セキュリティ

ITマネジメント（内部統制）

知ってますか？キャスビー、EDR、ピーサート

2019年のセキュリティ対策、5つのヒント（後編）

2019年に企業が取り組むべきセキュリティ対策について5つのヒントとは？
前編では、ビジネス推進のステークホルダー拡大の影響、また働き方改革によるワークプレースの多様化について解説しました。後編では、情報システムの管理において不可欠なアップデートマネージメントについて、また広範なクラウドサービスでのセキュリティ、企業におけるセキュリティ実践のリーダーシップとスタイルについて紹介します。

ヒント 3

システムのアップデートマネージメント

業務にかかわるシステム運用の話に特化してみましょう。ウェブでも、社内システムでも構いません。いずれの場合でも、稼働中のシステムをハッキングされ、情報を窃取される事件があとを絶ちません。このインシデントの企業への打撃は尋常ではありません。

原因の大半は、「稼働しているシステムのメンテナンスやアップデートを放置、あるいは放棄している」という運用上のミスに起因します。そこをきちんと行うと「8割はリスクが下がる」という専門家もいます。

昨今はシステム構成要素の多くが、自作のアプリケーションよりむしろ、毎週何百というアップデートがあるオープンソースソフトウェアやサードパーティのものになっています。クラウドプラットフォームを使っていることでサーバーをケアする必要がなくなってきたせいか、このアプリケーション層が放置されてしまうことがあるかもしれません。この放置状態の解決に取り組むにしても、社内の情報システム資産のカタログがそもそもない、という現実に直面することさえあります。

それでも、あきらめずにアップデートマネージメントに取り組むと、システムのリスクは激減します。まずは、オープンソースのツールで、OWASP Dependency Check（オワスプ・依存性チェックツール）や、VULS（バルス）というスキャナーを利用してみるのも良いでしょう。商用製品もいくつかあるようです。

システムのアップデートに計画的に取り組むと、副次的な効果もあります。つまり、コンポーネントのバージョン、ライセンス、プラットフォームの設定、管理の流れを把握できます。これらは情報システム運用にかかわる不可欠な要素であり、シフトレフトの第一歩、と言えるでしょう。

ヒント 4

クラウドサービスの一括コントロール

システムをスクラッチから開発統合する時代は鳴りをひそめ、現在はあらゆるビジネス機能がウェブを活用した既存のサービスとして調達される時代となっています。特に業務システムは、この流れの恩恵を大きく受けています。会計、人事、労務、マーケティング、コマース、またITガバナンスにいたるまで、すでにサービス・パッケージが「クラウドサービス」という名前をつけて乱立しており、検討しはじめてから稼働開始までの時間は非常に短くなっています。

昨今、G SuiteやOffice 365でメールやスケジュールを、顧客管理にSalesforceやKintone、ファイル共有はDropboxやBoxなどと目的にあった複数のクラウドサービスを組み合わせて活用している企業は珍しくなくなりました。それにともない、業務データの置き場所は、物理的に社内にある状態から、クラウドサービスや、それぞれのサービス間の連携によって行き来する流れとなりました。

社内外のネットワーク通信がこれほどシームレスになると、オンプレミスにデータを置いていれば安全だということも神話でしかありません。そのような状況で情報システム部門がまず取り組むべきは、会社が許可しているクラウドサービスだけでなく、社外や個人端末も含めて従業員が利用しているサービス(シャドーIT)の把握と、それらを利用するID/権限の管理です。

その第一歩として、CASB(Cloud Access Security Broker ／キャスビー)という、あらゆるクラウドサービスにアクセスするときにセキュリティを一括コントロールするソリューションが市場投入されています。これによって、シャドーITも含め従業員が利用しているクラウドサービスを一貫したセキュリティポリシーで管理できるとともに、類似サービスの統合など、業務改善に切り込むこともできます。さらに許可したサービスでも、データの暗号化を施していくというクールな機能も売り出されています。

