AIが“声”でだます時代へ…セールスフォース情報漏洩が突きつけたクラウド運用の盲点

23161095　大木絢楓

概要

- 2025年10月9日、世界中で多くの大手企業が利用するクラウドサービス「セールスフォース」を通じ、大規模な情報漏洩が発覚した。
- 「セールスフォース自体のシステムには脆弱性が確認されていない」ことから人の操作や判断を狙った“社会工学的攻撃”によって、内部から情報が抜かれた可能性が高い。

なぜ漏洩？

攻撃者は企業の従業員に対し担当者と偽り電話をかけ、

「システム更新のために一時的にアプリをインストールしてほしい」

「セキュリティ強化のための確認をお願いしたい」

→従業員が指示通りにアプリをダウンロードすると、それが偽装されたマルウェアであり、端末に保存されていたログイン情報や顧客データが外部へ送信された。

AIのリスク

- 従来のフィッシング詐欺といえば、メールやSMSによる偽サイト誘導が主流だったが、今は社内ミーティングの録音やオンラインセミナー動画などで簡単に“音声”を手に入れることができる。
- その声で電話をかければ、『あの人の声だから信頼できる』と従業員は疑わない。

  →人間の心理を狙った手法

- 多要素認証（MFA）
- ゼロトラストセキュリティ

(ゼロトラスト:すべてを信頼しない)

人は「見慣れたメール」「聞き慣れた声」「信頼する企業名」などに安心感を覚えるが、一人ひとりが「疑う力」を持つべきである。

コメント

- 電話は本当に脆弱だと思う。声だけだと信用できないからビデオ通話を利用することになったとしても、すぐに映像までもAIで偽造する世界になるだろう。
- 人間の脆弱性をつくボイスフィッシングを簡単に実行できるようにするAIが、野放図に提供されてしまっていることも、今回の問題の一因なのではないか。
- 音声はテキストよりも情報量が多い且つ、電話となると即時の判断が求められるため、冷静に見極めるのはさらに難しくなりそう。

感想

- 若者でも信じ込んでしまう精巧な作りに非常に危機感を感じた。
- SNSでも有名人の声を使った読み上げ機能が流行っているが、濫用し放題でもあると感じた。
- どれだけシステムを強化してもターゲットが人となればそれらは全く意味がなく、むしろ狙う側は容易になってしまうと思った。