Mit der richtigen Formel vor Cyberangriffen schützen

Neue Gefahren durch künstliche Intelligenz

Keywords
- *Cybersecurity*
- *Training*
- *künstliche Intelligenz*

Daten aus Industrieunternehmen sind ein lukratives Ziel für Angreifer, die inzwischen vermehrt auch KI-Tools einsetzen. Während sich vernetzte Anlagen und Systeme z.B. durch Firewalls, Antivirenprogramme und Co. gegen Hackerangriffe schützen lassen, gibt es noch einen weiteren bedeutenden Risikofaktor: die Mitarbeiter. Für einen effektiven Schutz vor Cybercrime, ist ein regelmäßiges Training nützlich, um für Phishing zu sensibilisieren und den Umgang mit KI-Tools zu schulen.

Branchenübergreifend sind Mitarbeiter eine der größten Schwachstellen in puncto Cybersicherheit. Ungeschulte Mitarbeiter können Angreifern unwissentlich die Türen zum Unternehmen öffnen – und das bereits durch einen falschen Klick.

Phishing-Angriffe sind eine der häufigsten Methoden, um Mitarbeiter zu täuschen, durch sie an sensible Informationen zu gelangen oder sich in das Unternehmensnetz einzuschleusen.

Was ist Phishing?

Bei Phishing handelt es sich um gefälschte E-Mails, die von Cyberkriminellen versendet werden. Sie zielen darauf ab, an vertrauliche Informationen zu gelangen oder Schadsoftware wie Malware zu installieren und sich so Zugriff auf das Unternehmensnetzwerk – inklusive IT-Systemen oder vernetzten Maschinen und Anlagen – zu verschaffen. Phishing-Mails enthalten nicht nur Aufforderungen, sensible Informationen preiszugeben, sondern häufig auch schädliche Links oder Anhänge. Sobald diese angeklickt oder heruntergeladen werden, kann die Malware das Gerät infizieren und Cyberkriminellen eine Tür in das Unternehmensnetzwerk öffnen.

Mit ein wenig Übung konnten Phishing-Mails bislang gut an unprofessionellen Designs, fehlerhafter Grammatik oder Rechtschreibung erkannt werden. Doch dies ändert sich nun. Grund ist der Einsatz von künstlicher Intelligenz (KI).

Neue Gefahren durch künstliche Intelligenz

KI bietet viele Möglichkeiten, um Prozesse in Unternehmen zu beschleunigen oder zu optimieren. Auch zur Verbesserung der Cybersicherheit kann künstliche Intelligenz einen wichtigen Beitrag leisten. Diese Vorteile haben allerdings auch Cyberkriminelle schnell erkannt. Viele Hacker nutzen generative KI-Tools wie GPT-4, um ihre Taktiken zu verbessern. Die Fortschritte in der KI ermöglichen es Angreifern, authentisch aussehende Phishing-Mails zu erstellen, die von legitimen E-Mails nur schwer zu unterscheiden sind. Traditionelle Methoden zum Erkennen von Phishing-Angriffen stoßen dadurch mittlerweile an ihre Grenzen.

KI-Tools in den Händen von Mitarbeitern

Aber nicht nur in den Händen von Cyberkriminellen können KI-Tools Schaden für Unternehmen anrichten. Immer mehr Mitarbeiter nutzen Tools wie ChatGPT für alltägliche Aufgaben – vom Schreiben professioneller Inhalte bis hin zur Behebung von Fehlern in Quellcodes. Meist sind sie sich nicht darüber im Klaren, dass dies ihr Unternehmen dem Risiko von Datenschutzverletzungen und Sicherheitslecks aussetzen kann.

Auch wenn der Chat mit KI-Bots privat erscheinen mag, sammeln diese Tools alles,

was dort eingegeben wird. Darüber hinaus liefern KI-Tools nicht immer zuverlässige Informationen. Da die KI-Engines von Eingaben der Nutzer „lernen“, können sie Fehlinformationen oder sogar schadhaften Code enthalten.

Tipps zum Schutz vor KI-gesteuerten Cyberangriffen

- Absender von E-Mails überprüfen und deren Identität bestätigen. Dies ist entscheidend, da es sich um einen Bereich handelt, den Hacker nur sehr schwer fälschen können.
- Validierung von Hyperlinks in unbekannten Texten und E-Mails. Dazu mit dem Mauszeiger über die Links fahren und sie auf verdächtige URLs überprüfen, die nicht mit der Textbeschreibung übereinstimmen. Auf diesem Weg lässt sich vermeiden, dass das Gerät und das Netzwerk versehentlich Sicherheitsbedrohungen ausgesetzt werden.
- Bei der Nutzung von KI-Tools für die Arbeit sollten die Eingaben (Prompts) keine persönlichen Informationen wie Namen, E-Mail-Adressen usw. enthalten.
- Finanzielle Informationen, Quellcode oder interne Kommunikation sollten aus Prompts in KI-Tools entfernt werden.
- Keine Inhalte, die sich auf die Unternehmensstrategie beziehen, in ein KI-Tool eingeben.

