LEARN-PHISH - Leveraging (Explainable) AI for Resilient Networks to support PHISHing Awareness

Nutzung (erklärbarer) KI für widerstandsfähige Netzwerke zur Unterstüzung der PHISHing-Awareness

Problem: E-Mail-Phishing-Angriffe sind nach wie vor die häufigste Einfalltür für Angreifer. Selbst wenn das Netzwerk und die Software auf dem aktuellen Stand sind, kann das gesamte Unternehmen gefährdet sein, wenn ein Mitarbeiter auf einen Link in einer Phishing-E-Mail klickt, seine Zugangsdaten auf einer bösartigen Website eingibt oder unabsichtlich Malware herunterlädt. Durch den Einsatz von künstlicher Intelligenz sind auch die ursprünglichen Erkennungsmerkmale, wie beispielsweise schlechte Rechtschreibung oder Grammatik, hinfällig. Zudem sind durch KI auch automatisierte Spear-Phishing-Angriffe, also gezielte Angriffe auf einzelne Personen, möglich. Aus diesem Grund sind neue Forschungsansätze nötig.

Unsere Lösung: Im Rahmen eines zukünftigen Forschungsprojekts möchten wir eine offene Plattform entwickeln. Auf dieser können sich Unternehmen zusammenschließen, um sich mittels künstlicher Intelligenz (KI) gegenseitig bei der Phishing-Abwehr zu unterstützen. Zu diesem Zweck entwickeln wir einen Phishing-Button für gängige E-Mail-Clients, mit dem sich verdächtige E-Mails direkt mit KI prüfen lassen. Im Anschluss soll die KI mittels Explainable AI (XAI) erklären, anhand welcher Merkmale sie die E-Mail als Phishing oder legitim klassifiziert hat. Dadurch soll ein Feedback erfolgen, sodass bei den Mitarbeitenden ein Lernerfolg erzielt wird. Zusätzlich wollen wir automatisierte Phishing-Simulationen integrieren, bei denen die Mitarbeitenden in unterschiedlichen Abständen eine Phishing-E-Mail erhalten. Dabei wird datenschutzfreundlich geprüft, ob jemand darauf geklickt hat. Falls dies der Fall ist, erfolgt ebenfalls mittels XAI eine eingebettete Schulung.

Die gemeldeten E-Mails sammeln wir auf der MISP-Plattform. MISP steht für „Malware Information Sharing Platform“ und ist eine Plattform zum schnellen Austausch von Informationen über Cyberangriffe. Die gemeldeten E-Mails werden dann dazu genutzt, KI-Modelle zu trainieren und dadurch zu verbessern. Mithilfe der MISP-Plattform können die trainierten Modelle datenschutzfreundlich (ohne dass echte E-Mails ausgetauscht werden müssen) mit anderen Unternehmen geteilt werden.

Wir suchen: Experimentierfreudige Unternehmen zur Teilnahme an einem zukünftigen Pilotprojekt, in dem eine auf das jeweilige Unternehmen zugeschnittene Lösung entwickelt und evaluiert wird. Je nach Größe und den Gegebenheiten des jeweiligen Unternehmens besteht die Möglichkeit, entweder einen eigenen MISP-Server zu nutzen oder auf einen externen MISP-Server zuzugreifen.

So profitieren Sie bei einer Teilnahme am Projekt: (1) Wir implementieren in Ihrem Unternehmen ein Anti-Phishing System und gewährleisten die fachliche Betreuung. (2) Wir unterstützen Lernprozesse in Ihrem Unternehmen, indem Mitarbeitende Feedback zu gemeldeten E-Mails erhalten und so Ihre Kompetenz im Umgang mit Phishing-E-Mails erweitern können.

Kontakt:
Prof. Dr. Florian Adamsky florian.adamsky@hof-university.de
Prof. Dr. Christian Groth christian.groth@hof-university.de

Hochschule Hof
University of Applied Sciences