セキュリティリスクの拡大による対応の変化

サイバー攻撃に対する100%の「防御」は不可能であるとの認識が広がり、セキュリティ対応の重心は「検知/対応/復旧」へ移動している。
セキュリティ対応の高度化と複雑化から、複数のセキュリティ製品/サービスを組み合わせて統合的なセキュリティ対応を行うことが求められるが、情報システム部門がそれを自営することは限界を迎えつつある。
そのため、ITベンダーによるマネージドサービスやクラウドを活用したセキュリティ対応へと変化が始まっている。

背景と現在の状況

クラウド/コンシューマITなどの活用は企業内に浸透しつつあり、これらの活用を考慮した新たなセキュリティ対応が必要になっている。IoTの普及により、ネットワークに接続された各種センサーなどの数や種類が増えるにつれ、潜在的なサイバー脅威も増加し、物理インフラとネットワークインフラの統合セキュリティが必要となっている。
海外からの標的型攻撃やDDos攻撃などによる重要インフラを中心としたセキュリティリスクが増加することが懸念されている。外部からの攻撃だけでなく、社員や協力企業の要員による内部からの情報漏洩事故の発生事例を受け、監視や防止のしくみ作りが行われつつある。
法制面では、我が国のサイバーセキュリティに関する基本理念を定めた「サイバーセキュリティ基本法」が全面施行された(2015年1月)。経済産業省は「サイバーセキュリティ経営ガイドライン」を策定し(2015年12月)、セキュリティへの経営層の関与を強く求めた。企業は監督官庁からのセキュリティ強化指示の対応に追われている。

3～5年後の姿

2020年に向けてサイバー攻撃のリスクが高まると共に、IoTの普及が進み様々なデバイスへのハッキングが行われている。セキュリティ対応は「防御」から「検知/対応/復旧」へ重心が移動している。セキュリティ対応の高度化と複雑化から、複数のセキュリティ製品/サービスを組み合わせて統合的なセキュリティ対応を行うことが求められるが、情報システム部門がそれを自営することは限界を迎えつつある。そのため、ITベンダーによるマネージドサービスやクラウドを活用したセキュリティ対応へと変化させた企業が出ている。

「防御」から「検知/対応/復旧」へ重心が移動

2015年に金融庁/総務省/経済産業省などからセキュリティインシデントに対応するため、CSIRT[1]などの体制整備が求められた。これをきっかけに企業の多くはCSIRTを立ち上げたものの、技術力とセキュリティ対策投資を伴わず、3～5年後には形ばかりの体制になっている企業が多くなっている。

セキュリティ対策投資が進まない一因として、サイバー攻撃が見えないことが挙げられる。サイバー攻撃を可視化し、経営層にセキュリティ対策の必要性を認識させるためにセキュリティベンダーの監視サービスと自社での監視機能をハイブリッドで融合した、より高度なインシデント検出機能が大手企業を中心に展開され始めている。

セキュリティに敏感な経営層をもつ企業はセキュリティリスクを経営リスクと位置付け、経営を守る観点から事業継続計画(BCP)のなかで、セキュリティ対策を災害復旧(DR)と統合的に計画/管理している。ビジネスへの影響の大きさに応じて、対応に必要な投資の優先順位を決め、巧妙化するとともに執拗なサイバー攻撃に対する100%の「防御」は不可能であると認識して、「検知/対応/復旧」に重心を置いたセキュリティ対策を行うよう指示している経営層が増え始めている。
セキュリティの事後対策の充実に向けては、企業内のセキュリティ専門人材の育成が必要となる。この人材に投資できるかが中長期の企業セキュリティ戦略の推進に大きな影響をもたらしている。

IoTの普及に対応する新たなセキュリティ対策

スマートビルやスマートハウスなどのインターネットに接続されたデバイスを多数使用したシステムへのハッキングが行われ被害が発生している。IoTの普及により、ネットワークに接続されたデバイスの数と種類は膨大なものになり、保護対象の管理は困難になっている。大量のデバイスから発生する膨大なデータの処理を高速化するため、エッジコンピューティングによる分散処理が進み、防御のための境界が拡大している。また、ビッグデータの組み合わせ分析やマッチング技術の進化に伴い、個人情報やプライバシー保護の課題が顕在化している。

