INTERVIEW

Mirko Ross, CEO der Asvin GmbH in Stuttgart.

»Die Cybermafia ist technisch immer einen Schritt voraus.«

Wer es mit den Online-Kriminellen aufnehmen will, muss ihre Methoden kennen, so Mirko Ross, Gründer der Stuttgarter IT-Sicherheitsfirma Asvin.

Herr Ross, künstliche Intelligenz schafft in vielen Branchen neue Möglichkeiten. Gilt das auch für Kriminelle?
Oh ja. Generative KI hat zum Beispiel das Phishing auf ein neues Niveau gehoben. Früher konnte man gefälschte E-Mails meist an Tippfehlern oder holprigem Stil erkennen. Heute sind sie nahezu perfekt formuliert und kaum mehr von echten Nachrichten zu unterscheiden.

Und woher stammen die täuschend echten Absenderadressen? Meist aus offenen Quellen. Kriminelle sammeln Daten in sozialen Netzwerken oder kaufen sie im Darknet. So tauchen plötzlich Mails von Kollegen oder Geschäftspartnern auf – mit echten Adressen, aber betrügerischem Inhalt.

Wie kann man sich gegen diese Professionalität wehren?
Vor allem mit wacher Aufmerksamkeit. Jeder sollte Betreff und Absender prüfen – nicht nur auf Fehler, sondern auf Plausibilität. Beispiel: Eine Mail fordert die Unterzeichnung eines Vertrags über Docusign. Da muss man sich fragen: Gibt es diesen Vorgang überhaupt? Ist er abschlussreif? Und im Zweifel: anrufen und nachfragen.

Das klingt nach gesunder Skepsis. Reicht das aber, wenn die Angriffe immer raffinierter werden?
Es wird zweifellos schwieriger. Mit KI lassen sich Stimmen täuschend echt imitieren, sogar mit Emotion. Wer eine Sprachnachricht vom Chef erhält, die zur Überweisung auffordert, sollte besser nicht sofort handeln, sondern ersteinmal gegenprüfen.

Also nicht einmal ein Videocall ist sicher?
Leider nein. Vor Kurzem haben sich Täter in die Videokonferenz eines internationalen Unternehmens eingeschleust. Sie spielten KI-generierte Sequenzen des Vorstandschefs ein – perfekt getimt, so dass die Mitarbeiter glaubten, ihr Chef spreche live. Das Ziel war es, Überweisungen zu Gunsten der Cyberkriminellen auszulösen.

Das klingt ja fast wie Science-Fiction.
Ist aber Realität. Solche Deepfake-Angriffe werden häufiger. Und sie zeigen: Jeder, vom Praktikanten bis zum Vorstand, muss sich der Gefahr bewusst sein.

Welche Grundregeln empfehlen Sie?
Erstens: Gesundes Misstrauen ist keine Paranoia, sondern eine notwendige Vorsichtsmaßnahme. Zweitens: Es muss Klarheit über Abläufe und Zuständigkeiten herrschen: Rückrufnummern, Vier-Augen-Prinzip, Freigabe in zwei Schritten müssen Standard sein. Drittens: Schulungen. Je besser Mitarbeitende die Tricks kennen, desto weniger anfällig sind sie.

Und die Täter – stoßen sie irgendwann an Grenzen?
Technisch kaum. Was sie bremst, ist Aufwand. Je schwieriger ein Angriff durchzuführen ist, desto weniger wahrscheinlich wird er. Andererseits sind Kriminelle durchaus bereit zu investieren, wenn Sie einen hohen Gewinn erwarten, und das macht es für einzelne Unternehmen gefährlich. Deshalb gilt: Wer die Methoden kennt, kann gegenhalten. Ignoranz aber ist die größte Schwachstelle.

Das Interview führte **WALTER BECK**
Redaktion Magazin Wirtschaft, walter.beck@stuttgart.ihk.de

! VERANSTALTUNGSTIPP

Zum 7. Cybersicherheitsforum Baden-Württemberg am Donnerstag, **27. November**, werden viele Vertreter aus Unternehmen und Institutionen erwartet. Vorträge halten Prof. Jan Hesthaven, Präsident des KIT, Prof. Dr. Christian Dörr vom Hasso-Plattner-Institut, Brigadegeneral Dr. Volker Pötzsch (Bundesamt für Verteidigung) und Nicole Matthöfer, Präsidentin Cybersicherheitsagentur Baden-Württemberg.

Info und Anmeldung:
https://cybersicherheitsforum-bw.de