

Mobbing, Rufschädigung, Manipulation: Auswirkungen von Deepfakes

Wie falsche Informationen Stimmung machen können

In einer zunehmend digitalisierten Welt sind Deepfakes zu einer neuen Bedrohung geworden. Manipulierte Informationen können nicht nur psychologische Schäden verursachen, sondern auch zu finanziellen Verlusten führen. Was tun? Auch als Betriebsrat ist es wichtig, Desinformationen schnell zu erkennen.



Redaktion

Stand: 19.2.2024

Lesezeit: 02:30 min



© Adobe | our_future / KI

Sie werden immer besser und professioneller. Die Rede ist von Deepfakes (visuelle oder textliche Täuschung), die inzwischen das Internet fluten. Diese manipulierten Inhalte dienen nicht nur betrügerischen Absichten, sondern können auch gezielt eingesetzt werden, um Menschen zu beeinflussen. Im Einzelfall kann das auch für Unternehmen zu einer ernsthaften Bedrohung werden. Laut Digitalverband führen Deepfakes bei vielen Menschen zu Verunsicherung. Denn der Laie kann die Realität oft nicht von dem "Fake" unterscheiden. 8 von 10 Deutschen (81 Prozent) sagen, sie würden ein Deepfake nicht erkennen. 44 Prozent geben an, schon einmal auf ein Deepfake reingefallen zu sein. 70 Prozent sind der Meinung, Fotos und Videos könne man heute nicht mehr vertrauen und 63 Prozent sagen sogar, Deepfakes machen ihnen Angst. Und schlimmer noch: 60 Prozent sehen in Deepfakes sogar eine Gefahr für unsere Demokratie. Diese Verunsicherung ist auch in unserer Arbeitswelt allgegenwärtig!

Es ist so einfach! Mit einem Dollar pro Monat lädt man sich eine Software für Deepfakes auf den Rechner.

Prominenten Personen einfach Worte in den Mund legen

Es ist so einfach! Mit einem Dollar pro Monat lädt man sich eine Software für Deepfakes auf den Rechner. Benötigtes Videomaterial liefert das Fernsehen genug. Besonders beliebt und einfach zu faken: Nachrichtensprecher! Keine Hintergrundmusik und kein Rauschen! Perfekt für die Erstellung eines gefälschten Videos. Hier ein Beispiel: Im September 2023 preist der ZDF-Moderator Christian Sievers in einem Internet-Video auf der Plattform X (ehem. Twitter) eine Tradingsoftware an – doch das Video ist gefälscht. Der vermeintliche Sievers erklärt nun, wie eine Software es jedem ermöglicht, "mit minimalen Investitionen große Geldsummen zu verdienen" – und zwar ab 15.000 Euro pro Monat. Und bittet natürlich um Überweisung! Die Menschen fallen darauf rein. Schließlich gilt er als öffentliche Person als besonders vertrauenswürdig. Während dieser Aktion hat der reale Christian Sievers keine Ahnung von seinem gefakten Klon.

Stellen Sie sich nun vor: Als prominente Person könnte auch der Inhaber oder Vorstand Ihres Unternehmens oder Sie als Betriebsratsvorsitzende betroffen sein. Der Schaden wäre groß: Finanziell und imageschädigend für das Unternehmen und auch persönlich. Selbst wenn danach alles in der Presse revidiert würde – es bleibt immer etwas hängen.

Wussten Sie, dass schon mit einfachen Apps ein Gesicht in einen Porno montiert werden kann?

Deepfake: Pornodarsteller

Wussten Sie, dass schon mit einfachen Apps ein Gesicht in einen Porno montiert werden kann? Gratis-Apps wie FaceMagic, Reface und FacePlay wurden millionenfach in den App-Stores heruntergeladen und die Betreiber setzen sich leider nur bedingt dafür ein, dass Ihre Anwendungen keine Persönlichkeitsrechte verletzen. Ein aktuelles Beispiel sind generierte Nacktbilder von dem beliebten Popstars Taylor Swift. Diese haben bei Fans und sogar in der US-Politik Empörung ausgelöst. Dreist mit Hilfe von KI gefälscht! Eines der Bilder wurde im Onlinedienst X 47 Millionen Mal aufgerufen, bevor es nach 17 Stunden wieder entfernt wurde. Doch wie lebt die betroffene Person mit dieser Diskriminierung? Taylor Swift ist zwar prominent, aber kein Einzelfall! In einer Studie der Cybersicherheitsfirma Deeptrace konnten die Forscher schon im Jahr 2019 zeigen, dass über 95 Prozent der Deepfakes, die im Internet zu finden sind, pornografischen Inhalt haben. Eine andere Studie zur Bekämpfung von Deepfakes des Wissenschaftlichen Dienstes des Europäischen Parlaments aus dem Jahr 2021 kam zu dem Urteil: „Frauen in einen virtuellen sexuellen Kontext zu zwingen, reduziert sie zu wehrlosen Objekten. Daher können Deepfake-Pornografie und andere nicht einvernehmliche sexuelle Inhalte als eine neue Form der sexuellen Gewalt verstanden werden“, heißt es darin. Passiert das im betrieblichen Kontext, sind Sie als Betriebsrat in der Pflicht (AGG).

