Werden Hacker 2025 mehr KI bei Ransomware-Angriffen einsetzen?

Kurze Antwort: Ja. Es wird erwartet, dass Angreifer ihren Einsatz von künstlicher Intelligenz, insbesondere von großen Sprachmodellen, weiter ausbauen, um vertrauenswürdige Personen zu imitieren und Opfer dazu zu bringen, Zugriff oder Vertrauen zu gewähren.

Warum KI bei Hackern so beliebt geworden ist

Suchergebnisse, Nachrichtenfeeds und alltägliche Gespräche sind mittlerweile von KI-Bezügen durchdrungen, und dieselbe Begeisterung hat auch bei Cyberkriminellen Einzug gehalten. Wenn die meisten Menschen von KI sprechen, meinen sie damit in der Regel große Sprachmodelle wie jene, die hinter ChatGPT und ähnlichen Tools stehen und die menschliche Kommunikation überzeugend nachahmen können. Angreifer haben erkannt, dass diese Fähigkeit für Social Engineering äußerst nützlich ist. Anstatt sich auf generische Phishing-E-Mails zu verlassen, können sie Nachrichten, Stimmen oder Gespräche erzeugen, die einem echten Kollegen, Lieferanten oder einer Autoritätsperson stark ähneln, wodurch es erheblich leichter wird, das Vertrauen eines Ziels zu gewinnen, bevor zugeschlagen wird.

Mit ausgefeilteren Imitationstaktiken ist zu rechnen

Der Trend für 2025 besteht nicht darin, dass KI-gestützte Angriffe grundlegend neu sind, sondern dass sie ausgefeilter und geschäftsmäßiger werden. So wie seriöse Unternehmen KI-gestützte Vertriebsagenten und automatisierte Outreach-Tools einführen, verfeinern auch Angreifer ihre eigenen KI-gestützten Imitationstechniken. Das bedeutet überzeugendere Nachrichten, die Vorgesetzte, Kollegen oder vertrauenswürdige Partner nachahmen, allesamt darauf ausgelegt, die Arbeitsbeziehungen auszunutzen, auf die sich Menschen tagtäglich verlassen. Die Gefahr besteht darin, dass ein Gespräch, das sich persönlich und legitim anfühlt, in Wirklichkeit von einem hochentwickelten KI-System stammen könnte, das darauf ausgelegt ist zu manipulieren, nicht zu helfen.

Was das für die Verteidigung bedeutet

Da diese Imitationstaktiken ausgereifter werden, sollten Organisationen davon ausgehen, dass vertrauensbasierte Angriffe allein durch Intuition schwerer zu erkennen sein werden. Die Überprüfung von Anfragen über unabhängige Kanäle, anstatt einer Nachricht oder einem Anruf blind zu vertrauen, wird immer wichtiger. Da diese Angriffe darauf ausgelegt sind, das menschliche Urteilsvermögen zu umgehen, bietet das Vorhandensein automatisierter Erkennungs- und Reaktionsfähigkeiten, wie sie in Cyber Crucible's FortressAI integriert sind, eine zusätzliche Schutzebene, wenn Social Engineering die Abwehrmechanismen einer Person erfolgreich überwindet.

https://player.vimeo.com/video/1046827321

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Revision #1
Created 2026-07-24 05:08:09 UTC by Dennis Underwood
Updated 2026-07-24 05:08:09 UTC by Dennis Underwood