これらのことから、従来のセキュリティ対策では対応が困難であり、デバイスを接続するネットワークとセキュリティを一体で設計する動きが始まっている。例えば、デバイスとエッジサーバ間の通信の認証/暗号化/盗聴と改ざん防止のしくみ作りや、基幹系システムのネットワークとIoT系のネットワークを分離したオーバレイネットワークの構築などである。また、プライバシー保護のため、匿名加工技術と匿名加工情報の利活用のしくみ作りが行われている。

マネージドセキュリティサービスやクラウドの活用

事業部門主体のIT駆動型ビジネスの拡大や、クラウド/モバイル/IoTなどのビジネスへの活用が広がることにより、拡張を繰り返したシステム全体のグランドデザインの見直しが必要になっている。また、多くの企業が2000年代前半に策定した情報セキュリティポリシーは、この様なビジネスの変化に追従できておらず、大幅な見直しが必要になっている。

セキュリティ対策の高度化と複雑化が進み、企業の情報システム部門自らが複数のセキュリティ製品/サービスを組み合わせて統合的なセキュリティ対策を自営することは限界を迎えつつある。自社で対応する範囲と外部に委託する範囲の再整理を行い、ITベンダーによるコンサルティング/マネージドセキュリティサービス/アウトソーシングや、クラウドを活用したセキュリティ対策へと変化させた企業が出ている。

オンプレミスより複数のセキュリティ標準の認証を受けているクラウドの方が、よりセキュアなシステムの構築/運用が可能であるという考えが広がり、セキュリティ対策が自営できないことを理由としたクラウドへのシフトが始まっている。オンプレミス上の自社開発アプリケーションやパッケージからSaaSへのシフト、PaaS/IaaS上での開発/運用へのシフト、およびSaaS型セキュリティサービスの活用が行われている。このとき、多様なセキュリティ対策をオンプレミスとクラウドに適正配置することに加え、オンプレミスとクラウドを一体としてセキュリティを確保するためのネットワーク仮想化技術や統合運用のアーキテクチャの必要性が認識され始めている。

ITベンダーから提供されるマネージドセキュリティサービスやクラウドなどを活用することにより、セキュリティ製品/サービスの評価/導入/監視/運用などは、一部の企業では情報システム部門の役割では無くなっている。役割の中心は、企画フェーズではセキュリティポリシーの策定、保護するべき情報資産の棚卸/アクセス権限の整理/優先順位付けの合意形成などになる。計画立案フェーズでは、セキュリティ対策の必要性を経営層と事業部門に伝え、対策レベルの合意形成とそれを実現するための予算の獲得、優先順位に応じた対策実施スケジュールの策定などになる。実行フェーズでは、内部対策の実施、インシデント発生時の事業部門との調整と経営層に対するビジネスへの影響報告などになっている。

セキュリティ対策を確実に実施している企業がある一方で、入口対策だけなど最低限のセキュリティ対策に留まっている企業もある。これらの企業は社会的な評価の失墜やブランド価値や市場での競争力低下のリスクを抱えている。

AI同士の戦い

全てのビジネスでAIの活用が広がっているなかで、セキュリティ分野においてもAIによるサイバー攻撃の検知が進んでいる。多数の攻撃を学習させることで、パターン認識の精度を上げ、未知のウィルスによる攻撃の検知が実用化され、多くの企業で使われている。
AIによる処理は検知のみではなく、侵入後の封じ込め対応もAIが行っている。侵入を検知すると、関係すると思われる不正な通信を自動的に遮断するとともに、感染したサーバなどを自動的に隔離している。
攻撃にもAIが用いられている。攻撃側は、AIにより防御されていることを前提として、その裏を突く攻撃やウィルスであることの偽装をAIにより実装している。その結果、AI同士の攻防が繰り広げられている。AIの優劣がセキュリティ対応の重要な差別化要因になっているため、セキュリティ製品ベンダーはAIの能力向上に力を入れている。

[1] 企業内に設置するコンピュータセキュリティの専門チーム
(Computer Security Incident Response Team)