エグゼクティブサマリー：2022年脆弱性インテリジェンスレポート：状況は改善しつつも高まる複雑性

サイバー脅威を取り巻く環境は5年前とは根本的に異なり、蔓延する複雑で多様なサイバー犯罪エコシステムが、グローバル企業を餌食にして利益を上げる世界になっています。ランサムウェアグループや初期アクセスブローカーが、サイバー犯罪経済に拍車をかけているボットネットオペレーターと国家が支援する脅威アクターらの仲間入りを果たしています。その手口と標的対象は幅広く、事業規模や業種に関係なく、事実上あらゆる組織に影響を与えています。

進化を続けるサイバー脅威

- 2021年は、サイバー脅威の発生頻度および規模が史上最大となり、平均で11日ごとに大規模なエクスプロイトイベントが発生しました。2022年になると、ゼロデイエクスプロイトと大量エクスプロイトの「アウトブレイク」がわずかに低減しましたが、攻撃の速度と規模の上昇という、複数年にわたる傾向は変わりません。
- サイバー犯罪のビジネスモデルと攻撃者の行動が進化する中、前年と比べて全体的な傾向がわずかに変化し続けると予想されます。こうした変動からは、敵対者とその動機に関して微妙な違いが読み取れます。しかし、グローバル企業のリスク環境が持続的に緩和されることはほとんどありません。

セキュリティ脅威がセキュリティ運用チームの上手を取るケースも

- 新しい脆弱性が発見されてから攻撃に利用されるまでの期間は引き続き短縮される傾向にあり、2022年には、当社レポートに記載の脆弱性の56%が発見から7日以内に悪用され、広範囲にわたる攻撃の40%以上がゼロデイエクスプロイトから始まっています。この結果は、セキュリティチームが新しい脆弱性にパッチを適用するまでの時間が短くなっている、もしくは全くないということを意味し、すでにキャパシティオーバーな状態にあるセキュリティリソースにさらに大きな負担がかかっていることがわかります。
- 慎重な緊急パッチ適用や、堅牢なインシデント対応に向けた手続きを用意するのは有益ではありますが、日々必要なリソースの確保にすら苦労しているセキュリティチームに、さらに強力な緊急手順の実施を期待するのは無理な話です。効果的な侵害対応を実施する以前に、プロアクティブな資産管理、あるいは脆弱性管理など、基本的なセキュリティプログラムを強固にしておく必要があります。

テクノロジーの効果的な活用には専門知識が必要

- クラウドの導入が拡大し、利用する製品や技術が複雑になるにつれ、攻撃可能領域（Attack Surface）も拡大し、攻撃者が企業ネットワークを侵害する方法も増えます。セキュリティ対策製品は、組織のセキュリティに必要な要素ですが、昨今のサイバー脅威に対抗するには、クラウドとオンプレミ

スで可視性と保護を提供する製品群だけではなく、人間の持つ専門知識が重要となります。各企業の経営者たちは、技術的な製品をもってしか複雑な攻撃に対応できない、という思い込みから一度離れて、高いモチベーションによって行われる攻撃を検知し、阻止するためには何が必要かを考え直す必要があります。

エグゼクティブへのアドバイス

- 昨今の脅威状況では、セキュリティチームが攻撃の後手に回り、リアクティブな対応を余儀なくされており、それがセキュリティ対策の有効性と持続可能性の低下を招く要因となっています。企業をリードする役員やエグゼクティブたちは、セキュリティ対策の課題を可視化するとともに、それが破られた時に想定されるインパクトを想定することで、事業に役立てることができます。
- 2022年から2023年にかけての厳しいマクロ経済状況は、機密データや事業運営の整合性を損なわずに効率を高めようとするリスク管理チームに、さらなるプレッシャーを与えることになりました。特にマクロ経済が不安定な場合、リソースに制約がかかるため、結果として隠れたリスクの増加や、緊急インシデント対応能力を含む効果的なセキュリティ運用に必要な技術的専門知識の喪失につながる可能性があります。
- 役員やエグゼクティブは、広がり続けるセキュリティ脅威の持つ性質と、自社が高度な攻撃とよくある低レベルな攻撃の両方に狙われている事実を認識しなければなりません。セキュリティの評価指標および企業のリスクモデルは、ビジネス的な視点を取り入れ、より広域な戦略的な計画に組み込まれていくべきです。担当部門だけがセキュリティに責任を負うのではなく、企業全体で取り組むことが理想です。
- 受容可能なリスクとは、明確化されたリスクであるべきです。役員やエグゼクティブは、セキュリティ対策のリソースの制約と現実の脅威環境が、知的財産の機密性、機密データとサプライチェーンの完全性などの事業運営の継続性にどのように影響するかについて、完全に理解した上で、社内にその情報を共有する必要があります。リスクが経営層が、リスクの意味合いを理解し、明治化している限りにおいて、ビジネス上の意思決定でそのリスクを受け入れるのは理にかなっていると言えます。

Rapid7の2022年脆弱性インテリジェンスレポートの全文を入手（英語）

レポートをダウンロード