20.07.2023

AI-based cyber attacks and banks

Financial institutions are frequently the target of fraudsters. Artificial intelligence (AI) is a very interesting field for cyber-criminals, too, enabling them to design their attacks in an increasingly sophisticated manner.

“All the hype about chat GPTs sees cyber-criminals becoming quite creative”, the US cyber security company Palo Alto networks found. The organisation’s threat research team has uncovered numerous fraud attempts. Using fake websites or by criminals exploiting AI to pretend they are your boss, they are trying to persuade employees to perform urgent payments. “Chat GPT frauds are on the increase”, these experts conclude.

The Bundesamt für Sicherheit in der Informationstechnik (BSI) is worried that AI will be used for future deception attempts, using “faked voices or videos”. Criminals can for instance fake voices and leave manipulated voice messages from an apparently well-known telephone number in a bank employee’s or bank customer’s mailbox. Video recordings can be faked, too. The only thing AI doesn’t manage so far is to imitate live video or audio conversations, Nviso hacker Leidecker says. “Still, that could change in the future, since technology is developing fast”.

Companies using AI see themselves confronted with new vulnerabilities. In a chapter headed “KI wird gehackt – systemische Anfälligkeiten einer expandierenden Technologie” (KI is being hacked – systemic vulnerabilities of an expanding technology), the Swiss Re reinsurance company warns in its Sonar report for 2023 of just this. Not only are professional hackers able to manipulate models to create errors and data breaches; they can also manipulate data, so that premium calculations for instance can be distorted.

Protect yourself by...

- disclosing as little information about yourself as possible. It is on social networks in particular that you should divulge information very sparingly.
- being wary when receiving requests by e-mail or telephone. Even e-mails from known senders and telephone calls received from familiar telephone numbers can be fake!
- treating e-mail and text message attachments with great caution.
- contacting your financial institution in case of any uncertainties or ambiguities.