

Deepfakes: die Täuschung der digitalen Realität

Wie Kriminelle Deepfakes nutzen und wie Sie sich davor schützen können

In einer Welt, in der die Grenzen zwischen Realität und digitaler Manipulation verschwimmen, haben Deepfakes in den letzten Jahren zunehmend an Bedeutung gewonnen. Aber was sind Deepfakes eigentlich? Wie sie entstehen, wie Sie sich vor dieser modernen Form der Täuschung schützen und was Betriebsräte in dem Zusammenhang tun sollten.



Redaktion

Stand: 6.11.2023

Lesezeit: 04:15 min



Was sind Deepfakes?

Der Begriff Deepfake ist längst ein fester Bestandteil der digitalen Welt. Wer erinnert sich noch an das Bild vom Papst als Rapper oder Barack Obama, der Donald Trump in einem Video als völligen Idioten darstellt oder aber an die Weihnachtsbotschaft der britischen Queen Mum, in der sie den übermäßigen Verbrauch von Toilettenpapier kritisiert? Diese scheinbar humorvollen Medieninhalte haben eines gemeinsam – sie sind Produkte eines Deepfakes. **Der Begriff „Deepfake“ setzt sich übrigens aus „Deep Learning“ (einer Methode des maschinellen Lernens) und „Fake“ (Schwindel, Fälschung) zusammen.** In der Regel handelt es sich um Fotos, Videos oder Audios, die mithilfe künstlicher neuronaler Netze so bearbeitet oder gar komplett neu generiert werden, dass sie nur schwer als Fälschungen zu erkennen sind.

Das Besorgniserregende: Die Erstellung von Deepfakes wird immer einfacher.

Wie entstehen Deepfakes?

In unserer modernen Welt sind Deepfakes (leider) längst keine Seltenheit mehr. Sie verbreiten sich im World Wide Web wie ein Lauffeuer, insbesondere in den sozialen Netzwerken. Das Besorgniserregende: Die Erstellung von Deepfakes wird immer einfacher. Jeder, der Zugang zu einem leistungsstarken Computer mit einer hochwertigen Grafikkarte hat, kann Deepfakes erstellen. Die erforderliche Software steht online frei zur Verfügung.

Es ist kein Zufall, dass gerade die kriminelle Szene diese Technologie vermehrt für ihre Zwecke nutzt. Um einen Deepfake zu erstellen, benötigt das trainierte Computermodell Daten der Zielperson, beispielsweise in Form von mehreren Bildern, um deren Gesichtszüge, Mimik und Bewegungen zu analysieren und zu imitieren – ein Video einer Person stellt der Software ungefähr 60 Bilder pro Sekunde zur Verfügung. Anschließend kann diese Software die Zielperson mithilfe Künstlicher Intelligenz (KI) nachbilden und sie dazu bringen, Sätze zu äußern und Handlungen durchzuführen, die niemals wirklich stattgefunden haben. Auf der anderen Seite können Gesichter in bereits existierenden Videos durch das Gesicht einer Zielperson ersetzt werden.

Wie gehen Kriminelle vor?

Cyberkriminelle nutzen vielfältige Methoden, um ihre Opfer zu täuschen und finanzielle Schäden anzurichten. Eine alarmierende Taktik besteht darin, über Video-Chats insbesondere ältere Menschen mit dem altbekannten Enkeltrick zu überlisten, wodurch diese zu Überweisungen von beträchtlichen Geldsummen bewegt werden. Doch nicht nur Privatpersonen sind betroffen, auch Unternehmen sehen sich vermehrt mit dieser Betrugsmasche konfrontiert.

Der Einsatz von Deepfakes verleiht Angriffen wie Identitätsdiebstahl und der Umgehung der Identitätsüberprüfung eine beunruhigende Dimension.

Diese Cyberkriminellen setzen zudem auf raffinierte E-Mail-Manipulation. In täuschend echten Nachrichten, die angeblich von Führungskräften, Mitarbeitern, Geschäftspartnern, Kunden oder Dienstleistern stammen, fordern sie den Empfänger auf, bestimmte Aktionen durchzuführen. Da die E-Mails so authentisch erscheinen, glauben die Opfer, dass sie tatsächlich vom angegebenen Absender stammen. In der Folge werden vertrauliche oder sensible Daten preisgegeben, oder es erfolgen geschäftliche Transaktionen, wie etwa Geldüberweisungen auf angegebene Konten. Die zunehmenden Deepfake-Angriffe verändern die Bedrohungslage erheblich und betreffen nicht nur Unternehmen und Finanzinstitute, sondern auch

Prominente, Politiker und sogar den Durchschnittsbürger. Der Einsatz von Deepfakes verleiht Angriffen wie Identitätsdiebstahl (u. a. „Business E-Mail Compromise“) und der Umgehung der Identitätsüberprüfung eine beunruhigende Dimension. Unternehmen und Privatpersonen sind daher gleichermaßen gefordert, ihre Sicherheitsvorkehrungen zu verschärfen und aufmerksam gegenüber dieser wachsenden Bedrohung zu sein.



