KnowBe4

KI gegen KI

Abwehr von Cyberkriminellen mit einem KI-gestützten Programm für Security Awareness Training

KI gegen KI: Abwehr von Cyberkriminellen mit einem KI-gestützten Programm für Security Awareness Training

✦ Inhaltsverzeichnis

EINFÜHRUNG

Cyberkriminelle setzen verstärkt auf KI. Für uns bedeutet das neue Gefahren. Von Deepfakes bis hin zu KI-generierten Phishing-E-Mails – die neue Technologie hat sich zu einer leistungsstarken Waffe im Repertoire von Akteurinnen und Akteuren mit schlechten Absichten in aller Welt entwickelt.

Fachkräfte aus der Informationssicherheit wie Sie können den Spieß jedoch umdrehen. Vielleicht setzen Sie KI bereits in Ihrem Tech Stack ein. Mit dieser Technologie lässt sich auch die Human Firewall stärken. Denn bei Cybersicherheit geht es nicht nur um die Sicherheitsprodukte, die Sie installiert haben, sondern auch um die Menschen, für die Sie diese Produkte installiert haben.

Nutzen Sie die Leistungsfähigkeit von KI zu Ihrem Vorteil, indem Sie Ihren Nutzerinnen und Nutzern relevantes Training anbieten und sie über aktuelle Cyberangriffe auf dem Laufenden halten.

In diesem Whitepaper erfahren Sie, wie Cyberkriminelle KI zu ihrem eigenen Vorteil einsetzen, wie ein robustes KI-gestütztes Programm für Security Awareness Training (SAT) und Phishing-Simulationen aussieht und wie Sie Ihr Cybersicherheitspaket mithilfe von KI abrunden können.

KI VERSCHÄRFT DIE CYBERBEDROHUNGSLAGE

Sofern Sie Ihre Zeit nicht damit verbracht haben, mit DALLE-3 Bilder vom Mond zu generieren, um dahinter zu leben, kennen Sie die unzähligen Möglichkeiten, wie Cyberkriminelle generative KI und damit verbundene Tools für ihre Zwecke einsetzen.

KI wird nicht nur für Desinformations- und Fehlinformationskampagnen verwendet, sondern auch zur Automatisierung von vielschichtigen und facettenreichen Social-Engineering-Angriffen. Spezielle technische Kenntnisse werden dabei nicht benötigt.

Informationssicherheitsteams verfolgen diese Entwicklung mit Sorge. In einem aktuellen Report des Sicherheitsunternehmens Netacea gaben 93 % der befragten Sicherheitsfachkräfte an, dass sie damit rechnen, innerhalb der nächsten sechs Monate täglich mit KI-Angriffen konfrontiert zu werden. Fast zwei Drittel sind der Meinung, dass KI-gestützte Angriffe der Regelfall werden.

✦ Warum Phishing-Angriffe und Social Engineering durch KI immer ausgefeilter werden

➔ Automatische Generierung von Content

- KI-Anwendungen, insbesondere aus der Computerlinguistik zur automatischen Verarbeitung natürlicher Sprache, die auf großen Sprachmodellen basieren, können überzeugende Phishing-E-Mails erstellen, die grammatikalisch korrekt und kontextbezogen sind. Herkömmliche Spamfilter erkennen solche ausgefeilten Phishing-E-Mails oft nicht.
- Untersuchungen haben ergeben, dass die Erfolgswahrscheinlichkeit bei KI-generierten Phishing-E-Mails höher liegt als bei manuell erstellten Phishing-E-Mails. Eine Studie der Agentur der Europäischen Union für Cybersicherheit (ENISA) zeigt, dass mithilfe von KI in großem Maßstab hochgradig personalisierte Phishing-Mitteilungen erstellt werden können, die den Schreibstil bestimmter Personen imitieren.

