Presseinformation

Finanzsektor wappnet sich gegen Cybercrime-Industrie

Phishing und Social Engineering sind die größten Cyberbedrohungen

Hamburg, 01. Oktober 2024 – **Finanzdienstleister in Deutschland sind alarmiert: 74 Prozent der Banken und Versicherer stellen sich darauf ein, dass Cyberkriminelle verstärkt Künstliche Intelligenz einsetzen, um Identitäten von Kunden oder Mitarbeitenden zu stehlen (45 Prozent) oder zu simulieren (29 Prozent). Die Folge: Investitionen in strategische Anpassungen und mehr Technologieunterstützung. Das ergibt die Studie „Cybersecurity im Zeitalter von KI" von Sopra Steria.**

Wirtschaft und öffentliche Verwaltung erleben eine neue Dimension bei Cyberangriffen. Finanzdienstleister sind wie ihre Kunden vorrangige Ziele von Hackern, Erpressern, Betrügern und Datenspionen. „Angriffe lassen sich mittlerweile in industriellem Maßstab planen und umsetzen. Das geschieht beispielsweise, indem eine KI-Software Informationen automatisiert aus dem Internet und sozialen Netzwerken zusammensucht, auswertet und Phishing-E-Mails oder Websites erstellt. Das erleichtert die Vervielfältigung und die Personalisierung der Angriffe enorm", sagt Hermann Hienz, Leiter Cybersecurity im Geschäftsbereich Banking bei Sopra Steria.

Darüber hinaus können Tools ähnlich wie ChatGPT helfen, sogenannte Phishing-Kits für andere Cyberkriminelle zu entwickeln und gegen Geld anzubieten. So geschehen mit der Malware as a Service V3B. Der im Darknet angebotene Werkzeugkasten für Cyberangriffe enthielt unter anderem vorgefertigte Phishing-Websites für mehr als 50 Banken in zehn europäischen Ländern, darunter auch namhafte Institute in Deutschland.

„Es ist nicht klar, ob die Macher dieses Phishing-Kits im konkreten Fall GenAI oder eine andere KI nutzten. Dennoch ist das die Zukunft, auf die sich nicht nur Finanzdienstleister einstellen müssen. Es zeigt, dass die Professionalisierung und Vermarktung von Cyberattacken als Dienstleistung mit Tempo voranschreitet", so der Sopra-Steria-Berater.

Finanzdienstleister reagieren auf neue Risiken

84 Prozent der befragten Finanzdienstleister werden deshalb in den kommenden zwölf Monaten noch stärker in die eigene Cybersecurity investieren, so die Studie. 43 Prozent der Unternehmen arbeiten konkret an einer an das KI-Zeitalter angepassten Cybersecurity-Strategie. Branchenübergreifend sind es 33 Prozent. Informationssicherheit hat für Banken und Versicherer einen großen Stellenwert. Das Vertrauen der Kunden ist für die Branche ein zentraler Wettbewerbsfaktor. „Die regulatorischen Anforderungen sind für Banken größer als für andere Branchen und das Sicherheitsniveau ist entsprechend hoch. Um diesen Standard auch im KI-Zeitalter zu halten, braucht es eine laufende strategische und operative Weiterentwicklung", sagt Hermann Hienz.

Mit KI gegen KI vorgehen

Ein Handlungsfeld ist beispielsweise die wirksame Sensibilisierung für die neuen Risiken, auch mithilfe von KI-Technologie: „Nicht jeder Mitarbeitende oder jede Kundin fällt auf

dieselben Tricks herein. Unternehmen benötigen somit dieselben Möglichkeiten für Vervielfältigung und Personalisierung von Aufklärungsmaßnahmen wie die Angreifer", sagt Stefan Beck, Experte für Managed Security Services bei Sopra Steria. „Lernende KI-Tools können unter anderem helfen, individuelle Awareness-Lücken zu schließen und Aufklärungskampagnen an neue oder nicht bekannte Angriffsmuster anzupassen."

Weitere Investitionsfelder sind der Schutz der Netzwerke und die Arbeit der Security Operations Center (SOCs) der Finanzdienstleister. „Eine neue SOC-Generation wird stärker automatisiert arbeiten und damit die Reaktionszeit auf Cyberangriffe deutlich verkürzen. KI-Lösungen werden zudem dabei helfen, Muster genauer zu analysieren, Anomalien aufzudecken sowie schnell die richtigen Entscheidungen zu treffen, und diese selbstständig umsetzen", so Stefan Beck von Sopra Steria.

Infos und Material zur Studie

Der Report „Cybersecurity im Zeitalter von KI" kombiniert eine repräsentative Erwerbstätigenbefragung mit einer Unternehmensbefragung. Der Marktforscher F.A.Z. Business Media | research hat im April und Mai 1.003 Erwerbstätige ab 15 Jahren in Deutschland repräsentativ befragt. Im April hat das Institut zudem 564 Fach- und Führungskräfte der Branchencluster Finance (Banken und Versicherer), Automotive (inkl. Zulieferern) und öffentliche Verwaltung online befragt.

Studien-PDF für Journalisten zur redaktionellen Verwendung

Themenwebsite „Sopra Steria Discover – Cybersecurity im Zeitalter von KI"

Pressefoto Hermann Hienz

Pressefoto Stefan Beck

Pressekontakt
Sopra Steria: Nils Ritter, Tel.: +49 (0) 151 40625911, E-Mail: nils.ritter@soprasteria.com
PER-Agency: Maya Engelmann, Tel.: +49 (0) 40 253185-143, E-Mail: maya.engelmann@per-agency.com

Infografik:

Die Schwachstellen in der Cybersecurity aus Sicht von Finanzdienstleistern
(Online-Befragung von 214 Entscheidern und Fachkräften)

Unangemessene Reaktion auf Phishing 45 %

Unangemessene Reaktion auf KI-gestütztes Social Engineering 34 %

Unzureichende Vorbereitung auf Angriffe 34 %

Personalmangel in der Cybersecurity-Fachabteilung 25 %

Fehlende Prozesse/Organisation für die Cybersecurity 27 %

Ungeregelte KI-Nutzung 29 %

Ungeregelter Zugriff von Mitarbeitern von außen 27 %

Schlecht abgesicherte Zugänge externer Partner in den Lieferketten 16 %

Weiß nicht/keine Angabe 7 %

Quelle: Sopra Steria, F.A.Z. Business Media | research, April 2024