Die Gefahr von Manipulation und Deepfakes existiert täglich – auch für Unternehmen.

Achtung: Die Chef-Masche droht!

Machen Sie es sich bewusst: Die Gefahr von Manipulation und Deepfakes existiert täglich – auch für Unternehmen. So haben Betrüger in Hongkong 23 Millionen Euro mithilfe einer vorgetäuschten Videokonferenz erbeutet. Sie umgingen die Schwächen der Technik offenbar sehr geschickt – mit der „Chef-Masche“. Dabei gaben sich Kriminelle als hochrangige Manager aus, um hohe Geldtransfers zu veranlassen. Der gesamte Finanzvorstand wurde in dieser digitalen Konferenz gefakt. Welcher Mitarbeiter ist davor gewappnet, dass er mit Sicherheit richtig reagiert? Unternehmen müssen mehr denn je dafür sorgen, dass Mitarbeiter gut geschult und wachsam sind.

Deepfakes haben das Potenzial, erhebliche Schäden anzurichten.

Was tun gegen Deepfakes?

Deepfakes haben das Potenzial, erhebliche Schäden anzurichten. Opfer können unter schwerwiegenden psychischen Problemen leiden.

Auch finanzielle Schäden für Einzelpersonen, Unternehmen und Organisationen können erheblich sein. In Zeiten rascher Veränderungen ist es wichtiger denn je, gut geschult zu bleiben. Jedes Unternehmen sollte regelmäßig Sicherheitstrainings für seine Mitarbeiter anbieten.

Außerdem bieten zahlreiche Institutionen Informationsplattformen an, die dazu dienen, über aktuelle Entwicklungen aufzuklären. Ein solches Beispiel ist das [Fraunhofer-Institut für Angewandte Integrierte Sicherheit](#), dessen Forscher sich damit beschäftigen, KI-generierte Fakes mithilfe trainierter Systeme zu analysieren. Durch praktische Beispiele können Verbraucher mehr über Deepfakes erfahren. Auf Plattformen wie [Make.org](#) haben Bürger, Vereine, Verbände und Unternehmen die Möglichkeit, konkrete Vorschläge zur Veränderung einzubringen, darunter auch ein Forum, das sich speziell mit dem Thema Fakes befasst. Ebenso informiert das [Bundesamt für Sicherheit in der Informationstechnik](#) auf seinen Websites ausführlich über Deepfakes.

Ein verdächtiges Deepfake können Sie auf folgender Website prüfen:

[DeepFake-o-meter](#)

Die Forscher der University at Buffalo haben eine Software namens DeepFake-o-meter entwickelt, die Videodateien analysiert und nach Merkmalen von Deepfake-Videos sucht.

Fazit: Der Vertrauensverlust in unsere Medien ist akut. Eine Umfrage von Statista zeigt, dass die überwiegende Mehrheit der Befragten (84 Prozent) sich eine Kennzeichnungspflicht für Deepfakes wünscht, um sie besser erkennen zu können. Mehr als die Hälfte (60 Prozent) befürwortet sogar ein vollständiges Verbot von Deepfakes. In diesem Zusammenhang ist es entscheidend, genau hinzusehen und wichtige Botschaften kritisch zu hinterfragen.

Aber nicht alle Aspekte von Deepfakes sind negativ zu sehen: Tatsächlich erkennen über die Hälfte der Befragten auch positive Anwendungsmöglichkeiten. 55 Prozent sind der Meinung, dass Deepfakes sinnvoll im Bereich Kino oder Kunst eingesetzt werden könnten. Es bleibt zu hoffen, dass diese positiven Anwendungen in Zukunft überwiegen werden! (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