企業がサイバー攻撃に対するレジリエンス強化のためにすべきこと

DXC Technology、マーク・ヒューズ

企業にはサイバーレジリエンス、つまり進化する脅威を前にして、攻撃に耐え、運用を継続し、新しいテクノロジーを活用できる能力が必要です。

多くの出来事によって記憶に残る年となるであろう2020年は、サイバーセキュリティの領域においてはデータ侵害の年でした。

新型コロナウイルス (COVID-19) が世界中に広がり、何千万人もの人々がリモートワークを余儀なくされた一方で、多くのハッカーや国家レベルの攻撃者達は、隙があればこれまで以上に高度な攻撃を組織的に行いました。

これらの動きが重なり合う中で、企業や組織へのセキュリティ侵害はもはや「もし経験したら」ではなく「いつ経験するか」という問題になりました。

文化的変化

DXCはこの進化する脅威への対応を必要とするお客様を支援していますが、セキュリティが単なるテクノロジーの問題ではないことを認識する企業が増えています。セキュリティはビジネスにとっても、さらには取締役会にとっても重要な課題です。Cybersecurity Ventures社は、2025年までに全世界の企業に対するサイバー犯罪による被害額は年間10.5兆ドルとなり、ブランドの評判、顧客との信頼関係、規制順守、事業運営に影響を与えると指摘しています。

単にセキュリティを意識したり、防御策のみの戦略を策定したりするだけではもはや不十分です。企業にはサイバーレジリエンス、つまり進化する脅威を前にして、攻撃に耐え、運用を継続し、新しいテクノロジーを活用できる能力が必要です。これは、重要資産の保護、侵害の検出、インシデント対応の間でバランスに優れたポリシーとプロセスを確立する必要があるということです。

明確で総合的な戦略の策定

レジリエンスとは、すべての攻撃を防御できるという意味ではなく、セキュリティを侵害された場合に、すぐに被害から回復して機能を継続できる体制を構築することを意味します。

すべての企業が、さまざまなシステムやビジネス領域における目標、優先順位、およびリスク許容度に基づいて、レジリエンスが自社にとってどのような意味を持つのかを定義する必要があります。企業は、特定の問題を解決するのではなく、レジリエンスが組み込まれた枠組みを確立することによって、セキュリティ対策の導入、発展、変革を可能にする必要があります。

情報資産を保護するには、資産の詳細やその所在を把握していなければなりません。企業がレジリエンスを実現するには、テクノロジーインベントリを実施し、重要なアプリケーションの依存関係と脆弱性を洗い出して、これらの情報をリカバリ計画に組み込んでターゲットを再構築する必要があります。インフラストラクチャについて把握することで、すぐに実行可能な対応計画を明確化することが可能になり、インシデントから低コストで回復できるようになります。

次のステップは、インシデント対応計画を実行に移してリハーサルを実施することです。複数拠点に影響を与えるランサムウェア攻撃などの不測の事態や、インターネット接続なしで危機管理を実行する必要性に備えて、事業継続性を確保するための連絡方法と指揮系統を定義します。

企業内のすべてを完全に保護することはできませんが、多くの重要なデジタル資産とそれら資産間の相互関係に重点を置いた戦略的な対策を行うことで、従業員の所在や使用するデバイスに関係なく、データをプロアクティブに保護し、アクセスを制御できます。

レジリエンスは、すべての攻撃を防御できるという意味ではなく、セキュリティを侵害された場合に、すぐに被害から回復して機能を継続できる体制を構築することを意味します。

明確なガバナンスの確立

優れたインシデント対応計画では、インシデントが発生したの際のさまざまな行動の責任者が明確に定義され、対応のすべての手順とベストプラクティスが定められています。責任者が明確でなければ、誰も実行方法がわからない対応計画になりかねません。

事業継続性を確保し、規制上の義務を順守するためにはすばやい行動が求められるため、インシデント対応戦略では迅速なエスカレーションと対応を可能にする必要があります。これはつまり、経営陣や取締役会が確実に対応戦略を理解する必要があるとともに、パートナー、法務チーム、インシデント対応部門、司法当局など、必要な第三者に事前に協力を求める必要もあるということです。

サイバーレジリエントな文化の醸成

プロセスと管理戦略を策定するだけではレジリエンスを実現することはできません。組織のレジリエンスを実現するのは、資産とデータに関わる人たちです。

業務担当者からIT担当者、経営幹部に至るまで、すべての従業員がサイバーレジリエンスの考え方を理解する必要があります。これは自分自身が脅威を防衛する最前線であることを認識することから始まります。また、継続的なセキュリティ認識トレーニングで組織文化を強化します。たとえば、ゲームの手法を応用して、セキュリティポリシーの影響を従業員に体験させ、誤ったら処罰するのではなく、正しい行動に対して報酬を提供します。

ゼロトラストの考え方を導入

セキュリティ業界は急速に進化するサイバー脅威を常に追いかけています。

セキュリティ管理が強化されるにつれて、攻撃者は新たな攻撃戦略で今までにない方法を生み出しています。セキュリティポリシーに劇的な変化を与えた要因の1つは、セキュリティの境界がはるかに流動的になり管理が難しくなったことです。クラウドや社外データセンターのデータが増えると同時に、自宅で個人所有のデバイスを使用して作業する従業員が増えたことで、セキュリティはもはや信頼できる内部ネットワークを保護するだけの問題ではなくなりました。

セキュリティ管理に対する過去の投資が安全性を確保すると考えてはいけません。最新の攻撃手法を理解し、既存のセキュリティ管理と計画の妥当性を継続的に評価してください。

こうしたリモートアクセスへの移行がセキュリティに与える影響を軽減するために、ネットワークにつながるすべてが敵対的だと想定するモデルであるゼロトラストアーキテクチャーを導入する企業が増えています。ゼロトラストでは、継続的な検証が行われ、特定のポリシーに基づいて適切なコンテキスト内でのみアクセスが許可されます。

レジリエンスへの道のり

サイバーレジリエンスは明確なセキュリティ戦略から始まります (関連記事:英語)。またそれは、プロジェクトのロードマップとさまざまな説明責任に即している必要があります。これらの計画により、セキュリティ戦略の適切な実行が可能になり、リスク管理に基づいた意思決定を行うことができます。

また、基盤として適切なインフラストラクチャとセキュリティ管理を展開するためのガイドラインを提供し、テクノロジーの変化に柔軟に対応できる強固なサイバーセキュリティアーキテクチャーも必要です。

どのような計画も攻撃を100%抑えることはできませんが、サイバーレジリエントな文化により、不注意、リスク、被害を最小限に抑えながら、組織がミッションクリティカルなセキュリティ戦略への集中を継続することが可能になります。

お客様のセキュリティ戦略を強化することが大切です。**DXCのセキュリティ脅威インテリジェンスレポート** (英語) をご購読ください。

著者について

マーク・ヒューズ
DXC Technologyのオファリング・戦略パートナー担当上級副社長。サイバーディフェンス、セキュアインフラストラクチャ、デジタルID、データ保護など、DXCのグローバルセキュリティ組織およびオファリングの責任者。以前は、BT Security社の最高責任者を務めていました。