AI の進化とセキュリティリスク

AI による新たなセキュリティリスク

音声合成技術を使った電話の本人の成りすまし
AI による画像や動画の加工
フェイクニュースによる情報操作 ...etc

以前から心配されておりましたが、残念ながら AI の音声合成技術を悪用した詐欺事件が発生してしまいました。
イギリスのある会社では、AI の合成音声による親会社の上役から、社長あてに本物そっくりの電話があり、緊急でハンガリーの取引先に 24 万ドル振り込んでしまったそうです。
そもそも、携帯電話とかは、本人似せた音声合成の声で会話しています。AI を使えば特定人物とそっくりの訛りや声の特徴で、本人に成り代わって会話ができることはすでにわかっており、本物かどうかは聞き分けることは無理だと言われておりました。これが、悪戯レベルでなく、実際の詐欺に使用され始めたのですから、私たちはどのように対策すればよいのでしょうか？ AI によるオレオレ詐欺が増えてくるのも時間の問題でしょうし、企業もメールや Web ページ対策だけでなく、電話への対応も必要です。その時、本人の電話なのかどうかはどのように聞き分ければよいのでしょうか？
ネット上では、フェイクニュースを仕分けする AI も活躍していますが、AI にフェイクニュースを作らせ発信させたら、誰が悪事を繰り返しているのかその元凶を見つけることが難しくなります。メディアでも、歪曲報道が氾濫していますが、何を基準にフェイクと判断するかは、誰がどのように規制するのでしょう？
こうなると、企業や団体を狙う悪意のある第三者は、AI を利用し、法律に触れないぎりぎりの方法で、あらゆる手を使って攻撃を仕掛けてきます。リモート勤務が可能なテレワークでは、実は、仕事をしていたのは AI のロボットの成りすましで産業スパイが紛れ込んでいたり、上司の命令通り仕事をしていたら、実は指示を出していたのは競合会社の AI だったということも十分あり得る世界になってきました。
そのため、ゼロトラストの考え方で、業務に関係のある作業はすべて指示があった段階から正式な承認や手順に従った指示に基づいているかどうかを疑わなければなりません。また、実行する人やロボットも、決められた者が決められた通りに行ったものかエビデンスを残す必要があります。そうなると、確認作業も煩雑になり、効率が悪いのですが、この辺りをどのような取り決めでどこまで行うかについても、セキュリティポリシーの決め方が重要になってきます。
技術の進歩により、以前では問題視していなかったレベルのリスクでも、定期的にリスクの見直しと、対応策の作成を実施する必要があります。そのためにも、IT 関係者はもちろん、全社員が常にセキュリティ事故や IT 技術の最新情報を入手し、IT リテラシーを高め、リスクに対応する感度を高めておくことが大切になります。