➔ Personalisierte Spear-Phishing-Angriffe

- KI-Algorithmen können riesige Datenmengen aus Social Media und anderen Internetquellen auswerten und Informationen zu Zielpersonen zusammenstellen. Dadurch können Cyberkriminelle extrem überzeugende Spear-Phishing-E-Mails generieren, auf die Zielpersonen eher hereinfallen.
- Im Data Breach Investigations Report von Verizon wird erläutert, wie in KI-gestützten Social-Engineering-Angriffen präzise Informationen über die Interessen, Kontakte und Verhaltensweisen einer Person dafür genutzt werden, um die Erfolgschance dieser Angriffe zu erhöhen.

➔ Automatische Generierung von Phishing-Websites

- Mithilfe von KI lassen sich massenweise gefälschte Websites erstellen, die seriösen Websites täuschend ähnlich sehen. Diese Websites werden in Echtzeit angepasst, um unerkannt zu bleiben und authentischer zu erscheinen. Dadurch erhöht sich die Wahrscheinlichkeit, dass die Zielpersonen ihre Anmeldedaten eingeben.
- Laut einer in der Fachzeitschrift Computers & Security veröffentlichten Studie können KI-gestützte Phishing-Websites ihr Design und Verhalten anhand der Interaktion mit Nutzerinnen und Nutzer sowie anhand von Daten zur Bedrohungslage dynamisch anpassen, um länger unerkannt zu bleiben.

➔ Deepfake-Technologie

- KI-generierte Deepfakes sind realistisch wirkende Audio- oder Videoinhalte, in denen reale Personen imitiert werden. Cyberkriminelle geben sich mithilfe von Deepfakes als Führungskräfte oder vertrauenswürdige Personen aus und versuchen, die Zielpersonen zur Herausgabe sensibler Daten oder zur Autorisierung von Überweisungen zu verleiten.
- Die Cybersecurity and Infrastructure Security Agency (CISA) warnt vor Deepfakes in Zusammenhang mit Social-Engineering-Angriffen und verweist darauf, dass diese immer raffinierter werden und immer schwieriger zu erkennen sind.

KI ist zwar gerade in aller Munde, stellt jedoch keinen völlig neuen Angriffsvektor dar. Auch mithilfe von KI generierte Phishing-Mitteilungen (und zwar jede Menge davon) sollen emotionale Reaktionen hervorrufen und verängstigte Opfer zu Fehlern verleiten – z. B. Geld zu überweisen oder Malware in Systeme einzuschleusen. Die Abwehrmaßnahmen sind identisch. Es gilt, auf die gängigen Warnsignale für Social Engineering zu achten.

Aber wäre es nicht praktisch, zur Abwehr von KI-gestützten Angriffen ebenfalls KI einzusetzen?

KI CLEVER EINGESETZT: ROBOTER AN UNSERER SEITE

KI wird nicht nur von Cyberkriminellen eingesetzt, sie ist auch in Cybersicherheitstools integriert.

Ein wichtiger Einsatzbereich ist die intelligente E-Mail-Sicherheit. Veraltete E-Mail-Filter stützen sich auf die Analyse von Anhängen oder die Suche nach bekannten Malware-Signaturen. KI-gestützte E-Mail-Sicherheit geht darüber hinaus. Hier wird der tatsächliche Inhalt von E-Mails analysiert und nach subtilen Mustern und semantischen Besonderheiten gesucht, um moderne Social-Engineering-Angriffe zu erkennen.

KI und maschinelles Lernen spielen auch eine wichtige Rolle bei der Überwachung, Analyse und Erkennung von Cyberbedrohungen in Echtzeit. KI-Algorithmen können in Organisationen riesige Datenmengen (u. a. Netzwerktraffic, Endpunkte, Cloud-Services) erfassen und auswerten. Das bedeutet, dass die ersten Anzeichen einer Bedrohung mithilfe von KI früh erkannt und Warnungen zeitnah ausgelöst werden können, wodurch eine schnellere Reaktion auf Vorfälle möglich ist.

Die technische Seite ist jedoch nur ein Aspekt in der Bekämpfung von Cyberkriminalität. KI kann und sollte eingesetzt werden, um die Human Firewall zu stärken.

