Hilfloses Opfer für KI-Scams?

Wie gefährdet ist die öffentliche Verwaltung?

(BS/Prof. Dr. Robert Müller-Török/Prof. Dr. Alexander Prosser*) Durch die Presse gehen häufig Berichte über Enkeltricks, wo hilflose und verletzliche, zumeist ältere Personen von professionellen Betrügern um ihre Ersparnisse gebracht werden. Seltener gibt es Berichte über CEO-Frauds, wo sich Betrüger als Mitglieder der Unternehmensleitung ausgeben und so offenbar schlecht geschulte Mitarbeiter zu hohen Überweisungen verleiten. Hierbei trifft es mittlerweile auch Unternehmen wie die Hofpfisterei mit einem Schaden von 1,9 Millionen Euro oder die börsennotierte Leoni AG mit einem Schaden von rund 40 Millionen Euro.

Mittlerweile nutzen die Kriminellen auch Künstliche Intelligenz (KI), wie dieser Tage ein internationaler Konzern in Hongkong erfahren musste. Ein Mitarbeiter erhielt per E-Mail eine Einladung zu einer Videokonferenz, in der ihn 15 Kollegen und Vorgesetzte davon überzeugten, Überweisungen im Wert von 24 Mio. Euro auszuführen. Es handelte sich bei diesen Kollegen und Vorgesetzten allesamt um Deep Fakes, d.h. es waren durch KI erzeugte Avatare, die aussahen und sprachen wie die tatsächlichen Personen. Für den privaten Bereich sagte am 13. Juni 2023 *Jennifer DeStefano* vor dem US-Senat aus, dass sie einen Anruf ihrer „entführten" Tochter erhalten habe, der auf Deep Fake basierte – also frei erfunden war.

Das zugrunde liegende Problem ist an sich seit Langem bekanntes: Wie kann man in elektronischen Medien sicher sein, dass Daten (Mail, Telefonanruf, Videokonferenz, Film etc.) tatsächlich von dem vorgeblichen Absender stammen?

Die Antwort: die digitale Signatur

Ebenso einfach ist die Antwort, die auf einer über 30 Jahre alten Technologie basiert: die digitale Signatur, in Europa als elektronische Signatur bezeichnet und als fortgeschrittene bzw. qualifizierte elektronische Signatur seit 1999 in der Signaturrichtlinie bzw. seit 2014 in der eIDAS-VO kodifiziert. Das bekannteste technische Verfahren hierzu basiert auf RSA (Patent von 1983), einem asymmetrischen Verschlüsselungsverfahren.

Nur die digitale Signatur ermöglicht es, eine Datei so zu signieren, dass für den Empfänger nachprüfbar ist, ob es sich beim Absender/Ersteller der Datei tatsächlich um den handelt, für den er sich ausgibt. Ein digital signiertes Video ist authentisch – ein nicht signiertes Video nicht. Ebenso kann die digitale Signatur in Videokonferenzsysteme integriert werden, ganz analog zu PDF-Readern, aus denen heraus eine digitale Signatur geprüft werden kann. So ist es einfach umsetzbar, dass am Beginn einer Videokonferenz digital signierte Einladungen zum betreffenden Call in die Chatfunktion hochgeladen werden und die Signaturen von den anderen Teilnehmern gleich im Konferenzsystem geprüft werden können (analog zum Unterschriftenfenster im PDF-Reader). Damit hat man dann die Sicherheit, tatsächlich mit den angegebenen Personen zu kommunizieren.

Bislang allerdings wird die digitale Signatur in Deutschland weder von Privaten noch von Behörden ernsthaft genutzt. Sieht man von ELSTER ab, wo zumindest die fortgeschrittene Signatur verbreitet ist, fristet die digitale Signatur in Deutschland ein Mauerblümchendasein.

Die digitale Signatur ist deshalb nicht verbreitet, da Deutschland bei Einführung der eID/des nPA einen fatalen Doppelfehler beging: Zunächst war die darauf basierende Signatur prohibitiv teuer: Es handelte sich um eine kartenbasierte Lösung. Damit musste ein teurer Kartenleser gekauft werden; auch war auf dem ePerso kein Signaturzertifikat enthalten, dieses musste zusätzlich erworben werden – seit Sommer 2017 werden keine Signaturzertifikate mehr auf dem Markt angeboten. Zum anderen wurde die De-Mail staatlicherseits forciert, die faktisch einer „Briefmarkenpflicht für E-Mails" entsprach. Dass das scheiterte, war erwartbar. Heute gibt es keine staatlicherseits angebotene Gratis- oder auch nur kostengünstige Lösung, was die beiden Autoren – beide Österreicher und seit Langem im Besitz der österreichischen Handysignatur, seit 5. Dezember 2023 ID Austria – verwundert: Sie können damit gratis beliebig viele Dateien signieren, wie insgesamt über drei Millionen Nutzer von 9,1 Millionen Einwohnern.

Nur geringe Verbreitung der Signatur

Im öffentlichen Bereich ist die digitale Signatur ebenso wenig verbreitet: Behörden versenden E-Mails, denen es an einer automatischen Signatur durch den Mailserver mangelt, der sogenannten DKIM-Signatur, welche seit 2007 kodifiziert ist (RFC 4870) und sicherstellt, dass die Mail tatsächlich von einem bestimmten Server stammt, der damit indirekt auch die Senderauthentizität gewährleistet.

Anscheinend, und so belegen die den Autoren vorliegenden E-Mails von Bundesbehörden, scheint die digitale Signatur ausgehender E-Mails zumindest nicht der Standard zu sein. Auch die Zugangseröffnung für signierte Mails für Bürger nach § 3a VwVfG fehlt sogar beim Bundespräsidenten und auch beim Bundeskanzler, diese verweisen auf die gescheiterte De-Mail.

Während der Erstellung dieses Beitrages wurde überdies ein Problem mit der deutschen eID im Blog CtrlAlt publiziert und von der Tagespresse breit aufgegriffen. Demnach kann bei der Verwendung eines einfachen Kartenlesegeräts ohne eigene Intelligenz und ohne eigenes PIN-Pad (Cat-B) die PIN-Eingabe zur Freigabe der eID abgefangen und manipulativ eingesetzt werden. CtrlAlt gelang es auf diese Weise, für einen Dritten ein Bankkonto zu eröffnen. Das BSI bestätigte die Schwachstelle, schob aber die Verantwortung auf den Nutzer, da dieser für seine dezentrale Arbeitsumgebung selbst verantwortlich sei. Vorbehaltlich einer genaueren Prüfung des Sachverhalts kann festgestellt werden, dass es sehr wohl in der Verantwortung des BSI lag, Cat-B-Kartenleser überhaupt für die eID zugelassen zu haben.

Fazit

Da die einzige handhabbare Möglichkeit der Authentisierung digitaler Datenströme kaum verbreitet und darüber hinaus imagemäßig beschädigt ist, steht Deutschland KI-Scams, wie im Titel angeführt, buchstäblich hilflos gegenüber.

**Prof. Dr. Robert Müller-Török lehrt an der Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg, Prof. Dr. Alexander Prosser an der Wirtschaftsuniversität Wien.*