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.

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