutzung von Browser-Erweiterungen. Sie begrenzen das Tracking auf den Seitenanbieter, sperren lästige Werbeeinblendungen aus und verkürzen so, ganz nebenbei, die Ladezeiten von Webseiten merklich. Aber Achtung: Man sollte nur Browser-Erweiterungen installieren, denen man vertraut, sonst holt man sich leicht statt eines Privatsphärenschützers einen Spionagehelfer in den Browser (SSN 04/2020).

Bei den Browser-Einstellungen empfiehlt es sich, zumindest so genannte „Third-Party Cookies“ zu deaktivieren. Empfehlenswerte Browser-Erweiterungen sind beispielsweise der Privacy Badger oder HTTPS Everywhere der EFF. ClearURLs entfernt Tracking-Bestandteile aus URLs. Mit Decentraleyes werden lokale Ressourcen statt solcher von einem zentralen Content Delivery Network (CDN) injiziert. uBlock Origin blockiert nicht nur lästige Werbeeinblendungen sondern auch bösartige und gefährliche Domänen. Und wer sein Netzwerk bereits auf DNS-Ebene von einem dedizierten Gerät aus filtern möchte, dem empfiehlt sich Pi-hole. Zu guter Letzt kann man über „Cover Your Tracks“ (ehemals Panopticlick) prüfen, wie eindeutig der „Fingerprint“ des eigenen Browsers ist und was man dagegen tun kann.

Verräterische Uploads

Am 18.05.2020 berichtete die Investigativ-Journalismus-Webseite „bell¿ngcat“, wie mittels einer Bier-Bewertungs-App Militärpersonal identifiziert und vertrauliche Dokumente gefunden werden können: Manche der in Untappd hochgeladenen und mit einer Örtlichkeit (wie z. B. einer Bar) verknüpften Fotos des getrunkenen Bieres zeigen neben dem Bierglas Militärausweise, Kreditkarten und Militärdokumente. Jedes Besucher-Profil besitzt zudem eine „Timeline“ der Örtlichkeiten, an denen die Person bereits ein Foto hochgeladen hat. So konnten sogar geheime oder inoffizielle Militärbasen identifiziert und chronologische Abläufe von Reisen zwischen Militärbasen und privaten Aufenthaltsorten rekonstruiert werden.

Ähnliches erlaubt die „Heatmap“ der Fitness-App Strava: Wie Nathan Ruser bereits am 27.01.2018 erkannte, kann diese genutzt werden, um Militärbasen zu erkennen und detailliert zu kartographieren. Bereits am 08.07.2018 berichtete bell¿ngcat, wie dank der Fitness-App von Polar das Haus und die Jogging-Gewohnheiten eines hochrangigen Militäroffiziers einer Nuklearwaffenbasis herauszufinden waren – samt vollem Namen.

Auch Bewertungen auf Google Maps oder Amazon bieten Einblick in Aufenthaltsorte, Vorlieben und Gewohnheiten von Personen. Wenn diese Angaben z. B. über die Suche nach Benutzernamen, Aufenthaltsorten, Freunden, Bekannten oder Verwandten mit Daten anderer sozialer Netzwerke wie Swarm korreliert werden, ergibt sich schnell ein aussagekräftiges Gesamtbild.

Für Sammelpunkte, die Ernennung zum „Local Guide“ oder „Top Reviewer“ machen Menschen ihr Leben öffentlich und sich selbst zum freiwillig gläsernen Menschen. Beim nächsten Joggen, Biertrinken oder Bewerten sollte man vielleicht darüber nachdenken, ob man diese Spuren wirklich hinterlassen möchte.

secorvo
security consulting

Github Code Scanning

Nachdem Github am 18.09.2019 das Code-Analyse-Unternehmen Semmle übernommen hat, bietet Github auf Basis der CodeQL-Technologie seit dem 30.09.2020 auf Github automatisierte Code Scans an. Diese Funktionen wie Scans auf Schwachstellen im Code und den Abhängigkeiten oder auch die Suche nach hartkodierten Geheimnissen sind sowohl für Enterprise-Modelle als auch über öffentliche Repositories verfügbar. Sobald Änderungen am Code in ein Repository hochgeladen werden, können entsprechende Code Scans automatisch durchgeführt und Schwachstellen zeitnah ausfindig gemacht werden. Eine einfache Möglichkeit, Schwachstellen aufzudecken ohne in komplexe Technologien oder teure Werkzeuge investieren zu müssen. Insbesondere für finanziell häufig klamme Open-Source-Projekte ist dieses Angebot ein Mehrwert. Erste Erfahrungsberichte bestätigen das: Durch die Anpassungsmöglichkeiten an die jeweiligen Anwendungsumgebungen war es im Jenkins-Projekt möglich, sieben Schwachstellen in verschiedenen Plug-Ins zu identifizieren, die generische Code Scanner nicht finden konnten.

