Gartner

- News Release -

参考資料
本資料は、ガートナー発信のSmarter with Gartnerの記事を和訳し一部追記したものです。
本資料の原文を含めSmarter with Gartnerのすべての記事は、以下でご覧いただけます。
https://www.gartner.com/smarterwithgartner/

2018年7月10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、2018年のセキュリティ・プロジェクトのトップ10を発表

CISOは、リスクを軽減させるとともにビジネスに大きなインパクトをもたらす
10のセキュリティ・プロジェクトに注力することが必要

米国メリーランド州ナショナル・ハーバー発－2018年6月6日－ガートナーは現地で開催した『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』において、2018年のセキュリティ・プロジェクトのトップ10を発表しました。

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。「最高情報セキュリティ責任者 (CISO) は、リスクを最大限軽減させるとともにビジネスに最大のインパクトを与えるプロジェクトに集中することが必要です。これらはプログラムではなく、真の意味での支援テクノロジのプロジェクトです。ほとんどのCISOにとって、これらは新しいテクノロジ・プロジェクトであり、企業におけるこれらの導入率は50%未満です」

CISOが注目すべきセキュリティ・プロジェクトのトップ10は以下のとおりです。

1. 特権アカウント管理

このプロジェクトは、攻撃者による特権アカウントへのアクセスをより困難にするとともに、異常なアクセスの挙動をセキュリティ・チームが監視することを意図しています。CISOは、最低限すべての管理者に必須の多要素認証 (MFA) を設定する必要があります。また外部委託先などの第三者によるアクセスについても、MFAを使用することをガートナーは推奨します。

2. CARTAに基づく脆弱性管理

ガートナーの「継続的でアダプティブなリスク／トラストのアセスメント (Continuous Adaptive Risk and Trust Assessment: CARTA)」アプローチにインスピレーションを受けたプロジェクトは、脆弱性管理への対応として優れた方法であるとともに、大幅なリスク軽減の潜在性を有しています。パッチの適用処理が機能せず、IT部門が数多くの脆弱性に対処しきれない場合に、このようなアセスメントの実施を検討します。すべてにパッチを適用することはできませんが、リスク・マネジメントの活動に優先順位を付けて実行することで、大幅にリスクを軽減させることができます。

3. アクティブ・アンチフィッシング

従業員が継続的にフィッシング攻撃の被害に遭っている企業向けのプロジェクトです。これにはテクニカル・コントロール、エンドユーザー・コントロール、プロセス再設計という3本柱の戦略が必要です。テクニカル・コントロールでは、可能な限り多くのフィッシング攻撃をブロックします。ただし、この防衛戦略の中では、ユーザー自身も積極的な役割を果たすようにしなければなりません。

4. サーバ・ワークロードのためのアプリケーション・コントロール

このプロジェクトは、サーバ・ワークロードのために「Default Deny (デフォルトで拒否)」やゼロ・トラストを実施しようと考えている企業が検討すべきオプションです。 ほとんどのマルウェアはホワイトリストに登録されていないため、このプロジェクトではアプリケーション・コントロールによってマルウェアの大部分をブロックします。前出のマクドナルドは、次のように述べています。「これは、非常に強力なセキュリティ態勢で、SpectreおよびMeltdownに対して有効であることが実証されています」。アプリケーション・コントロールは、包括的なメモリ保護と共に使用します。IoT (モノのインターネット) およびベンダー・サポートが終了しているシステムにとって、非常に有用なプロジェクトです。

5. マイクロセグメンテーションおよびフローの可視性

このプロジェクトは、データセンターのトラフィック・フローへの可視性とコントロールを求める、フラットなネットワーク・トポロジを採用している企業に適しています (オンプレミスとサービスとしてのインフラストラクチャ [IaaS] の両方)。このプロジェクトの目標は、データセンターへの攻撃が横方向に拡散することを阻止するところにあります。前出のマクドナルドは次のように説明しています。「攻撃者が攻撃を仕掛けてきたとしても、その進行は必ず阻止されます」。まず可視性をセグメンテーションの出発点にします。ただし、セグメンテーションをしすぎないようにしなければなりません。基幹アプリケーションから始め、ベンダーにはネイティブなセグメンテーションのサポートを要求します。