Wie erkennen Sie ein Deepfake?

Die Identifizierung von Deepfakes erfordert ein scharfes Auge und Aufmerksamkeit für Details. Hier sind einige Anzeichen, auf die Sie achten können:

1. **Gesichtsausdruck und Schärfe:** Prüfen Sie, ob der Gesichtsausdruck unnatürlich wirkt oder das Gesicht leicht verschwommen ist. Merkwürdige Mimik oder ein leerer Blick können Hinweise darauf sein, dass es sich um eine Fälschung handelt.
2. **Übergang zwischen Kopf und Hals:** Unschärfe oder ungewöhnliche Übergänge zwischen Kopf und Hals können auf ein weniger professionell erstelltes Deepfake hinweisen.
3. **Blinzeln:** Achten Sie darauf, ob die Person in einem Video vielleicht nie blinzelt. Dies kann ein Hinweis auf eine Manipulation sein.
4. **Bildqualität:** Untersuchen Sie die Bildqualität zwischen der Person und ihrem Gesicht im Vergleich zum Rest des Körpers oder dem Hintergrund. Auffällige Unterschiede deuten auf eine mögliche Manipulation hin.
5. **Live-Deepfakes und die Nase:** Bei Live-Deepfakes kann es hilfreich sein, darauf zu achten, ob die Person regelmäßig blinzelt oder nicht. Ein weiterer Tipp besteht darin, die Person auf die Nase tippen zu lassen, da KI-Systeme immer noch Schwierigkeiten haben, dieses Detail realistisch zu simulieren.

Achtung: Die Deepfake-Technologie entwickelt sich ständig weiter und nicht alle Fälschungen sind leicht zu erkennen. Ein gesundes Maß an Skepsis und das Hinterfragen von Inhalten im Internet sind immens wichtig, um sich vor möglichen Täuschungen zu schützen.

Rechtliche Einordnung von Deepfakes

Grundsätzlich können Sanktionen drohen, wenn Personen mithilfe von Deepfakes Videos erstellen. So besteht zum Beispiel die Möglichkeit, dass ein Verstoß gegen das Recht am eigenen Bild, das Allgemeine Persönlichkeitsrecht und/oder Urheberrecht vorliegt. Die Europäische Union arbeitet derzeit an einem KI-Gesetz. Diese neuen Vorschriften legen Verpflichtungen für Anbieter und Nutzer fest, die sich nach dem Risiko richten, das von dem KI-System ausgeht. Ziel ist es, bis Ende des Jahres eine Einigung zu erzielen.

Betrifft Sie dieses Thema als Betriebsrat?

Es ist sicher ratsam, sich als Betriebsrat nicht nur beruflich, sondern auch in persönlicher Hinsicht mit diesem Thema auseinanderzusetzen. Deepfakes reichen von kriminellen Aktivitäten und der Verbreitung von Falschinformationen im Web bis hin zu Cyber-Mobbing. Besonders, wenn Sie Kinder haben, sollten Sie sich bewusst machen, welche Auswirkungen Deepfakes haben können und Ihren Nachwuchs darüber aufklären.

Die Zusammenarbeit mit dem Arbeitgeber, insbesondere in Bezug auf IT-Sicherheitsschulungen für die Belegschaft, kann für alle Beteiligten vorteilhaft sein.

Wichtig ist, nicht alles ungeprüft zu akzeptieren, was auf Plattformen wie Facebook, Twitter und anderen sozialen Medien veröffentlicht wird. Ein kritischer Blick schadet nie – sowohl in beruflichen als auch in persönlichen Angelegenheiten. Die Zusammenarbeit mit dem Arbeitgeber, insbesondere in Bezug auf IT-Sicherheitsschulungen für die Belegschaft, kann für alle Beteiligten vorteilhaft sein. (sw)

Kontakt zur Redaktion

Haben Sie Fragen oder Anregungen? Wenden Sie sich gerne direkt an unsere Redaktion. Wir freuen uns über konstruktives Feedback!

redaktion-dbr@ifb.de