Datenschutz in Videokonferenzsystemen

Mit der zunehmenden Nutzung von Web- bzw. Videokonferenzen seit Beginn der Corona-Pandemie haben sich viele Datenschutzaufsichtsbehörden zu deren Zulässigkeit und zu den an diese zu stellenden Datenschutzanforderungen geäußert. Mit der neuen Orientierungshilfe der Datenschutzkonferenz (DSK) vom 23.10.2020 fassen die Aufsichtsbehörden nun (endlich) ihre Auffassung zusammen. Darin wird weiterhin von einem Auftragsverarbeitungsverhältnis zum Anbieter ausgegangen; dafür führt das Papier als neue Rolle die des „Veranstalters“ als Verantwortlichem ein. Für den Austausch von bspw. Gesundheitsdaten soll zuvor eine Einwilligung eingeholt werden, der Kommunikationskanal wird zur eigenständigen Inhaltsverarbeitung erklärt.

Mit der Checkliste zur Orientierungshilfe können Unternehmen überprüfen und dokumentieren, ob das von ihnen eingesetzte Tool den Anforderungen der Aufsichtsbehörden entspricht oder ob Nachbesserungsbedarf besteht, etwa bzgl. der vertraglichen Nutzungsgrundlagen, Betroffeneninformationen oder der technischen Einstellungen. Dabei erscheinen die Antworten auf die Checkpunkte durch die bekannten Einschätzungen der DSK bereits determiniert, sodass die Verantwortlichen lediglich zum bereits vorbestimmten Ergebnis (Unzulässigkeit) geführt werden. Die in ersten Stellungnahmen teilweise eklatanten Begründungsmängel setzen sich auch in den gemeinsamen Papieren abgeschwächt fort, daher ist der tatsächliche Nutzen leider begrenzt.

Hallo Admin

Am 10.11.2020 berichtete der Sicherheitsforscher Kevin Backhouse vom Github Security Lab, wie man mit einer einfachen Methode Administrator-Privilegien in der Desktop-Variante von Ubuntu 20.04 erlangen konnte. Hierfür leitete der Sicherheitsforscher die Datei „.pam_environment“ auf „/dev/zero“ um. Nach Änderung einer Benutzereinstellung (wie z. B. der genutzten Sprache) versucht der Hintergrunddienst „accounts-daemon“ die umgeleitete Datei einzulesen und landet in einer Endlosschleife. Danach kann der Dienst (durch ein eingebautes Sicherheits-Feature, das den Zugriff auf sensible Dateien verhindern soll) von einem normalen Benutzer zum Absturz gebracht werden.

Bei der nächsten Anmeldung wird der Benutzer dann von GNOME mit dem Dialog zur erstmaligen Einrichtung eines Administrator-Accounts begrüßt – da der Login-Manager nicht mit dem „accounts-daemon“ kommunizieren kann, nimmt er an, es gäbe keine Benutzer auf dem System.

Die Sicherheitslücke zeigt eindrucksvoll, wie sämtliche Schutzmaßnahmen sehr einfach durch das Versetzen des Systems in einen Ausnahmezustand umgangen werden konnten. Eine schöne Metapher für viele Sicherheitslücken – sind es doch oft Sonderfälle, die ausgenutzt werden können. Diese funktionieren übrigens auch beim Menschen: Versetzt man jemanden durch Zeitdruck, Androhung von Konsequenzen, Schmeicheleien o. ä. in einen Ausnahmezustand, fällt er auf Social Engineering herein.

