特集

サイバー攻撃に対する新しい概念「サイバーレジリエンス」に注目!

綜合警備保障株式会社

Web版ではより詳しい内容がご覧いただけます
ユーザ協会 D10050

ますます高度化・巧妙化するサイバー攻撃に対処するために、攻撃を受けることを前提とした上で、被害を最小限に抑え迅速な事業回復の実現を目指す「サイバーレジリエンス」が注目されています。綜合警備保障株式会社 商品サービス戦略部で、主に中小企業のセキュリティ対策を担当する竹内 祥氏に、「サイバーレジリエンス」の考え方や実践方法についてうかがいました。

商品サービス戦略部
情報セキュリティサービス推進室 課長代理
竹内 祥氏

1IPに対して1日9,000超のサイバー攻撃を観測

企業を標的にしたサイバー攻撃が活発化しています。警察庁サイバー警察局は、2024年上半期に報告されたランサムウェア※1の被害件数は114件あり、そのうち中小企業の被害が73件に及んだと発表しています。被害報告件数は対2021年度比で約2倍弱に増え、現在も高水準で推移しています。また2024年6月には出版大手企業のサーバーが攻撃を受け、提供する動画配信サービスなどの一時停止を余儀なくされ、大きな話題になりました。

このような現状を竹内氏は、アンチウイルスソフトなどで攻撃を「防御」する従来の手段だけでは、対策が困難な時代が到来したと分析しています。

「サイバー空間では、攻撃者が圧倒的に有利な立場にいます。警察庁は2023年にサイバー攻撃を受けた1件のIPアドレスに対し、1日あたり平均約9,145回のサイバー攻撃を観測したと発表しました。どの企業のシステムも、毎日全世界から9,000回を超えるサイバー攻撃を受ける可能性があるということになります。攻撃数は対2015年比で約12.5倍に増大しました(図1参照)。また、2022年にランサムウェア被害を被った企業の87%がアンチウイルスソフトを導入していましたが、その内92%のソフトがランサムウェアを検出できず、無防備状態で汚染されたと言います」(竹内氏)

サイバーレジリエンスで被害を最小限に抑え込む

従来の「防御」中心のセキュリティシステムが、高度化したサイバー脅威に十分に対応できなくなった昨今、「サイバーレジリエンス」が注目されています。

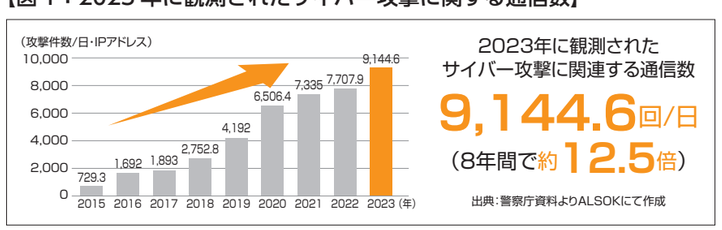
「サイバーレジリエンスは、『サイバー攻撃は避けられない』を前提に成立している考え方で、『発生した被害を最小限に抑え、迅速に回復する組織の能力』を意味します。攻撃を受けた後の対策や復旧に重点が置かれ、サイバーレジリエンス能力を高めることで、企業の耐攻撃力や事業継続力の向上に貢献すると期待されています」(竹内氏)

サイバーレジリエンス能力を高めるために、竹内氏は四点のセキュリティ対策の実践(図2参照)を提唱しています。第一に「情報資産の洗い出しとリスク評価」の確認です。会社が所有するさまざまな情報資産が、どこにどのような状態で保存されているかを洗い出し、それぞれのリスクを評価した上で、守るべき優先順位をつけ、関係者間で共有します。有事の際に速やかな対応で被害を最小限に抑える、サイバーレジリエンスの第一歩になります。

そして優先順位の高い情報資産から、「基本的なセキュリティ対策」として技術的対策、組織的対策、物理的対策を施します。技術的対策とはアンチウイルスソフトなどの導入、組織的対策とは資産情報の保存ルールを作る、意識向上のための研修を実施するなど、有事に対応したルール作りや体制の整備を意味します。物理的対策例は、ファイルサーバー※2を収納するラックの施錠や、サーバールームの出入り管理の強化などが挙げられます。