KI FÜR MENSCHEN: SECURITY AWARENESS TRAINING MIT PFIFF

Die Herausforderungen in der Informationssicherheit bleiben trotz der Vorteile, die KI mit sich bringt, bestehen:

- ➔ Erforderliche Wachsamkeit der Nutzerinnen und Nutzer aufgrund der rasanten Weiterentwicklung von KI-Technologien
- ➔ Mangelnde Abwehr von KI-gestützten Angriffen durch herkömmliche Sicherheitsmaßnahmen / Notwendigkeit von innovativen Verteidigungstaktiken
- ➔ Fehlende Ressourcen (Personal- und Zeitmangel), um auf neue Bedrohungen angemessen zu reagieren

Ein Hoffnungsschimmer stellen Fortschritte in Bezug auf Security Awareness Training und Phishing-Simulationen dar. KI kann laufende SAT-Programme modernisieren:

✦ Automatisiertes und nachhaltiges Training

KI-gestütztes SAT kann den Arbeitsaufwand für die für Sicherheitstraining verantwortlichen Teams deutlich reduzieren. Stellen Sie sich ein KI-gestütztes, anpassungsfähiges Trainingssystem vor, in dem Personen auf der Grundlage ihres individuellen Lernverlaufs automatisch ein Training zugewiesen wird. Die Effektivität absolvierter Trainingsmodule, aktuelle Ergebnisse aus SAT-Übungen und individuelle Präferenzen, z. B. bezüglich des Formats (Video, Quiz, Animation, Spiel), werden ebenso berücksichtigt wie die Dauer, um allen ein maßgeschneidertes Training bereitzustellen.

KI-gestütztes SAT kann den Arbeitsaufwand für die für Sicherheitstraining verantwortlichen Teams deutlich reduzieren.

Ein solcher Ansatz würde nicht nur Administratorinnen und Administratoren entlasten. Es würde auch die Relevanz des Trainings für die einzelnen Nutzerinnen und Nutzer erhöhen, sodass die Lerninhalte mit höherer Wahrscheinlichkeit nachhaltig verinnerlicht werden.

Nach Abschluss des ersten Trainings können mithilfe von KI auch Quizfragen generiert werden. Quizfragen können sich auf die Trainingsinhalte oder die Richtlinien der Organisation beziehen. Das Erstellen der Quizfragen übernimmt dabei generative KI. Im Quiz werden die wichtigsten Erkenntnisse wiederholt. Es soll sichergestellt werden, dass die Informationen nicht nur vermittelt, sondern auch verstanden wurden.

✦ Optimierte simulierte Phishing-Kampagnen

Eine KI-gestützte Engine könnte automatisch den aktuell besten Phishing-Test für jede Nutzerin und jeden Nutzer auswählen. Stellen Sie sich vor, Sie könnten für jede einzelne Nutzerin und jeden einzelnen Nutzer eine eigene Phishing-Kampagne erstellen, die auf das individuelle Niveau zugeschnitten ist.

Warum sollten Sie sich auf KI-generierte Kampagnen beschränken? Generative KI-Tools können Ihnen auch beim Erstellen von Phishing-Vorlagen helfen, um Ihre Organisation mit ganz verschiedenen Vorlagen und Dimensionen auf Angriffe vorzubereiten. Die Fähigkeit, sich an neue Bedrohungen anzupassen und neue Phishing-Vorlagen zu erstellen, ist vor dem Hintergrund sich ständig weiterentwickelnder Bedrohungsvektoren von entscheidender Bedeutung.

✦ KI + Crowd = unschlagbar gut

In einem SAT-Programm sollten Nutzerinnen und Nutzer die Möglichkeit haben, simulierte Phishing-E-Mails und E-Mails, bei denen der Verdacht auf Phishing besteht, zu melden. Ihre Nutzerinnen und Nutzer möchten bei der Abwehr von Cyberangriffen helfen. Geben Sie ihnen die geeigneten Tools zur Hand, mit denen sie Ihre Umgebung proaktiv verteidigen können.

Generative KI-Tools können Ihnen auch beim Erstellen von Phishing-Vorlagen helfen, um Ihre Organisation mit ganz verschiedenen Vorlagen und Dimensionen auf Angriffe vorzubereiten.

