Secorvo Security News

August 2022

Deep Fake

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

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

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

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

Security News

Video-Fake-Ident

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

Nach dem Untersuchungsbericht von Martin Tschirsich bedurfte es für die Angriffe keiner kostenintensiven Hard- oder Software. Es genügte, vor der Kamera ein manipuliertes Video abzuspielen, in dem das Passfoto auf dem Ausweis ersetzt worden war. Die Manipulati-

onen wurden von keiner der sieben getesteten Lösungen erkannt. Zwar nennt der Bericht keine Hersteller, es ist aber zu befürchten, dass die Angriffe bei den weitaus meisten Video-Ident-Lösungen funktionieren.

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

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

Pimp my Tesla

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

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

Kein Konzernprivileg

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

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

Ob ein Schadensersatz überhaupt eine abschreckende, d. h. sanktionierende Wirkung haben oder vielmehr

nur zum Schadensausgleich dienen darf, ist Gegenstand von Vorlagefragen des AG München vom 03.03.2022 an den EuGH.

Viele Daten sind besonders

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

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

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

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

Jagd auf Cookie-Banner

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

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

Webseitenbetreiber, die ihre Cookie-Banner auf Rechtskonformität prüfen möchten, finden u. a. beim

Landesbeauftragten für Datenschutz und Informationssicherheit Baden-Württemberg hilfreiche Hinweise und Beispiele.

Verhältnismäßig

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

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

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

Secorvo News

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

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

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

Hokus Pokus Fidibus

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

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

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

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

Veranstaltungshinweise

Auszug aus Veranstaltungsübersicht IT-Sicherheit und Datenschutz

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

Fundsache

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

Impressum

Secorvo Security News – ISSN 1613-4311

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

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

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

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