Gartner

- News Release -

2018年7月24日

報 道 関 係 各 位

ガートナー ジャパン株式会社
広報室

ガートナー、セキュリティ・リーダーが優れた成果を出すために、信頼とレジリエンスを構築してセキュリティを拡張する方法を明らかに

『ガートナー セキュリティ&リスク・マネジメント サミット 2018』
(7月24～26日、八芳園) において、
セキュリティ・リーダーが直面している課題の解決策を提示

ガートナー ジャパン株式会社 (本社：東京都港区、以下 ガートナー) は、本日より開催している『ガートナー セキュリティ&リスク・マネジメント サミット 2018』のオープニング基調講演において、複雑化するデジタル・セキュリティに対して、セキュリティ・リーダーがどのように取り組みを拡張し行動すべきかを、3つのシンプルな質問を基にした議論の中で明らかにしました。

ガートナーのアナリストはセキュリティ・リーダーに向けて、セキュリティに関する従来の、そして新たな課題を解決するために、「人、プロセス、テクノロジを適応させるための拡張」「リスク・ガバナンスへのアプローチを変え、継続性と包括性を高めるための拡張」「スタッフ増員以外の方法でセキュリティ機能を増強するための拡張」を、それぞれどのように行うべきかについて、ガイダンスを提供しました。

これらの拡張は、「何が重要なのか」「何が危険なのか」「何が現実なのか」という3つのシンプルな質問によって把握することができます。ガートナーのアナリストは、一連のシナリオを通じて議論を展開しました。

「何が重要なのか」：組織全体の視点でリスクを捉える

ガートナーは、すべてのイニシアティブに対して、組織全体の視点でリスクを捉えることをセキュリティ・リーダーに提案しています。従来、リスクは狭い視野 (通常はリスク・オーナーの視点) で捉えられてきました。

ガートナーの主席アナリストのサム・オーヤイー (Sam Olyaei) は次のように述べています。「狭い視野を乗り越える上で大きな助けになるプラクティスがあります。まず、リスクのオーナーシップと責任を明確にして、説明責任という組織文化を確立、支援します。次に、組織全体のリスク一覧表 (リスク・レジスタ) を作成し、すべてのリスク領域の中で最優先に取り組むべきものを明確にします。そして最後に、リスクとその対策を、ビジネスの目的と目標に対して確実にマッピングします」

ビジネス上のリスクはサイバーリスクに由来する場合もあります。リスク全体の中に占めるサイバーリスクの重大性は、ますます高まっています。この部分への対策として、統合リスク管理 (IRM) が重要となります。

前出のオーヤイーは次のように述べています。「IRMによって、リスクの優先順位付けおよびリスク対策計画との関連付けを、容易かつシンプルに行えます。サイバーセキュリティおよびテクノロジのリスクを、さらに幅広く運用リスクと統合させ、先を見通すリスク監視の基盤を確立することをガートナーは推奨します。また、リスクに関する評価指標を定義してリスクを測定するとともに、リスクの予兆となる指標を特定します」

「何が危険なのか」:資産とエコシステムへの可視性を構築する

企業のエコシステムが拡大するに伴い、エコシステム内における相互の関連性を把握することは、ほぼ不可能になります。ある問題がエコシステム内に波及して広がっていくと、予期せぬ結果を引き起こす可能性が高まりますが、そこでのオーバーリアクションはむしろマイナスの影響をもたらすと、ガートナーのアナリストは述べています。

ガートナーのリサーチ バイス プレジデント 兼 最上級アナリストのニール・マクドナルド (Neil MacDonald) は次のように述べています。「2017年に一般に公開された脆弱性は、1万5,000件を超えています。しかし、重大性および緊急性が最も高いとされた脅威は、このうちのわずかです。大抵の場合、状況を評価して慎重に対応するための時間が、ある程度あります。しかし、主要メディアで盛んに報じられることにより、時としてこれらの脅威があっという間に最優先で取り組むべき対象に変わることがあります」

例えば、注目されるセキュリティ・リスクが常に存在する一方で、データを見れば、過去10年を通じて侵害対象となった脆弱性は実際には全体のわずか8分の1でしかないことが明らかだとマクドナルドは述べています。

セキュリティの脅威への対応では、信頼関係の課題の解決に重点が置かれがちですが、セキュリティ・リーダーは、レジリエンス (回復力) の目標から逸れないようにしなければなりません。組織的なレベルから技術的なレベルまで、レジリエンスは複数のレベルを網羅するよう設計する必要があります。

前出のマクドナルドは次のようにも述べています。「レジリエンスには全社規模の視点で取り組み、ビジネス・パートナーやITパートナーと連携してレジリエンスの目標を設定します。次に、危機管理およびコミュニケーション計画を策定することで、条件反射的な対応や習慣的な対応が引き起こすリスクを軽減します。3番目に、高可用性のためだけではなく、リカバリと継続性も含めたテクノロジとプロセスを構築します。最後に、これらのリカバリおよび継続性の計画の有効性を実証するために、何度もテストをくり返すべきです」

「何が現実なのか」:他者への権限の強化を通じてリスク・マネジメントを拡張する

セキュリティ・リーダーには、環境とリスクの適切なコントロールが求められます。そうしたコントロールは、1社のベンダーや1つのテクノロジだけではなく、複数のベンダーやテクノロジに適用できるとともに、リスクおよびコンプライアンスの環境が発展するのに合わせて変えられるものである必要があります。

ガートナーのリサーチ バイス プレジデント、ピーター・ファーストブルック (Peter Firstbrook) は次のように述べています。「アダプティブなコントロールによって、セキュリティはテクノロジのイネーブラへと変化します」

ファーストブルックは、成功の可能性を飛躍的に高めるためには、社内の他者への働き掛けが重要であるとしています。

さらにファーストブルックは次のようにも述べています。「ビジネス・プロセスのオーナーおよびITチームは、効果的なリスク・マネジメントのために、それぞれの専門知識を提供しなければなりません。これによって、リスクのプロフェッショナルは、変化するテクノロジとビジネスの現実を理解できるようになります。他の役割を担うユーザーがリスク・プロフェッショナルからのガイダンスとアドバイスを受けて、それぞれの職務においてリスク・ベースの考え方を採り入れられるよう、奨励していくべきです。このようにしてセキュリティの変革と規模の拡大を行うことは、セキュリティに関わる全員にメリットをもたらすWin-Winの手段となります」

ガートナーのサービスをご利用のお客様は、ガートナー・スペシャル・レポート「The Resilience Premium of Digital Business: A Gartner Trend Insight Report」で、レジリエンスの考え方の詳細をご覧いただけます。このレポートでは、確固たる姿勢でレジリエンスに取り組むことにより、避けられない破壊的状況からデジタル・ビジネスを回復させるための心構え、資源、計画を確立できるという点にフォーカスを当てています。

ガートナーは7月24～26日、『ガートナー セキュリティ&リスク・マネジメント サミット 2018』を開催しています。本サミットでは、国内外のアナリストならびにコンサルタントが、どのようにリーダーシップ能力を研鑽し、世界的に高まっているセキュリティ・リスクの問題に対してセキュアなデジタル・ビジネスを実現していけばよいのかについて、幅広いトピックにおける最新のトレンドや最先端の知見や洞察を提供いたします。

本サミットの詳細については下記Webサイトをご覧ください。
http://www.gartner.co.jp/event/srm/

本サミットのニュースと最新情報は、ガートナーのTwitter (https://twitter.com/Gartner_jp)でもご覧いただけます (#GartnerSEC)。