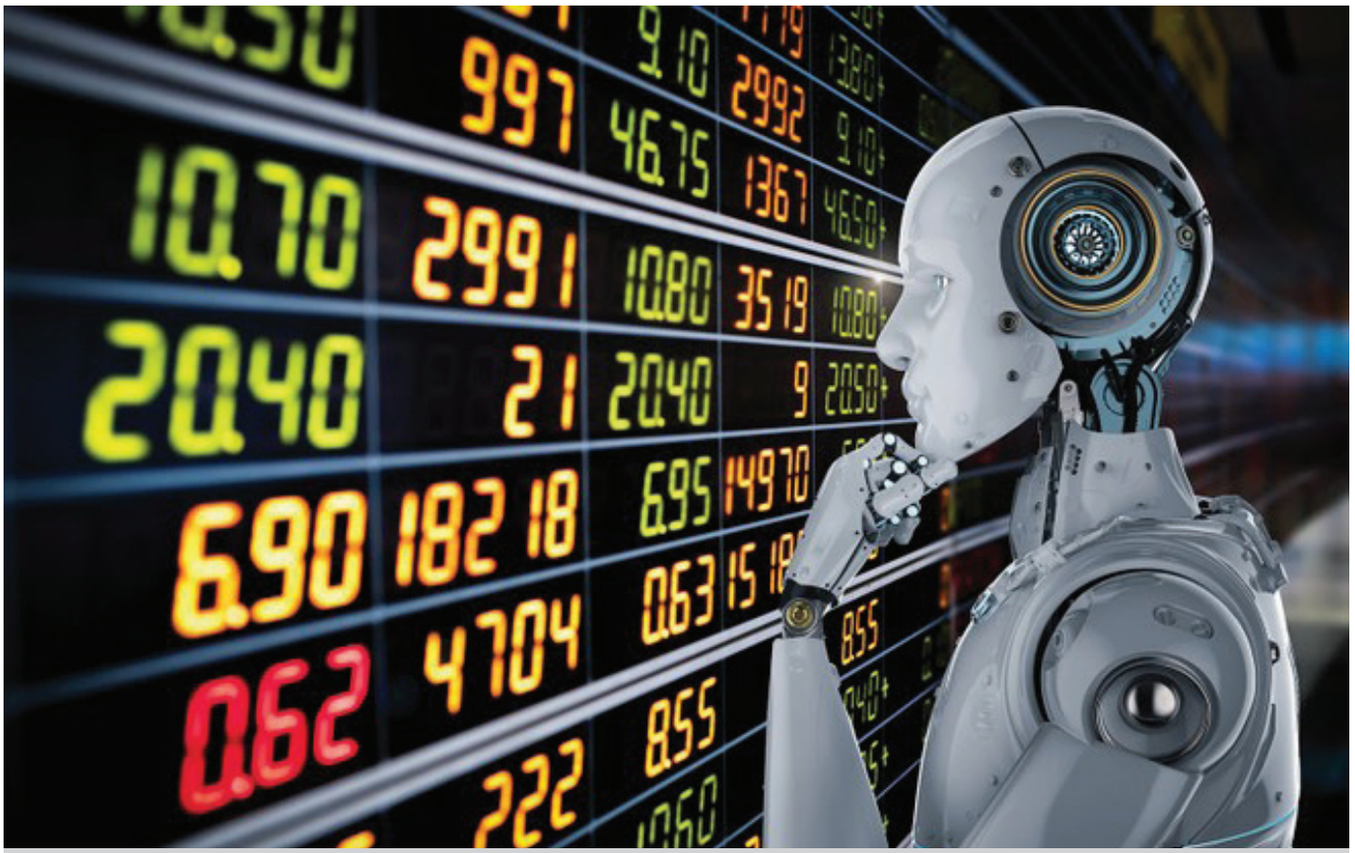

AI có thể mang lại rủi ro gian lận và thao túng thị trường.

NGUY CƠ TỪ SHADOW AI TRONG HOẠT ĐỘNG TÀI CHÍNH

Phạm Bá Thọ[1], Trương Đình Dũng[2], Nguyễn Hoàng Nam[1]

[1]Trường Sĩ quan Chính trị, Bộ Quốc Phòng
[2]Trường Cao đẳng Kỹ thuật Thông tin, Bộ Quốc Phòng

Trí tuệ nhân tạo (AI) đã và đang thay đổi cách thức các tổ chức vận hành và quản lý. Tuy nhiên, cùng với những tiềm năng to lớn, AI cũng mang đến những thách thức không nhỏ đối với an ninh mạng, đặc biệt khi xu hướng "Shadow AI" đang gia tăng. Năm 2025, Shadow AI được dự báo sẽ trở thành mối lo ngại lớn về an ninh mạng đối với các doanh nghiệp và tổ chức trên toàn cầu, ảnh hưởng trực tiếp đến hoạt động tài chính và kinh doanh.