Wichtiger denn je ist ein ganzheitliches Sicherheitskonzept, das nicht nur technische, sondern insbesondere auch menschliche Faktoren und bewährte Praktiken einschließt. Folgende Schritte können Unternehmen ergreifen, um sich besser gegen aktuelle Gefahren aus dem Netz zu wappnen:

- **E-Mail-Filterung und -Authentifizierung**: Unternehmen sollten fortschrittliche E-Mail-Filter und -Authentifizierungssysteme einsetzen, um verdächtige E-Mails frühzeitig zu erkennen und zu blockieren.
- **Patch-Management:** Die Aktualisierung von Software und Systemen ist entscheidend, um bekannte Schwachstellen zu beheben und Angriffspunkte zu minimieren.
- **Monitoring und Incident Response**: Die kontinuierliche Überwachung des Netzwerks und eine effiziente Incident-Response-Strategie sind unverzichtbar, um Angriffe frühzeitig zu erkennen und abzuwehren.
- **Künstliche Intelligenz nutzen**: Unternehmen können selbst KI-Tools einsetzen, um verdächtiges Verhalten zu erkennen und automatisch Gegenmaßnahmen zu ergreifen.
- **Regelmäßiges Cybersecurity Training**: Schulungen und Phishing-Simulationen können Mitarbeiter für die Gefahren von Phishing-Angriffen und anderen Social-Engineering-Techniken sensibilisieren. Wichtig ist, dieses Training mit kurzen Lerneinheiten regelmäßig durchzuführen, um jederzeit auch die neuesten Angriffsmethoden zu kennen und darauf vorbereitet zu sein. Dabei sollten die individuellen Positionen, Abteilungen, Standorte und Risikolevel der Mitarbeiter berücksichtigt werden. Denn während ein HR-Mitarbeiter vielleicht eine gefälschte Bewerbung per Mail erhält, bekommen Mitarbeiter in der Buchhaltung eine falsche Zahlungsaufforderung und Produktionsmitarbeiter wiederum eine falsche Information zu Änderungen im Produktionsprozess.

Um das Sicherheitsrisiko durch das eigene Team zu reduzieren, ist regelmäßiges Security Awareness Training unerlässlich. Moderne Trainingsplattformen mit Machine Learning dienen als effektives Tool, um individuell das Sicherheitsbewusstsein aller Mitarbeiter zu schärfen und sich auch vor neuesten Gefahren aus dem Netz zu wappnen.

Der Autor
Dirk Rausse,
Regional Sales Director
DACH & Nordic, Cybeready

Wiley Online Library

Cybeready, Santa Clara, USA
dirk@cybereready.com · www.cybereready.com/de

Fernwartung für sicherheitskritische Anlagen

Der IT-Sicherheitsspezialist genua unterstützt für seine Fernwartungslösung genubox neben seiner bewährten nativen Microsoft-Windows-App nun auch den Remote-Zugriff via Webinterface. Die Fernwartung wird damit noch unabhängiger von Zeit, Ort sowie dem Betriebssystem des Fernwartungs-Clients. Selbst mobile Fernwartungs-Sessions von unterwegs auf sicherheitskritische Maschinen und Anlagen, z.B. über den Browser eines Tablet-PCs, lassen sich so zuverlässig geschützt durchführen. Das neue Webinterface erlaubt den https-basierten Aufbau einer Remote-Desktop-Verbindung zu einem Rendezvous-Server, um eine vorkonfigurierte Fernwartungssession zu initiieren. Die Identität des Benutzers wird dabei über Identity Provider wie Okta, Azure Active Directory oder Keycloak mittels des Identitätsprotokolls OpenID Connect geprüft. Der Rendezvous-Server kann sich dabei in der demilitarisierten Zone (DMZ) des LAN-Betreibers, des Fernwarters oder in der Cloud befinden. War der Log-in erfolgreich und wurde die Fernwartungssession vom Anlagenbetreiber genehmigt, sehen Fernwarter anschließend alle mittels RDP (Remote Desktop Protocol), VNC oder SSH (Secure Socket Shell) angebundenen Zielsysteme, für die sie autorisiert sind. Dabei wird äußerst granular gesteuert, welcher Fernwarter mit welcher Applikation auf welches Zielsystem zugreifen darf. So werden moderne Zero-Trust-Konzepte unterstützt. Als Rendezvous-basierte Lösung entspricht die Fernwartung dem vom Verband Deutscher Maschinen- und Anlagenbau (VDMA) empfohlenen

© Genua

Goldstandard für sichere Fernwartungsarchitekturen. Sie erfüllt zudem alle BSI-Empfehlungen an eine sichere Fernwartung im industriellen Umfeld. Je nach Anforderungen sind Hardware-basierte, virtualisierte oder hybride Setups möglich. **www.genua.de**