Secorvo News

Adventsrätsel

Am 01.12.2020 startete die sechste Staffel des Adventsrätsels „Krypto im Advent“, einer Initiative von Secorvo in Zusammenarbeit mit der Pädagogischen Hochschule Karlsruhe. Sie führt jährlich rund 4.000 Kinder und Jugendliche spielerisch an Verschlüsselungstechniken heran. Dabei gilt es, über 24 Tage spannende Verschlüsselungs-Rätsel zu lösen, um einen der über 250 Sachpreise zu gewinnen.

Auch Schulklassen und Profis können miträtseln, letztere allerdings außer Konkurrenz. Anmeldungen sind auch nach dem 01.12. noch möglich (Krypto-im-Advent.de); die Teilnahme ist kostenlos.

Erzählen Sie es weiter – und rätseln Sie gerne mit!

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
01.-02.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, Hamburg)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)
März 2021	
03.-04.03.	Future Security 2021 (Fraunhofer VVS, Nürnberg)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Fundsache

Europol veröffentlichte am 05.10.2020 den Bericht "Internet Organised Crime Threat Assessment" (IOCTA): aktuelle Bedrohungen durch die organisierte Kriminalität auf gut 60 Seiten. Aufgeführt werden konkrete Beispiele wie die „Versteigerung“ geraubter Daten und Schwierigkeiten, z. B. auch in Deutschland die Infrastruktur von „Bulletproofed“-Hostern zu stören. Durchaus empfehlenswert, um sich einen Überblick über die aktuelle Bedrohungslage zu verschaffen und gegebenenfalls die eigenen Schutzmaßnahmen anzupassen.

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de

secorvo
security consulting

Secorvo Security News

Dezember 2020

Beweislastumkehr

Am 26.11.2020 hat die Datenschutzkonferenz der deutschen Aufsichtsbehörden (DSK) einen Beschluss zur Datenschutzkonformität von Windows 10 Enterprise gefasst. Das Dokument liest sich – selbst (oder gerade) für einen „in der Wolle gewaschenen" Datenschützer – äußerst befremdlich.

In aller Ausführlichkeit wird zunächst festgehalten, dass Microsoft mehrfach versichert hat, dass Windows 10 bei Konfiguration der Telemetrie-Stufe „Security" keine Telemetriedaten (Daten über das Nutzungsverhalten) an Microsoft übermittelt. Mit Bezugnahme auf eine (dem Beschluss beiliegende) BSI-Untersuchung vom Januar 2020 kommt die DSK zu dem Ergebnis, dass „Verantwortliche nicht abschließend von ihrer (...) Prüf- und Nachweispflicht für den datenschutzkonformen Einsatz von Windows 10 hinsichtlich der Übermittlung von Telemetriedaten" entlastet werden können. Dabei kommt die referenzierte BSI-Untersuchung zu dem Schluss, dass „sich keine Hinweise ergeben, dass Windows 10 Enterprise (...) Daten an Microsoft übertragen hat, die aus h. S. ein Risiko oder das Offenlegen vertrauenswürdiger Informationen darstellen. Insbesondere konnte keine Übertragung von Telemetriedaten an Microsoft beobachtet werden."

Für ihr Urteil genügte der DSK, dass eine bestimmte Verbindung „nicht im Klartext analysiert werden konnte" – mithin die Möglichkeit besteht, dass Microsoft entgegen der anderslautenden Zusicherungen darüber doch Telemetriedaten übermitteln *könnte*. Das Verdikt wirkt wie eine merkwürdige Gemengelage aus Skepsis, Vorurteilen und Unterstellungen – und wird viel Unsicherheit hervorrufen. Warum sich die Aufsichtsbehörden hier so in Stellung bringen, während zeitgleich Millionen Webseiten und Milliarden Apps offensichtlich rechtswidrig Nutzerdaten erheben und (nicht nur) in die USA übermitteln, dürfte auch Datenschützern schwer zu vermitteln sein.

Inhalt

secorvo
security consulting

Security News

Besenrein

Am 07.07.2020 veröffentlichte The Register einen exklusiven Artikel darüber, wie Cyberkriminelle mehr als 240 Subdomänen existierender Organisationen übernehmen konnten. Ursächlich dafür waren Subdomänen mit verwaisten DNS-Einträgen, die auf zwischenzeitlich aufgegebene Azure-Ressourcen zeigten. Die Angreifer erstellten Ressourcen mit denselben Namen neu und empfingen anschließend den gesamten Datenverkehr, der für die noch im DNS hinterlegte Subdomäne bestimmt war.