Shadow AI là gì?

Shadow AI là thuật ngữ được dùng để chỉ việc nhân viên trong các tổ chức sử dụng các công cụ AI mà không có sự phê duyệt, giám sát hoặc quản lý của bộ phận phụ trách về công nghệ thông tin hoặc an ninh mạng. Với sự phát triển nhanh chóng của công nghệ AI như ChatGPT, Gemini, Grok, DeepSeek… việc dễ tiếp cận và sử dụng những công cụ này, dẫn đến việc nhân viên sử dụng chúng nhưng thiếu sự kiểm soát của các đơn vị, cá nhân có trách nhiệm. Theo báo cáo mới đây của Arize AI (Hoa Kỳ) - một nền tảng nghiên cứu theo dõi thông

AI có thể can thiệp trong lĩnh vực tài chính. Ảnh: nhandan.vn.

tin công bố của doanh nghiệp lớn, 56% các công ty thuộc danh sách Fortune 500 xem AI là "yếu tố rủi ro", tỷ lệ này tăng vọt so với mức 9% trong năm 2022. Shadow AI làm gia tăng mối đe dọa nội bộ vì tổ chức không thể theo dõi hoặc quản lý dữ liệu được xử lý bởi các công cụ này. Chẳng hạn, nếu một nhân viên dùng AI để phân tích dữ liệu khách hàng mà không qua hệ thống bảo mật nội bộ, dữ liệu đó có thể bị rò rỉ mà không ai hay biết. Trong năm 2023, đã có nhiều trường hợp sử dụng deepfake giọng nói được tạo bởi AI để lừa đảo tài chính, và xu hướng này dự kiến tăng mạnh trong năm 2025.

Theo báo cáo từ Google Cloud năm 2024, các tổ chức ngày càng khó khăn trong việc kiểm soát Shadow AI, với 67 công cụ AI tạo sinh trung bình được sử dụng trong một công ty, nhưng 90% trong số đó không có giấy phép hoặc phê duyệt chính thức. Điều này củng cố nhận định rằng, Shadow AI đang vượt ngoài tầm kiểm soát. Các chuyên gia đã chuyển mối quan tâm từ các cuộc tấn công bên ngoài sang các mối đe dọa nội bộ, đặc biệt là nguy cơ từ Shadow AI do khả năng lạm dụng AI tạo sinh và AI không được kiểm soát.

Một số nguy cơ từ Shadow AI đối với hoạt động tài chính và kinh doanh

Với tốc độ phát triển của AI và sự thiếu hụt các chính sách quản lý, Shadow AI có thể dẫn đến một số thách thức sau:

Rủi ro bảo mật và rò rỉ dữ liệu

Khi nhân viên sử dụng các công cụ AI không được phê duyệt (ví dụ: chatbot, công cụ phân tích dữ liệu, hoặc nền tảng AI bên thứ ba), dữ liệu nhạy cảm như thông tin khách hàng, giao dịch tài chính hoặc chiến lược kinh doanh có thể bị rò rỉ hoặc lưu trữ trên các hệ thống không an toàn. Các công cụ này thường không tuân thủ các tiêu chuẩn bảo mật của tổ chức, làm tăng nguy cơ tấn công mạng hoặc vi phạm dữ liệu nghiêm trọng.

Vi phạm quy định và pháp lý

Các tổ chức tài chính phải tuân thủ nhiều quy định nghiêm ngặt như GDPR (Quy định bảo vệ dữ liệu chung), CCPA (Đạo luật Quyền riêng tư người tiêu dùng), PCI-DSS (Bộ tiêu chuẩn bảo mật dữ liệu thẻ thanh toán) hoặc các quy định của Ủy ban Chứng khoán và Giao dịch Hoa Kỳ (SEC) và Cơ quan quản lý ngành tài chính (FINRA). Sử dụng AI không được

kiểm soát có thể dẫn đến vi phạm và bị phạt nặng. Ví dụ: Nếu sử dụng AI để tự động ra quyết định về tín dụng mà không tuân thủ các quy định về công bằng tài chính, công ty có thể bị kiện.