「そして最も重要なポイントが、3・2・1ルールによる『重要なデータのバックアップ』です。このルールは、『少なくとも三つのバックアップを作成する』『二つの別のメディアに保存する』、そして『一つのバックアップをオフラインで保管する』という、データ保存に関する基本的な考えです。さらに定期的なバックアップを行うことで、脅威から情報資産を保護し、短時間での復旧を可能にします。特に外付けのハードディスクなど、オフラインのメディアへの保存は欠かせません。ランサムウェアに感染すると、同じネットワーク上にあるメディアに感染が及び、すべてのバックアップが暗号化されてしまう危険性があるからです。また『インシデント※3対応計画の策定』も必須です。有事の際の対応手順書を必ず準備しましょう。対応チームの責任分担や権限を明確にするほか、顧客などへの連絡手順の設定や業務継続のための代替措置など、有事の際に予想される業務マニュアルも、文書化しておくことでより柔軟な対応に結びつきます」(竹内氏)

【図 1：2023 年に観測されたサイバー攻撃に関する通信数】



【図 2：サイバーレジリエンスの考え方に基づくセキュリティ対策】

情報資産の洗い出しとリスク評価
- 守るべき情報資産を洗い出し、どこに保存されているかを洗い出す
- 洗い出した情報資産それぞれのリスクを評価する

基本的なセキュリティ対策の実施
- リスク評価の結果を踏まえて、優先順位をつけて対策を実施する(技術的対策、組織的対策、物理的対策)

重要なデータのバックアップ
- 重要なデータはバックアップをとる(3・2・1ルール)
- 万が一に備えて、復旧手順を用意する

インシデント対応計画の策定
- インシデント対応の復旧手順を文書化する(インシデントの検知方法、対応チームの役割と責任、外部関係者〈法執行機関、顧客、メディアなど〉との連絡手順を含めます。業務継続のための代替措置も盛り込む)

「まず、サイバーセキュリティを経営課題として認識し、会社をあげて取り組む体制作りが大切です。経営層の中にはセキュリティ問題をコスト課題として捉え、対策ソフトなどの導入に消極的な例がよく見られます。しかし経営層と現場の距離が近く、会社の意思や決定が大企業と比べて伝わりやすい中小企業は、経営層の意識次第で『サイバーレジリエンス』が効率よく進捗しますので、ぜひ三つの取り組みを検討してください。

一つ目の取り組みは『アウトソース』の積極活用です。中小企業では、数少ないデジタル人材に企業のICT業務全般が集中する『一人情シス』状況が増えているため、アウトソーシングをはじめ、IT資産管理ツールや、AIを採用し自動復旧機能を持つセキュリティ対策ツールなどの導入が推奨されます。

二つ目は、危機管理チームを編成し『体制整備と教育・訓練』を進めることです。メンバーの役割分担と権限を社内に周知し、社員の危機管理意識を育成する研修なども行います。こうした積み重ねにより、社員が不審に気づいた際の連絡などがスムーズに行われ、速やかな初期対応が実現します。

三つ目はOS、アプリケーションは常に最新の状態に保ち、業務に関係のないソフトはインストールしない、Webも閲覧しないなど、従来の基本的な『健全なシステム』の維持です。

この20年で企業のIT環境は大きく変わりましたが、実は攻撃の手口に大きな変化は見られません。ランサムウェアの登場は2014年であり、フィッシングは2005年には確認されています。サイバー攻撃の被害は増加していますが、従来の基本的なセキュリティが多くの攻撃を防いでいるのも事実です。そのため、このような基本的な対策が重要になります」(竹内氏)

竹内氏の解説の通り、基本的な対策を徹底するだけでもサイバーレジリエンスを強化することは可能です。まずは、この基本的な対策がしっかりできているか、見直すことから始めましょう。

※1 ランサムウェア:パソコンやスマートフォンをウイルスに感染させて、保存されているファイルなどのデータを勝手に暗号化することで使用できない状態にした後、それを元に戻すことと引き換えに身代金を要求する不正プログラム。

※2 ファイルサーバー:ネットワークの仕組みを利用して、社内などでデータを管理共有するためのサーバー。

※3 インシデント:事象・出来事・事故などの意味を持つ英単語"incident"から、情報セキュリティの分野では、情報の漏えいや消失、情報システムの機能停止またはこれらにつながる可能性のある事象などのこと。

ALSOK

●会社概要
会　社　名:綜合警備保障株式会社
設　　立:1965年(昭和40年)7月16日
本社所在地:東京都港区元赤坂1-6-6
代表取締役:グループCEO兼CTO(最高技術責任者)村井 豪
代表取締役:グループCOO 社長執行役員 栢木 伊久二
事業内容:機械警備、常駐警備などのセキュリティ事業、綜合管理・防災事業、介護事業、セキュリティソリューション事業、情報警備事業など
URL:https://www.alsok.co.jp/

関連記事もWebで!
「中小企業の情報セキュリティ対策」
ユーザ協会 中小企業セキュリティ