

Wenn Daten zu Ködern werden: Wie KI Phishing verschärft

25.08.2026, 13:02 | IT, New Media & Software

Pressemitteilung von: *n-komm GmbH*



n-komm GmbH

Phishing gehört seit Jahren zu den häufigsten Einfallstoren für Cyberangriffe. Das Prinzip ist unverändert: Angreifer täuschen eine vertrauenswürdige Person oder Organisation vor, um Opfer zur Eingabe von Zugangsdaten, zur Freigabe einer Anmeldung, dem Öffnen eines Anhangs oder einer Zahlungsausführung zu bewegen. Verändert haben sich allerdings Qualität, Geschwindigkeit und Reichweite solcher Angriffe. Die zunehmende Verbreitung von Künstlicher Intelligenz (KI) ermöglicht es, große Datenmengen auszuwerten, glaubwürdige Nachrichten zu formulieren und Kampagnen mit geringem Aufwand zu personalisieren.

Das Bundesamt für Sicherheit in der Informationstechnik bewertet KI vor allem als Verstärker bekannter Angriffsmethoden indem Recherche beschleunigt, Sprachbarrieren überwunden und professionell wirkende Inhalte mit geringerem Aufwand erzeugt werden können. Dadurch nähert sich Massenphishing dem bislang aufwendigeren Spearphishing an. Sprachmodelle können öffentliche Informationen zusammenfassen, Zielgruppen sortieren und passende Texte in mehreren Sprachen erstellen.

Für einen Angriff sind nicht nur Passwörter oder Bankdaten relevant. Auch scheinbar harmlose Angaben können wertvoll sein: Name, E-Mail-Adresse, Arbeitgeber, Position, Geschäftspartner oder Informationen über laufende Projekte. Werden solche Daten verknüpft, entsteht ein Profil, aus dem sich ein überzeugender Köder konstruieren lässt.

Viele der Informationen stammen aus sozialen Netzwerken, Unternehmenswebsites oder Stellenausschreibungen. Hinzu kommen Daten aus Sicherheitsvorfällen, wobei ein Leak von Daten über deren initiale Veröffentlichung hinausgehen

kann. Gestohlene Datensätze können kopiert, verkauft und mit anderen Quellen kombiniert werden. Dies geschieht unter anderem in Untergrundforen und im Darknet, wo Zugangsdaten, Kundenlisten, Schadsoftware, Phishing-Kits und komplette Angriffsdienstleistungen gehandelt werden. Selbst Jahre später können solche Daten für Identitätsdiebstahl, Erpressung oder Social Engineering genutzt werden.

Wie gefährlich reale Daten als Vertrauensanker sind, zeigte eine Sextortion-Kampagne mit E-Mail-Adressen aus veröffentlichten ShinyHunters-Datensätzen. Die Täter nannten von einem Leak betroffene Unternehmen und behaupteten, Geräte und Kameras der Empfänger kompromittiert zu haben. Für die angebliche Nichtveröffentlichung intimer Aufnahmen forderten sie Bitcoin-Zahlungen. Auch wenn die Vorwürfe erfunden waren, wirkten sie durch die korrekten Angaben im Kontext plausibel. Ebenso können andere Kriminelle verfügbare Informationen später für neue Kampagnen nutzen.

KI verschärft dieses Risiko, weil sie Personalisierung skalierbar macht. Früher bedeutete eine individuell formulierte Nachricht erheblichen Recherche- und Zeitaufwand. Heute lassen sich in kurzer Zeit zahlreiche sprachlich korrekte Varianten erstellen, die an Tätigkeit, Branche und Kommunikationsstil der Zielperson angepasst sind. Rechtschreibfehler oder schlechte Übersetzungen verlieren dadurch als Warnsignal an Bedeutung.

Werkzeuge wie SpamGPT verbinden KI-gestützte Texterstellung mit Kampagnenplanung, Versand und Erfolgskontrolle. Dolphin X nutzt KI, um kompromittierte Systeme und gestohlene Informationen nach ihrem potenziellen Wert zu priorisieren. Mit diesen Funktionssammlungen unterstützt KI nicht nur die Formulierung des Köders, sondern auch die Auswahl der Opfer und die Verarbeitung erbeuteter Daten.

Parallel wächst das Angebot von Phishing-as-a-Service-Plattformen. Forg365 zielt auf Microsoft-365-Konten und verbindet KI-generierte Köder mit Device-Code-Phishing sowie dem Diebstahl von Sitzungstokens. Dabei wird das Opfer auf eine legitime Microsoft-Seite geführt und dazu gebracht, ein vom Angreifer kontrolliertes Gerät zu autorisieren. Im Anschluss können Angreifer mit gültigen Tokens oder Sitzungscookies eingerichtete Schutzmechanismen umgehen und auf Postfächer oder Cloud-Daten zugreifen.