Rủi ro gian lận và thao túng thị trường

AI không được giám sát có thể bị lợi dụng để thực hiện các giao dịch gian lận hoặc thao túng thị trường chứng khoán. Vì Shadow AI hoạt động ngoài tầm quản lý của bộ phận quản lý công nghệ thông tin và bảo mật, tổ chức không thể theo dõi cách các công cụ này được sử dụng, dữ liệu nào được đưa vào, hoặc kết quả đầu ra có chính xác không. Nếu AI phân tích dữ liệu sai hoặc bị thao túng, có thể dẫn đến việc ra quyết định sai lầm dựa trên thông tin không đáng tin cậy, đặc biệt trong các lĩnh vực như dự báo tài chính hoặc quản lý rủi ro.

Ảnh hưởng đến danh tiếng tổ chức

Nếu một tổ chức tài chính sử dụng Shadow AI và gặp sự cố (lỗi thuật toán, rò rỉ dữ liệu, hay quyết định sai lầm), có thể ảnh hưởng nghiêm trọng đến uy tín và lòng tin của khách hàng. Khi khách hàng biết rằng, một tổ chức không kiểm soát tốt AI, họ có thể lo ngại về độ an toàn và chính xác của các dịch vụ do tổ chức cung cấp.

Tốn chi phí khắc phục sự cố

Khi Shadow AI gây ra sự cố, tổ chức phải chi nhiều tiền để khắc phục từ sửa lỗi hệ thống, điều tra vi phạm pháp lý đến bồi thường cho khách hàng. Việc thu hồi dữ liệu bị rò rỉ hoặc sửa chữa sai sót trong quyết định tài chính có thể cực kỳ tốn kém và mất thời gian.

Một số giải pháp giảm thiểu nguy cơ từ Shadow AI

Trong bối cảnh AI ngày càng phổ biến, Shadow AI đang trở thành mối lo ngại lớn. Nếu không được quản lý chặt chẽ, Shadow AI có thể tiềm ẩn nhiều rủi ro về bảo mật, tuân thủ pháp lý và tính minh bạch. Để giảm thiểu các nguy cơ này, cần quan tâm tới một số vấn đề sau:

Một là, xây dựng chính sách quản lý AI toàn diện. Triển khai thực hiện khung chính sách rõ ràng về việc sử dụng AI, xác định các công cụ được phép và các yêu cầu về tính bảo mật, minh bạch.

Hai là, đào tạo nhân viên tuân thủ quy định sử dụng AI. Tăng cường nhận thức của nhân viên về nguy cơ và hậu quả của việc sử dụng Shadow AI, đồng thời hướng dẫn họ cách tuân thủ các quy định pháp lý và chính sách nội bộ.

Ba là, triển khai hệ thống giám sát Shadow AI. Sử dụng các công cụ giám sát thông minh để phát hiện và quản lý các hoạt động sử dụng AI không chính thức trong tổ chức.

Bốn là, tích hợp AI được kiểm soát. Cung cấp các công cụ AI được phê duyệt chính thức để giảm thiểu nhu cầu sử dụng các giải pháp bên ngoài không an toàn.

*
* *

Shadow AI không còn là một vấn đề mới, mà đã trở thành một mối đe dọa thực sự đối với an ninh mạng và quản lý doanh nghiệp trong năm 2025. Với những rủi ro phức tạp và khó lường, từ sự lạm dụng trong nội bộ đến việc bị khai thác bởi tội phạm mạng, các tổ chức phải nhanh chóng cải thiện chiến lược bảo mật của mình. Điều này bao gồm việc tăng cường quản trị AI, giám sát nội bộ, đào tạo nâng cao nhận thức sử dụng AI an toàn trong tổ chức, doanh nghiệp để chống lại các mối nguy hiểm từ Shadow AI ✍

TÀI LIỆU THAM KHẢO

1. The Cyber Express (2025), "The Shadow AI threat looming over 2025: A wake-up call for enterprises", https://thecyberexpress.com/shadow-ai-in-2025-a-wake-up-call/, truy cập ngày 09/01/2025.

2. SC Media (2025), "Cybersecurity in 2025: Agentic AI to change enterprise security and business operations in year ahead", https://www.scworld.com/feature/ai-to-change-enterprise-security-and-business-operations-in-2025, truy cập ngày 09/01/2025.

3. IBM (2024), "What is shadow AI?", https://www.ibm.com/think/topics/shadow-ai, truy cập ngày 25/10/2024.

4. FedTech (2025), "Shadow AI: Shining light on a growing security threat", https://fedtechmagazine.com/article/2025/01/shadow-ai-a-growing-security-threat-perfcon, truy cập ngày 10/01/2025.

5. Axios (2025), "Shadow AI creates new headaches for company IT teams", https://www.axios.com/2025/02/04/shadow-ai-cybersecurity-enterprise-software-deepseek?utm_source=chatgpt.com, truy cập ngày 04/02/2025.