Offensichtlich ist das Problem so groß, dass Microsoft am 29.09.2020 in der Netzwerksicherheitsdokumentation für Azure einen Artikel zur Verhinderung von Subdomain-Übernahmen ergänzte.

Merke: Auch in der Cloud betriebene Assets sollten einem kontrollierten Lebenszyklus unterliegen – Stichwort „Cloud Asset Management" – und am Ende „besenrein" abgeschlossen werden. Außerdem sollte man nicht davon ausgehen, dass in der Cloud betriebene Ressourcen „auto-magisch" sämtliche Konfigurationen selbst vornehmen und „einfach funktionieren". Bester Beweis dafür sind die seit Jahren immer wieder entdeckten falsch konfigurierten und damit für die ganze Welt zugänglichen AWS S3 Buckets.

Cookie-Einsatz im Fokus

Der Landesbeauftragte für Datenschutz und Informationsfreiheit hat am 25.11.2020 seinen Bericht zur Prüfung des Einsatzes von Cookies und Drittdiensten auf niedersächsischen Webseiten veröffentlicht. Die geprüften Webseiten genügten – wenig überraschend – nicht den Anforderungen der DSGVO, der Gerichte und der Aufsichtsbehörden. Häufig kommen so genannte „Consent Tools" zum Einsatz, die die Lage eher verschlimmern als verbessern: Einwilligungen werden häufig nicht wirksam eingeholt, Widerrufsmöglichkeiten fehlen ganz und die zur Verfügung gestellten Informationen zum Tracking sind mangelhaft. Dabei blieb bei der Prüfung gänzlich unbeachtet, dass es neben Cookies auch andere Tracking-Technologien gibt, an die die gleichen Anforderungen zu stellen sind.

Das Risiko, wegen unzureichender „Consent Banner" mit einem Bußgeld belegt zu werden, steigt: Europaweit häufen sich die Berichte über entsprechende Verfahren der Aufsichtsbehörden. Die Handreichung der niedersächsischen Aufsichtsbehörde gibt verständliche Hinweise, was möglich und erlaubt ist.

Gefährliche Ignoranz

Am 06.12.2020 veröffentlichte der Sicherheitsforscher Oskars Vegeris Details zu einer am 31.08.2020 an Microsoft gemeldeten kritischen Schwachstelle in Microsoft Teams. Sie konnte zur Ausführung beliebigen Codes aus der Ferne genutzt werden – plattformübergreifend. Nötig war dafür allein eine bösartige Chat-Nachricht. Die Schwachstelle war „wurmbar", d. h. es konnte Schadcode geschrieben werden, der sich selbstständig weiter verbreitet. Sie wurde Ende Oktober 2020 geschlossen – still und heimlich, da es sich bei Teams um ein sich „selbst aktualisierendes Produkt" handelt, und ohne CVE-Eintrag. Belohnt wurde der Sicherheitsforscher nicht für seinen Fund, da der Desktop-Client nicht Teil des Bug-Bounty-Programms ist – die Schwachstelle also „out of scope" war.

Ein beliebtes, aber gefährliches Vorgehen, da es die Finder kritischer Schwachstellen künftig motivieren könnte, solche Funde direkt auf dem Schwarzmarkt zu verkaufen oder zu veröffentlichen. Das sollte Microsoft eigentlich wissen: 2018 hatte die Sicherheitsforscherin „SandboxEscaper" nach einer ähnlichen Erfahrung mit Microsoft mehrere Zero-Day-Schwachstellen samt Exploit-Code auf Twitter und GitHub veröffentlicht.

Neue Datenschutzklauseln

Die Europäische Kommission hat am 13.11.2020 einen Entwurf für neue Standardvertragsklauseln, die zugehörige Angemessenheitsentscheidung und Leitlinien zur Verwendung zur öffentlichen Konsultation vorgelegt. Die Neugestaltung war bereits durch sich verändernde Übermittlungskonstellationen, vor allem aber durch das Schrems-II Urteil erforderlich geworden.

