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