働き方再考（第17回）

多様な働き方に安心を！エンドポイントセキュリティ強化のコツ

2024.01.22

コロナ禍でテレワークなどが導入されたことで、私たちの働き方は大きく変わった。感染拡大が収束した今ではクラウド環境でオフィスワークとテレワークを併用するハイブリッドワークも普及しつつある。いわば「働き方のいいとこどり」が可能となり、それ自体が企業の競争力強化につながっている。しかし、落とし穴もある。どこでも業務が遂行できるようになった反面、エンドポイントの拡大によるセキュリティリスクの高まりだ。規模の小さな企業もその例外ではない。

ビジネス的にも社会的にも求められるセキュリティの強化

企業のシステムを狙うサイバー攻撃はますます巧妙になり、高度化している。攻撃者はセキュリティ対策が脆弱なところに攻撃をかけ、効率良く成果を挙げようとしている。特に狙われているのがサプライチェーンの構成員でもある中小企業だということはご存じだろうか。

サプライチェーンでは企業同士が円滑に取引するために、ネットワークでつながっている。中心的な役割を果たしているのは大企業だが、大企業はしっかりしたセキュリティ対策を講じてる場合が多く攻撃者が攻撃を成功させるには時間も手間もかかる。そこでネットワークにつながっているセキュリティの脆弱な可能性の高い中小企業を狙っているのだ。

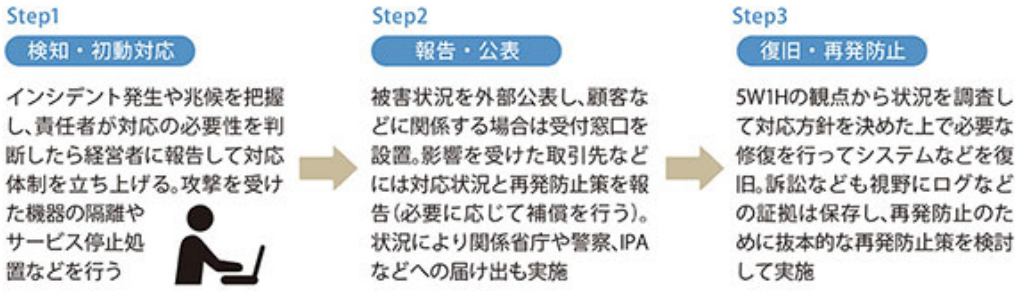
攻撃者はまず中小企業のシステムに侵入してIDやパスワードを盗み出し、不正なプログラムを送り込んで攻撃を広げる。近年流行しているランサムウエア攻撃でも同様の手口が使われている。実際にサプライチェーン経由でランサムウエア攻撃を受けて、事業がストップして被害を受けたケースが発生している。

取引先に迷惑をかけないというサプライチェーンの構成員としての責任を果たすために、中小企業にもセキュリティ対策の強化が求められているのである。

インシデント対応に求められる仕組みや体制をどう用意するのか

サイバーセキュリティの重要性への認識が広がる中で、ネットワークの出入り口で不正なアクセスやウイルスをブロックするUTMを導入している場合もあるかもしれない。しかし、どんな対策を講じていても100％防御することは不可能だと言われている今、求められているセキュリティ対策としてはそれだけでは不十分だ。

●インシデント対応の基本ステップ



本媒体の別の記事でもご紹介しているが、サイバー攻撃を受けたことに対応するためのプロセスは検知に始まる。まず異常の発生を検知し、それがインシデントかどうかを判断する能力が必要になる。次にインシデントに対応した適切な対策が求められる。不正なプログラムに感染した端末を特定し、被害の拡大を防ぐためにネットワークから切り離すなど具体的な対応をとる。

さらに重要になるのは、事象から原因を追求するとともに、影響範囲を特定するなど被害状況を把握し、関係する取引先などに通知を行う。その上で今後同様のインシデントが発生しないように防止策を講じて、端末やサーバー、ネットワークなどを復旧させ、必要に応じて一連のインシデントの情報を公開して報告するところまでが求められる。

こうしたインシデント対応を実現するためにはさまざまな要素が求められる。不正を検知する仕組みはもちろん、原因追跡や被害の可視化、システム復旧のための仕組みと手順など事前の対策が必要だ。そして集めた情報を分析して判断できる人材や体制がなくては、具体的な対策を講じることも、関係者への通知や報告もできない。

企業規模が小さく、専任のIT管理者がいない中小企業では対応できないと考えるのは当然だろう。しかし、一定規模の取引先企業に対して一連のインシデントレスポンスの体制を要求する企業も増えてきている。そこで注目されているのがエンドポイントの検知と対応のソリューションである「EDR（Endpoint Detection and Response）」の導入だ。

ただ、EDRを自社で運用するにもスキルやノウハウは必要になる。そこでお勧めしたいのが外部のEDRありのサポートサービスの活用だ。24時間365日体制でプロがシステムやネットワークを監視し、インシデント対応まで請け負ってくれる。安心してビジネスに打ち込むためにぜひ検討してみてはどうだろうか。