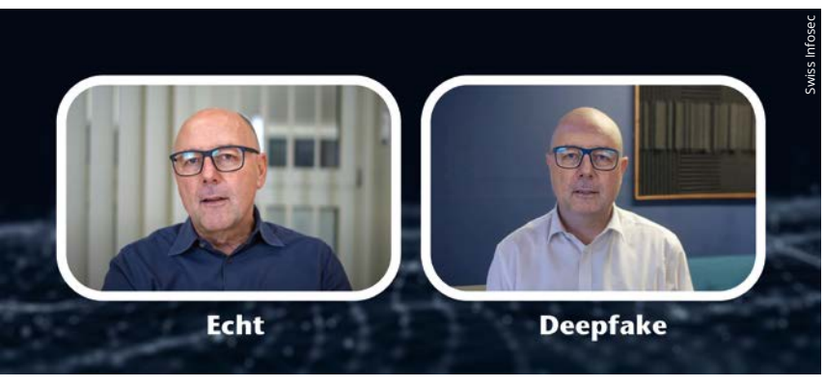
Phishing-Simulationen per Deepfakes

Als erstes Unternehmen in der Schweiz bietet Swiss Infosec eine Phishing-Simulation mit Deepfakes an, um Firmen für diese Form des Cyberangriffs zu sensibilisieren. Den Grundstein für die neue Dienstleistung legte ein kreativer Mediamatik-Lernender im Rahmen seiner Individuellen Projektarbeit.



Deepfakes halten Einzug ins Social Engineering – Ernst Martin Erni, CEO easylearn schweiz ag, ist eine der Testpersonen im Experiment «Phishing-Simulation per Deepfakes». Hier der Vergleich Echt – Deepfake.

Im Bereich Sicherheit bedeutet Social Engineering das Planen und Durchführen von Angriffen auf Informationen und Systeme unter Ausnutzung der «Schwachstelle Mensch». Das Ziel von Social Engineering ist, Mitarbeiter dazu zu bringen, Sicherheitsfehler zu begehen oder sensible Informationen offenzulegen. Sogenannte Phishing-Angriffe, meist via E-Mail und Telefon, sind die wohl bekannteste Form des Social Engineerings und gehören zu den grössten Bedrohungen für Unternehmen.

Deepfakes nutzen unter anderem digitale Fälschungen von Gesichtern, die mit künstlicher Intelligenz (KI) erstellt werden. Sie sind mittlerweile so realistisch, dass sie von der echten Person kaum zu unterscheiden sind. Angreifer bedienen sich immer öfter dieser Methode, um an vertrauliche Informationen zu gelangen oder gewünschte Aktionen zu provozieren. Der per digitale Plattform (Teams, Zoom etc.) zugeschaltete Geschäftsführer, der Überweisungen anordnet, kann, muss also nicht, der echte CEO sein (CEO-Fraud).

Phishing-Simulation per Deepfakes

Mit der neuen Dienstleistung «Phishing-Simulation per Deepfakes» des Unternehmens mit Sitz in Sursee (LU) wird untersucht, ob Angriffe per Deepfakes im Unternehmen erfolgreich wären. «Wir erstellen für die Videoanrufe ein Deepfake einer bekannten Person des Unternehmens, z. B. des CEO oder der Finanzchefin, her und bestimmen gemeinsam mit dem Unternehmen den Ablauf der Simulation», erklärt Ken Vogel, Head of Management Services bei Swiss Infosec. Die Resultate dieser Simulation dienen dann als Grundlage, um die Mitarbeiterinnen und Mitarbeiter für Phishing-Angriffe zu sensibilisieren.

Was erstaunt und die Anwendung dieser Angriffsmethode noch wahrscheinlicher macht: Der Aufwand für einen Deepfake-Angriff ist nur unwesentlich grösser als für einen Phishing-Angriff per E-Mail.

Wenn der Lernende zum Spezialisten wird

Im Rahmen seiner Ausbildung zum Mediamatiker wählte Kai Yu für seine Individuelle Projektarbeit (IPA) das Thema «Deepfakes». Yu konnte für sein Projekt zwei Unternehmen gewinnen, die an einer Phishing-Simulation mit Deepfakes teilgenommen haben und vom Erfolg dieser Methode überrascht waren. Die gewonnenen Erkenntnisse aus diesen und weiteren Phishing-Simulationen mit Deepfakes fliessen nun in die Dienstleistung «Phishing-Simulation per Deepfakes» der Swiss Infosec AG ein. Dies zeigt eindrücklich, dass hauseigene Potenziale bei Swiss Infosec erkannt und gezielt gefördert werden.

Awareness – wichtiger denn je

«Das Bewusstsein für Sicherheit ist dank Awareness zweifellos grösser geworden», ist Ken Vogel überzeugt und fügt an: «Der Begriff Phishing ist in der Öffentlichkeit und in Unternehmen angekommen. E-Mail-Absender und Links werden vermehrt kritisch hinterfragt.» Dennoch sei es unumgänglich, Mitarbeitende regelmässig für Sicherheit zu sensibilisieren. Erst recht, wenn neue Technologien und Angriffsmethoden – wie eben Deepfakes – zum Einsatz kommen. ●

► www.infosec.ch