Der vorgelegte Entwurf ersetzt und vereinheitlicht die bisherigen drei Varianten der Standardvertragsklauseln. Dafür werden innerhalb der Entwurfsklauseln vier Module gebildet: Modul 1 für die Übermittlung zwischen Verantwortlichen, Modul 2 für Auftragsverarbeiter, Modul 3 für Unterbeauftragungen durch Auftragsverarbeiter und Modul 4 für die Zusammenführung von personenbezogenen Daten, die der EU-Auftragsverarbeiter erhebt, mit Daten des Verantwortlichen aus einem Drittstaat. Die anwendbaren Regelungen ergeben sich aus der anfänglichen Festlegung der Konstellation. Die Umsetzungsfrist für den Übergang zu den neuen Klauseln soll ein Jahr ab Verabschiedung betragen.

Dem Schrems-II Urteil wird durch die verankerte Pflicht zur Prüfung der Umsetzbarkeit, entsprechende Meldepflichten und Kündigungsvorbehalte Rechnung getragen. Die Erneuerung der in die Jahre

gekommenen Standardvertragsklauseln war überfällig. Ansätze zur Lösung der Problematik von zu weit gehenden oder ungenügend kontrollierten staatlichen Zugriffen (Stichwort „US CLOUD Act“) enthalten die Klausel-Entwürfe jedoch nicht.

Spy in the Middle

Am 08.12.2020 veröffentlichte Cloudflare, wie der Konzern künftig durch Einsatz von „Oblivious DNS over HTTPS“ (ODoH), einem in Kooperation mit Apple und Fastly entwickelten Protokoll, die Anonymität von Anfragen mittels DNS over HTTPS (DoH) verbessern will. DoH ermöglicht die Namensauflösung über TLS-gesicherte HTTP-Verbindungen und war wegen der Nachvollziehbarkeit des Surfverhaltens durch Cloudflare in die Kritik geraten (SSN 09/2019). Bei ODoH ist die DNS-Anfrage verschlüsselt, sodass der Proxy-Anbieter den Inhalt nicht mitlesen kann. Weder der DNS-Anbieter noch der Betreiber des Proxy-Servers kann eine Anfrage einem Nutzer zuordnen – solange der Proxy-Betreiber nicht mit dem DNS-Anbieter kooperiert.

Dass DNS dringend Sicherheits- und Privatsphären schützende Funktionen wie Verschlüsselung benötigt, steht außer Frage. Mit welcher Technologie dies erfolgen wird, ist jedoch noch offen. TLS und HTTPS liegen zwar aus konzeptioneller Sicht auf dem falschen OSI-Layer, aber eine in der Praxis getestete und weit verbreitete Technologie ist erfahrungsgemäß sicherer als die Entwicklung eines neuen Protokolls. Auch ist die großflächige Änderung der bestehenden DNS-Infrastruktur z. B. in Form von Erweiterungen wie DNSSEC in der Praxis schwierig. Ähnlich der Entwicklung von Programmierbibliotheken ist es einfacher, bei den Nutzern eine neue „Bibliothek“ (ODoH) zu installieren, als eine bestehende Infrastruktur zu ändern.

Identifikation bei Auskunftsanfrage

Das Verwaltungsgericht Berlin entschied am 31.08.2020, dass bei einem Auskunftsersuchen eine „qualifizierte Form“ der Identifikation nur dann verlangt werden kann, wenn „begründete Zweifel“ an der Identität des Antragstellers bestehen. So sehen es auch § 59 BDSG und Art. 12 Abs. 6 DSGVO vor. Dem BayObLG genügt jedoch laut Beschluss vom 18.11.2020 bei einem schriftlichen Antrag auf Auskunft nicht, dass sich der Antragsteller mit vollständigem Namen und Geburtsdatum identifiziert. Dass auch die korrekte Adresse bekannt war, wie der Schriftwechsel mit den Gerichten zeigt, half auch nicht weiter. Vor Gericht und auf hoher See – ist man in Gottes Hand.

Windows 10 und die Daten

Am 26.11.2020 hat die Datenschutzkonferenz einen Beschluss zur Datenschutzkonformität der Telemetriefunktionen von Windows 10 Enterprise gefasst. Die Bewertung geht auf eigene Laboruntersuchungen einer DSK-Arbeitsgruppe und eine Analyse des BSI vom Januar 2020 zurück.

