Barrierefreie Version

Impuls zur Cybersicherheit: Wie Cyberkriminelle unsere Sinne herausfordern

Deepfakes zeigen täuschend echte, aber manipulierte Bilder oder Videos und werden mit Hilfe von KI-Tools erzeugt. Diese Fälschungen zeigen Personen bei Handlungen, die so niemals stattgefunden haben. Realität und Fiktion lassen sich nur schwer voneinander unterscheiden. Die Täuschungsmethode wird häufig für die Verbreitung politischer Desinformation (Fake News) und beim Betrug mit Social Engineering-Taktiken eingesetzt.

Voice Cloning ist eine besondere Variante von Deepfakes. Bereits kurze Audiosequenzen reichen aus, um eine Stimme mit Hilfe von KI-Tools zu imitieren. Daher suchen Kriminelle in sozialen Netzwerken zielgerichtet nach Audioclips, um diese für Betrugsmaschen wie den Enkeltrick missbrauchen zu können. Auch die Stimme der vermeintlichen Führungskraft, die telefonisch einen Geldtransfer anweist, kann künstlich erzeugt sein.

Hinterfragen Sie Informationen stets kritisch, überprüfen Sie deren Quellen und verifizieren Sie die Echtheit von Anfragen!

Hausinterne Zusatzinformationen: