Gartner

- News Release -

2018年7月25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、日本におけるセキュリティの重要アジェンダを発表

『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、
セキュリティに関する最新のトレンドや最先端の知見および洞察を紹介

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、都内で開催している『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』の中で、2018年の日本におけるセキュリティの重要アジェンダを発表しました。

日本では、2017年から2018年にかけて、マルウェア、標的型攻撃、セキュリティの脆弱性、仮想通貨の流出事件、クラウド上での情報漏洩、働き方改革やEU一般データ保護規則 (GDPR) への対応など、さまざまなセキュリティに関連するニュースが報道されています。昨今のデジタル・ビジネスの推進に加え、高度化する脅威や複雑化する情報セキュリティとリスク・マネジメントにどのように取り組むべきか、セキュリティ・リーダーは難しい課題に日々直面しています。

本サミットのコンファレンス・チェアであり、ガートナー リサーチ＆アドバイザリ部門 リサーチ ディレクターの礒田 優一は、こうした昨今のセキュリティ・ニュースやインシデントを踏まえて、2018年に日本のセキュリティ・リーダーが議論し取り組むべきセキュリティの重要アジェンダとして、次の6点を挙げ、解説しました。

1. **海外拠点／サプライチェーンのセキュリティをどこまで強化すべきか**
2. **脆弱性マネジメントはどうあるべきか**
3. **デジタル・ワークプレースのセキュリティのあるべき姿とは**
4. **エンドポイントのセキュリティの最適解とは**
5. **クラウドのセキュリティで注目すべきポイントは何か**
6. **デジタルのセキュリティについてリーダーが考えるべきことは何か**

1. 海外拠点／サプライチェーンのセキュリティをどこまで強化すべきか

海外拠点やサプライチェーンなどを複数有する企業にとって、それぞれの拠点のセキュリティをどこまで強化すべきかは悩ましい課題となっています。企業としては海外拠点／サプライチェーンも含め、すべてを守るのが理想ですが、現実には全部を完璧に守ることは不可能です。しかしながら、海外拠点やパートナーを含めたサプライチェーンにおいてインシデントが発生すれば、その説明責任は本社に求められます。説明責任を果たすためには、リーダーシップと、インシデント発生後の観点に立った対応が、日頃から必要となります。

2. 脆弱性マネジメントはどうあるべきか

2018年の年明け早々ニュースになったSpectre/MeltdownのようなCPUの脆弱性や、2017年に多発し大きく報道されたApache Strutsの脆弱性を突いた攻撃のほかにも、脆弱性に対する攻撃は日々発生しています。そうした脆弱性に関する公開情報のすべてに対して、理想を言えばタイムリーにパッチを適用して対応したいところですが、本番環境への影響などを考えると現実はそうはいきません。膨大な脆弱性情報を手動で管理するにも限度があります。そうしたジレンマを解決するには、リスクの可視化と自動化がポイントになります。リスクをベースに脆弱性の優先順位を判断、可視化し、自動化を検討しなければなりません。

3. デジタル・ワークプレースのセキュリティのあるべき姿とは

働き方改革の推進に当たっては、利便性とセキュリティを両立させることが理想的だとよく言われますが、現実には従来の企業ポリシーからの逸脱など、両立が困難な場合も多く、対策に苦慮している企業が多く存在します。今までは「どこまで許可してどこから禁止するか」という観点でセキュリティ対策が行われてきましたが、これからは、「禁止」ではなく「許可」した上でセキュリティ対策を行う、「人中心のセキュリティ」へと変革していく必要があります。

4. エンドポイントのセキュリティの最適解とは

働き方改革の推進や、デバイスの多様化などにより、エンドポイント・セキュリティへの関心が高まっています。すべての局面でベストかつ万能なソリューションがあれば理想的ですが、そうしたソリューションは現時点では存在しません。また変化も速い領域であるため、製品／ソリューションの選定に当たっては、「機能」「価格」面の比較ではなく、ベンダーが広い視野で「戦略」をきちんと説明できているか、などを見極めることも重要です。

5. クラウドのセキュリティで注目すべきポイントは何か

クラウドに関するセキュリティは多種多様で、さまざまな角度からのものがあり、その粒度もさまざまです。クラウドに関しては、近年ではサービスとしてのインフラストラクチャ (IaaS) の利用に関する初歩的なインシデントが多発しています。そうしたものの大半は、単純な「設定ミス」によるものであり、IaaSを利用するユーザー側に原因があります。クラウドはデジタル・ビジネスを推進していく上で中核となるものであり、ユーザー自らクラウドをセキュアに使いこなす必要があります。セキュリティのプロフェッショナルは、クラウド視点でのリテラシを向上させ、DevSecOpsで求められる新たなスキルや経験を積み、デジタル・ビジネスの推進をサポートしていくべきです。

6. デジタルのセキュリティについてリーダーが考えるべきことは何か

デジタル・ビジネスの推進においては、ビジネス・スピードとセキュリティを両立させることが理想ですが、実際にはビジネス・スピードが優先され、セキュリティは後回しになりがちです。しかしながら、セキュリティが軽視されると、セキュリティ・インシデントにつながり、ビジネス自体が破壊される結果にもなりかねません。かといって、セキュリティを必要以上に優先させてしまうと、今度は実験的な試みや新たなチャレンジを妨げることになります。これは非常に悩ましい問題であると言えます。2018年1月に発生したコインチェックにおけるNEM流出事件は、一企業の不祥事と捉えることもできますが、そこから得られる教訓も少なくありません。企業はデジタル・ビジネスが暴走しないための歯止めとなるような大きな指針を持つとともに、スピード感ある開発／運用の現場レベルでの方針を持つ必要があります。

前出の礒田は次のように述べています。「セキュアなデジタル・ビジネスの実現に向けて、企業のセキュリティ・リーダーの役割はますます重要になってきています。企業はビジネス・ス

ピードとセキュリティの両立が可能となるような指針を持ち、さらに経営者に対して対等な立場で意見が言える『真のセキュリティ・リーダー』を擁立する必要があります」

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、前出の礒田のほか、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)。