Die Übermittlung der Telemetrie-Daten an Microsoft kann auch personenbezogene Daten zum Nutzungsverhalten beinhalten, deren Übermittlung durch das verantwortliche Unternehmen v. a. gegenüber Arbeitnehmern einer Rechtsgrundlage und bei Übermittlung in Drittstaaten gesonderter Regelungen bedarf. Die Untersuchungen kommen zu dem Ergebnis, dass die geprüften Windows-Versionen die Deaktivierung der Telemetrieübermittlung grundsätzlich ermöglichen. Die DSK sieht die Microsoft-Kunden als Verantwortliche in der Nachweispflicht bzgl. der sicheren Unterbindung von Übermittlungen. Probleme bereitet hier die Ansteuerung eines Microsoft-Endpunktes in allen Einstellungsvarianten, der möglicherweise für eine dynamische Konfiguration der Telemetrieeinstellungen verwendet werden kann. Die diesbezüglichen Zusicherungen von Microsoft werden als nicht ausreichend angesehen. Für Windows Pro und Home besteht derzeit keine Deaktivierungsmöglichkeit.

Es drängt sich die Frage auf, wie Verantwortliche auch bei vergleichbaren Anwendungen regelmäßig eigenständig über die Zusicherungen der Anbieter hinaus nachweisen sollen, dass keine derartigen Übermittlungen an die Software-Anbieter stattfinden.

Vorsatz 2021: Keine unnötigen Risiken

Meldungen wie die vom 19.11.2020 über eine Sicherheitslücke im Server-Backend der Corona-Warn-App lassen sich unterschiedlich interpretieren: Laut Projekt belegt sie, dass „der Open-Source- sowie Community-Prozess einwandfrei funktioniert“; nach der Beschreibung der Entdeckung auf GitHub war es hingegen ein Zufallsfund. Sie fiel auf, als ein Scanner auf Basis des (in SSN 11/2020 beschriebenen) GitHub-integrierten Scanners trainiert wurde. Eines jedenfalls zeigt der Fall: Selbst kritisch in der Öffentlichkeit stehende Software kann Fehler enthalten. Daher empfehlen wir für 2021 einen grundlegenden Sicherheitsmechanismus: Unnötige Risiken vermeiden! Wer sein Auto öffnen lassen möchte, indem das Auto das Handy fragt, ob der Fahrzeughalter gerade vor ihm steht – bitte. Für sicherheitsbewusste Technik-Nutzer sollte aber eine Möglichkeit bestehen, einen solchen potenziell fehlerhaften Zugangsmechanismus zu deaktivieren.

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

Februar 2021	
01.-04.02.	28. DFN-Konferenz „Sicherheit in vernetzten Systemen“ (DFN-CERT, virtuell)
02.-03.02.	17. Deutscher IT-Sicherheitskongress (BSI, virtuell)
18.-19.02.	OWASP Global AppSec (OWASP, Dublin/IRL)
22.-26.02.	T.I.S.P. TeleTrusT Information Security Professional (Secorvo, Karlsruhe)
23.-25.02.	secIT 2021 (Heise Medien, Hannover)
März 2021	
03.-04.03.	Future Security 2021 (Fraunhofer VVS, Nürnberg)
29.03.-01.04.	DFRWS EU 2021 (DFRWS, virtuell)
April 2021	
19.-22.04.	PKI – Grundlagen, Vertiefung, Realisierung (Secorvo, Karlsruhe)
26.-29.04.	T.P.S.S.E. – TeleTrusT Professional for Secure Software Engineering (Secorvo, Karlsruhe)

Impressum

Secorvo Security News – ISSN 1613-4311

Redaktion: Dirk Fox (Editorial), André Domnick, Stefan Gora, Kai Jendrian, Michael Knopp, Sarah Niederer, Friederike Schellhas-Mende, Jochen Schlichting, Christian Titze

Herausgeber (V. i. S. d. P.): Dirk Fox,
Secorvo Security Consulting GmbH
Ettlinger Straße 12-14
76137 Karlsruhe
Tel. +49 721 255171-0
Fax +49 721 255171-100

Zusendung des Inhaltsverzeichnisses: security-news@secorvo.de
(Subject: „subscribe security news“)

Wir freuen uns über Ihr Feedback an redaktion-security-news@secorvo.de