サイバーセキュリティ最前線

サイバーセキュリティ担当者必見!!

プロが注意喚起する2024年のハイレベルなサイバー攻撃!!

年を追うごとに複雑化するサイバーセキュリティ分野。そこで、今号では2024年のトレンドを予測しつつ、㈱ブロード（東京都千代田区）に最適なソリューションをいくつか紹介してもらった。

複雑化するサイバーリスク

まず想定されるのがAIの影響だ。具体的には、多くの専門家がフィッシング（詐欺）メールの洗練化や防御・検知システムの回避、攻撃の大規模化などを懸念している。また、AIの悪用でゼロデイ脆弱性攻撃が増加するとの予測も。ゼロデイ脆弱性とは製品メーカーなどが認識しておらず、修正プログラムなどが存在しない状態のこと。この発見と悪用には高度な知識が必要だが、AIの進歩によって今後は一般のサイバー犯罪グループがあらたな脆弱性を検知して悪用するようになるかもしれない。ついで、想定されるのがIT関連の技術・サービスの進化による影響だ。たとえば、インターネットブラウザで利用可能な「ウェブアプリケーション」が増えることで、攻撃者にとってはログインに必要なアカウント情報（一般的にはIDとパスワード）がますます重要なターゲットになるだろう。また、接続端子の規格がType-Cに統一される動きが加速しているが、これは利便性が高まる一方で攻撃者側のハードルを下げることにつながる。具体的には空港などの公共の場で提供される充電用接続からデータを詐取する手口（ジュースジャッキング）がより容易に行われるようになるかもしれない。

また、2024年においても世界的なサイバー攻撃グループの動向に注意しなければならない。事実、内閣サイバーセキュリティセンター（NISC）はこのほど、米国家安全保障局（NSA）、米連邦捜査局（FBI）、米国土安全保障省サイバーセキュリティ・インフラ庁（CISA）とともに、中国を中心としたサイバー攻撃グループ「BlackTech（ブラックテック）」によるサイバー攻撃に関する合同の注意喚起を発出。BlackTechは10年頃から日本を含む東アジアと米国の政府、産業、技術、メディア、エレクトロニクス、電気通信分野を標的として活動するサイバー攻撃グループであり、今回の注意喚起では①セキュリティパッチ管理の適切な実施②端末の保護（いわゆるエンドポイント・プロテクション等）③ソフトウェア等の適切な管理・運用、ネットワーク・セグメンテーション④本人認証の強化、多要素認証の実装⑤アカウント等の権限の適切な管理・運用⑥侵害の継続的な監視⑦インシデント対応計画、システム復旧計画の作成等⑧ゼロトラストモデルに基づく対策が重要であると強調されている。

柔軟かつ適切な対応を

この注意喚起を踏まえ、実際にどのような対策が有効か、長年にわたってITセキュリティに取り組む㈱ブロード（東京都千代田区）に聞いてみた。まず、①については「企業の大小にかかわらずRidge Security社製のRidgeBotを提案したい。これを使えば脆弱性管理よりもハイレベルな『侵入テスト』を自動で継続的に実施できる。結果、脆弱性の検知はもちろん、脆弱性を踏み台にして別の侵害ポイントを探し出すための模擬攻撃を最新のAI技術で自動的かつ継続的に行い、対策が必要な箇所を特定することができる」と。また、②に関しては「パソコン上で稼働する『仮想のパソコン』でファイルやウェブサイトを開くことにより万全な保護を実現できる『HP SCE』がイチオシ」とのこと。さらに⑤に関しては「BeyondTrust社製の特権管理ソリューションを中心に適切な対応をすすめれば、リスクを大幅に低減できる」という。このほかにもブロードは多様なソリューションを有しているので、新年を迎えるにあたって相談してみるといいかもしれない。