6. 検知／対応

セキュリティ侵害は不可避であるという認識に基づき、エンドポイント、ネットワーク、ユーザー・ベースのいずれかのアプローチによって高度な脅威の検知、調査、対応能力を実装したいと考えている企業向けのプロジェクトです。3つの選択肢があります。

- エンドポイント保護プラットフォーム (EPP) + エンドポイントの検知／対応 (EDR)
- ユーザー／エンティティ挙動分析 (UEBA)
- 偽装テクノロジ (Deception)

EPPベンダーにはEDRを提供することを、そしてセキュリティ情報／イベント管理 (SIEM) ベンダーにはUEBA機能を提供することを強く要求すべきです。マネージド検知／対応 (MDR) サービスの「軽量版」をベンダーから直接調達することを検討します。最後の「偽装テクノロジ」は、高い信頼性が求められるイベントにおいて脅威を検知する仕組みを強化する綿密な方法を探している企業にとって、小規模ではありながらも新しい、理想的なオプションとなっています。

7. クラウド・セキュリティの態勢管理 (CSPM)

既存のIaaSおよびサービスとしてのプラットフォーム (PaaS) のクラウド・セキュリティ態勢を包括的かつ自動的に評価して、リスクが過度に高い領域を明らかにしたいと考えている企業

が検討すべきプロジェクトです。クラウド・アクセス・セキュリティ・ブローカ (CASB) をはじめ、複数のベンダーから選択できます。使用しているIaaSが1つだけの企業の場合、まずAmazonかMicrosoftを検討するのがよいでしょう。CASBベンダーに対して、これを必須要件とします。

8. 自動セキュリティ・スキャニング

DevOps形式のワークフローにセキュリティ・コントロールを統合したいと考える企業向けのプロジェクトです。まずオープンソース・ソフトウェア・コンポジション分析から始めて、テストをDevSecOpsワークフローのシームレスな一部として統合します (コンテナも含む)。開発者がツールを切り替えないようにし、自動化に向けて完全なAPI対応を必須にすることがポイントになります。

9. クラウド・アクセス・セキュリティ・ブローカ (CASB)

マルチエンタプライズ、クラウド・ベース・サービスの可視性とポリシー・ベースの管理のためのコントロール・ポイントを探しているモバイル・ワークフォースを有する企業向けのプロジェクトです。まず「発見」から始めて、プロジェクトの正当性を証明します。2018年および2019年は、ウェイト・センシティブなデータの「発見」と「モニタリング」が重要なユースケースとなります。

10. ソフトウェア・デファインド・ペリメータ

デジタル・システムと情報へのアクセスを認める対象を、指定の社外パートナー、リモート・ワーカー、外注先のみに制限することで攻撃範囲を狭めたいと考えている企業向けのプロジェクトです。現在使用しているVPNベースのアクセスに伴うリスクを改めて確認することから着手すべきです。

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」で詳細をご覧いただけます。本レポートでは、レジリエンス (回復力) への確固たる取り組みによって、不可避の破壊的状況からデジタル・ビジネスが回復するための心構え、資源、計画を確立できるという点に焦点が当てられています。

ガートナーでは『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、ナショナル・ハーバーに続いて、東京、サンパウロ、シドニー、ムンバイ (インド)、ロンドン、ドバイで開催し、ITセキュリティのトレンドに関する詳細な分析を提供していきます。

日本では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』を開催します。本リリースの内容については、会期中、前出のマクドナルドが「2018年セキュリティ・プロジェクトのトップ10」(7月25日 11:15～12:00、22A) のセッションで解説します。

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/

本サミットに関する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)。