20.07.2023

KI-basierte Cyberattacken und Banken

Finanzinstitute geraten häufig ins Visier von Betrügern. Auch für Cyberkriminelle ist künstliche Intelligenz (KI) äusserst interessant. Durch die Nutzung von KI werden die Angriffe zunehmend ausgefeilter.

«Der Hype um Chat-GPT macht Cyberkriminelle kreativ», stellt die US-Cybersicherheitsfirma Palo Alto Networks fest. Das Bedrohungsforschungsteam der Firma hat zahlreiche Betrugsversuche aufgedeckt. Mit gefälschten Websites oder indem sich Kriminelle dank KI als Chefs ausgeben wird versucht, Mitarbeitende zu dringenden Zahlungen zubewegen. «Chat-GPT-Betrügereien nehmen zu», so das Fazit der Fachleute.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sorgt sich, dass KI künftig bei Täuschungsversuchen genutzt wird, bei denen „gefälschte Stimmen oder Videos eingesetzt werden“. Kriminelle können beispielsweise Stimmen fälschen und manipulierte Sprachnachrichten von einer vermeintlich bekannten Telefonnummer auf der Mailbox von Bankmitarbeitern oder Kunden hinterlassen. Auch Videoaufnahmen lassen sich fälschen. Live-Gespräche per Audio oder Video zu imitieren, schaffe KI aktuell zwar noch nicht, sagt Nviso-Hacker Leidecker. „Das könnte sich in Zukunft aber ändern, da sich die Technik schnell weiterentwickeln wird.“

Firmen, die selbst KI-Systeme nutzen, sind mit neuen Verwundbarkeiten konfrontiert. Der Rückversicherer Swiss Re warnt in seinem Sonar-Bericht 2023 unter dem Kapitel «KI wird gehackt – systemische Anfälligkeiten einer expandierenden Technologie» davor. Professionelle Hacker seien nicht nur in der Lage, Modelle so zu manipulieren, dass Fehler und Datenlecks entstehen. Sie könnten auch Daten manipulieren, sodass z.B. Prämienberechnungen verfälscht werden.

Schützen Sie sich, indem Sie...

- möglichst wenig persönliche Informationen über sich preisgeben. Insbesondere auf Sozialen Netzwerken sollten Sie mit Informationen sehr sparsam umgehen.
- bei Anfragen per E-Mail oder Telefon misstrauisch sind. Auch E-Mails von bekannten Absendern und Anrufe von bekannten Telefonnummern können gefälscht sein!
- Anhänge von E-Mails und Kurznachrichtendiensten mit grosser Vorsicht behandeln.
- sich bei Unsicherheiten oder Unklarheiten an das Finanzinstitut wenden.