サイバーセキュリティ最前線

AIの悪用でサイバー攻撃が高度化!? セキュリティ技術の組み合わせで企業を守る!!

ChatGPTをはじめとした生成AI（大量のデータを学習し、文章や音楽、画像、映像などさまざまな形式のデータを作成する人工知能）の台頭や普及によって、2023年は日本でもAIへの関心が一段と高まった。が、一方で多くのサイバーセキュリティの専門家たちがAIの悪用を懸念している。そこで、今号ではそうした懸念に対応する㈱ブロードがオススメするセキュリティソリューションを紹介したい。

懸念されるAIの悪影響

サイバーセキュリティの専門家たちが懸念するAIの悪影響を大別すると、①攻撃側の高度化②ユーザー側のシステム上の脆弱性の増加のふたつになる。まず①については、フィッシングメールや詐欺メールの内容がAIの悪用でよりリアルになり、攻撃か否かの判断が難しくなると指摘されている。AIを用いて作成されるディープフェイク（リアルな映像や音声）が悪用される可能性もあり、生体的認証の見直しも必要になるかもしれない。また、AIがランサムウェア（身代金ウイルス）やマルウェア（悪意のあるソフトウエア）の操作など全体を制御するケースも危惧されている。

一方、②については、システムやソフトウェアの脆弱性（セキュリティ面での欠陥）が増す可能性が指摘されている。実際、米国のスタンフォード大学の研究者チームがプログラミングを行う際にAIを利用したグループとそうでないグループとの比較テストを実施したところ、前者のほうが慢心からより多くの脆弱性を生み出してしまったという。こうしたなか、多くの企業がAIによるランサムウェアの増加に不安を覚えている。警察庁によると2023年上半期のランサムウェアによる国内の被害件数は103件。なかには名古屋港がシステム障害により、トレーラーへのコンテナ積み込みなどの業務を何日も停止せざるを得ない状況に陥るといった大規模な事案もあった。ちなみに、こうした事案に個人情報の流出が重なると、調査や対応などにさらに時間を要することになる。たとえば、顧客情報含む個人データ約186万件の流出懸念が報じられた大手文具メーカーの場合、攻撃者の侵入経路や被害規模、流出懸念などの調査結果を公表するまでに約2カ月を要している。

サイバー脅威に対抗

長年、ITセキュリティに取り組む㈱ブロード（東京都千代田区）は、まずランサムウェアやマルウェアの対策として「HP SCE」（HP社）の導入をあげる。「このソリューションを導入すれば、パソコン上の『仮想のパソコン』でオフィス文書やウェブページを開くことができるようになるため、パソコン本体（エンドポイント）の安全性を高いレベルで維持することができる」と胸を張る。

さらに今年から提供をはじめた「Continuity Engine」（NeverFail社）を加えることで、さらに万全の体制を構築可能だという。「このソリューションはクローニング技術を活用したもので、ランサムウェアの影響やセキュリティパッチの適用、ハードウェア障害などに起因するサーバーのアプリケーションの利用可能時間を99・999%まで向上できる。小規模なシステムにも導入可能なので、中小企業にもオススメだ」そうだ。

そして、外部からの「不正アクセス」への対策については「さらに踏み込んだ『侵入テスト』（専門家が模擬攻撃で実際の侵入を試み、侵害経路を見出す方法）が必要」と指摘。これを完全自動化して実施できる「Ridge Bot」（Ridge Security社）がイチオシだ、とブロードの担当者は話す。「AIを活用して高いレベルの侵入テストを自動で繰り返し実施することで、ネットワーク内の弱点を継続的に監視できるようになる」という。

世界中の先進的なセキュリティ技術と情報を持つブロードからのアドバイスをぜひとも参考にしてほしい。