Dank dieser Tools können Nutzerinnen und Nutzer reale Phishing-Kampagnen schneller als mit herkömmlichen Methoden melden. KI-gestützte E-Mail-Sicherheitstools und die Hilfe aus der Crowd tragen zur Weiterentwicklung der KI bei, da Nutzerinnen und Nutzer und Sicherheitsteams Daten (in diesem Fall verdächtige und schädliche E-Mails) in großen Mengen identifizieren, überprüfen und sammeln.

Eine derartige KI-basierte Analyse von Phishing-Bedrohungsdaten schützt Ihre Organisation vor neuen Phishing-Angriffen. Dies trägt dazu bei, dass Sie proaktiv und schnell auf neue Phishing-Angriffe auf Ihre Organisation reagieren können.

FAZIT: KI WIRD BLEIBEN

Die Auswirkungen von KI auf die Gesellschaft sind nicht mehr nur theoretisch. Sie sind bereits zu spüren. Daher stellt sich nicht die Frage, ob Sie KI in Ihre Cybersicherheits- und SAT-Programme integrieren, sondern *wann*.

Organisationen müssen Feuer mit Feuer bekämpfen. Durch den Einsatz von KI in Programmen für Security Awareness Training können Unternehmen die Risiken durch den Faktor Mensch kontrollieren und Cyberkriminellen das Leben schwer machen.

Letztendlich ist die Investition in ein KI-gestütztes Security Awareness Training eine wichtige Strategie, um eine starke Sicherheitskultur zu gewährleisten und sich gegen die gewaltigen Cyberbedrohungen von heute und morgen zu schützen.

MEHR ERFAHREN → **Ansatz von KnowBe4 in Bezug auf KI-gestützte Security Awareness kennenlernen**

Weitere Ressourcen

Kostenloser Phishing Security Test
Finden Sie mit dem kostenlosen Phishing Security Test heraus, wie viele Mitarbeitende auf eine Phishing-Simulation hereinfallen (Phish-prone Percentage).

Kostenlose Vorschau des Trainings
Stöbern Sie in unserer Bibliothek mit Inhalten zum Thema Sicherheitsbewusstsein. Suchen Sie nach Titel, Kategorie, Sprache oder Content.

Kostenloses Automated Security Awareness Program (ASAP)
Erstellen Sie ein individuelles Security Awareness Program für Ihre Organisation.

Kostenloser Phish Alert Button
Bieten Sie Ihren Mitarbeitenden die Möglichkeit, Phishing-Angriffe mit einem Klick zu melden.

Kostenloser Domain Spoof Test
Finden Sie heraus, ob Hackerinnen oder Hacker eine E-Mail-Adresse Ihrer Domain spoofen können.

Über KnowBe4

KnowBe4 befähigt Ihre Mitarbeitenden, jeden Tag intelligente Sicherheitsentscheidungen zu treffen. Zehntausende von Organisationen weltweit stärken mit der KnowBe4-Plattform ihre Sicherheitskultur und reduzieren menschliche Fehler. KnowBe4 stärkt die Abwehrkräfte von Organisationen durch den Aufbau einer zuverlässigen Human Firewall mit New-School Security Awareness and Compliance Training.

KnowBe4 sorgt dafür, dass Nutzerinnen und Nutzer wachsam sind und Phishing, Ransomware sowie andere Social-Engineering-Bedrohungen abwenden möchten. Auf der Plattform steht Ihnen ein umfassendes Angebot zur Verfügung: Security Awareness and Compliance Training, Coaching in Echtzeit, KI-gestützte Social-Engineering-Simulationen und Phishing-Abwehr mithilfe der Crowd.

Die Inhalte werden in mehr als 35 Sprachen lokalisiert. Damit bietet KnowBe4 die weltweit größte Bibliothek mit stets aktuellen und ansprechenden Inhalten zur Stärkung Ihrer Human Firewall.

Weitere Informationen unter www.KnowBe4.com/de

KnowBe4

KnowBe4 Germany | Rheinstr. 45/46 | 12161 Berlin – Deutschland
+49 30 34 64 64 60 | www.Knowbe4.com/de | kontakt@knowbe4.com

04E06K01