Ein kompromittiertes Konto repräsentiert häufig den Ausgangspunkt weiterer Angriffe, da beispielsweise ein übernommenes Postfach das Auslesen von Kommunikationsverläufen, Kontakten, Rechnungen und interne Abläufen gestattet. Kompromittierte Adressen können weiterführend zum Versand neuer Phishing-Nachrichten von einer bekannten Adresse verwendet werden und sich auf echte Vorgänge beziehen, wodurch die Glaubwürdigkeit erhöht wird.

Über Textnachrichten hinaus bilden auch Stimmen, Bilder und Videos keine verlässlichen Identitätsmerkmale mehr. KI kann Sprachnachrichten erzeugen, Stimmen mittels kurzer Sprachaufnahmen imitieren und Bild- oder Videoinhalte manipulieren. Daraus ergibt sich die Schwierigkeit, dass eine vertraute Stimme oder fehlerfreie Nachricht nicht länger die Identität des Absenders beweisen.

Gerade weil KI Phishing-Nachrichten glaubwürdiger, personalisierter und skalierbarer macht, reichen technische Schutzmaßnahmen allein nicht aus. Mitarbeitende müssen lernen, auch professionell formulierte, kontextbezogene und sprachlich fehlerfreie Angriffe kritisch zu hinterfragen. Mit unseren Leistungen im Bereich Security Awareness bereiten wir Organisationen gezielt auf diese Entwicklung vor. Realitätsnahe Phishing-Simulationen, interaktive Trainings und individuell konzipierte, manuell durchgeführte Phishingkampagnen bilden aktuelle Angriffsmethoden praxisnah ab und zeigen, wie gut Beschäftigte auf KI-gestützte Täuschungsversuche, manipulierte Absenderidentitäten und glaubwürdige Social-Engineering-Szenarien reagieren.

Gleichzeitig ist entscheidend, frühzeitig zu erkennen, welche Informationen Angreifern bereits zur Verfügung stehen und wie diese für personalisierte Kampagnen genutzt werden könnten. Unsere Leistungen im Bereich Cyber Threat Intelligence schaffen hierfür die notwendige Transparenz. Durch Darkweb Monitoring, die Analyse der aktuellen Bedrohungslandschaft und die Untersuchung der externen Angriffsoberfläche identifizieren wir kompromittierte Daten, relevante Aktivitäten von Bedrohungsakteuren und potenzielle Angriffspunkte. So lässt sich besser einschätzen, welche realen Informationen als Grundlage für KI-gestützte Phishing-Angriffe dienen könnten. Die Verbindung aus Security Awareness und Cyber Threat Intelligence ermöglicht es Organisationen, sowohl das Verhalten ihrer Mitarbeitenden als auch ihre tatsächliche externe Gefährdungslage gezielt in die Phishing-Abwehr einzubeziehen.

n-komm GmbH

Unterweingartenfeld 6
Karlsruhe 76135
Deutschland

AlexanderKühn (CEO)

+49 721 35460-0

info@n-komm.de

n-komm.de

Portrait

Die n-komm GmbH mit Sitz in Karlsruhe ist ein IT-Dienstleister und Digitalisierungspartner für Unternehmen und öffentliche Verwaltungen. Das Unternehmen unterstützt seine Kunden bei der digitalen Transformation – von der Analyse und Konzeption über die Implementierung bis hin zum Betrieb und Support moderner IT-Lösungen.

Zum Leistungsspektrum gehören Lösungen für Dokumentenmanagement (DMS), Enterprise Content Management (ECM), digitale Geschäftsprozesse und Workflow-Automatisierung sowie Microsoft-365-Lösungen. Darüber hinaus entwickelt und realisiert die n-komm GmbH umfassende Konzepte im Bereich Cyber Security – von der Prävention über die Erkennung bis zur Reaktion auf Sicherheitsvorfälle.

Mit langjähriger Projekterfahrung, einem interdisziplinären Expertenteam und starken Technologiepartnerschaften begleitet die n-komm GmbH Organisationen bei der Umsetzung zukunftsfähiger Digitalisierungs- und Sicherheitsstrategien. Mit der jährlich stattfindenden n-komm Connect bietet das Unternehmen zudem eine Plattform für den fachlichen Austausch zu aktuellen Entwicklungen in den Bereichen Digitalisierung und IT-Sicherheit.

News-ID: 1321481 • Views: 189 (Stand: 11.10.2026)

Link zur Pressemitteilung:

<https://www.openpr.de/news/1321481/Wenn-Daten-zu-Koedern-werden-Wie-KI-Phishing-verschaerft.html>