これは、ただ導入すれば解決というほど、シンプルなソリューションではありません。企業に貢献するためには、まず利用されているクラウドサービスをどの程度把握し、管理できるのかということです。多様なアクセス手段が存在するため、クラウドサービスの利用をキャッチできないこともあります。また、会社のワークプレイスが多拠点になることを見据えて、ゲートウェイをどう設定し、またどう配備するかということも重要な検討課題です。事業推進に貢献する利便性とリスクテイクのバランスの適切さをどう考えるかが大きく問われるでしょう。

ヒント 5

セキュリティ推進のリーダーシップとスタイル

セキュリティの実施を担う部門をひとつに集約し、そこに押し付けることでは解決しません。特に流行りのCSIRTに実施と責任のすべてを負わせるべきではありません。CISO室など、リーダーシップの所在はひとつにするとしても、その施策の実現と改善のサイクルを回していくことは全部門の仕事になります。紋切り型のポリシーやガイドラインによって頭ごなしに全部門に押し付けるスタイルを避け、現実的で、段階的な改善を推進することが重要なポイントとなります。

そこで、高度なマネージメントの視点が必要となりますが、自社の取り組みを客観視し、段階的な改善のフォーカス分野を特定するため、外部の指標を活用することは良いスタートの助けになります。これには、アドホックな対応から徐々に成熟させていくという考え方や、内部で不足しているリソースを外部のリソースの活用によって企業のリスクにマッチするセキュリティを実現することも含まれます。最初の取り組みとしては、経済産業省が提供している「サイバーセキュリティ経営ガイドライン」も理解の促進に助けになります。また、具体的な取り組みの評価については、米国のセキュリティ専門団体によるセキュリティオペレーションのフレームワーク「CIS 20 Controls」を参考にするのも効果的でしょう。

また、サイバー攻撃の恒常的な標的となっているシステム開発や、ソフトウェアによる連携が必要となるIoTデバイス製品などを行なう会社の開発・運用部門では、リスクの高い技術リソースを扱うため、そのセキュリティ保持の実現はCSIRTだけではカバーできません。そこでCSIRTにあわせて、自社開発のサービスや製品開発に特化するセキュリティチームとしてPSIRT(Product Security Incident Response Team ／ピーサート)を別途設置した組織づくりをするアプローチがでてきています。

PSIRTが推進するプラクティスについては、詳細についてここでは割愛しますが、世界中の企業でインシデント対応チームのためのフォーラムであるFirst.orgが公開したPSIRT Frameworkというドキュメントや、ソフトウェアセキュリティに特化したコミュニティであるOWASPが公開しているOWASP SAMM(Software Security Maturity Model ／ソフトウェアセキュリティ成熟度モデル)、またシノプシスが提供しているBSIMM(Building Security In Maturity Model)などは、公開情報ですのでぜひ参考にしてください。

おわりに

2019年年頭のエンタープライズ・セキュリティとして、いくつかのトピックを取り上げました。これらすべては事後対応的にやることではなく、計画的に、戦略的に進められることばかりです。

政府の「サイバーセキュリティ月間」も例年通り2月から始まり、数多くのセミナーや研修などが開催されます。ここで皆さんが、あらかじめ問題意識を持って聞くのと、ただ情報の洪水に埋もれるのとではわけが違います。もっとも本稿では、皆さんがすでに認識していたことも多々記載されていたことでしょう。ただ、本稿がひとつの整理として、問題意識をもつ思考の一助になれば幸いです。今年はぜひ、戦略的にセキュリティに取り組んで行かれますよう。結果として、企業の、ひいては社会のセキュリティの実現にみなさんのお力をお貸しください。シフトレフト!

岡田良太郎（おかだりょうたろう）
株式会社アスタリスク・リサーチ 代表取締役/エグゼクティブ・リサーチャ

セキュリティリサーチャ。国内の企業や団体におけるセキュリティイニシアチブの継続的な支援に従事している。また、セキュリティ堅牢化・プロジェクトWASForum Hardening Project（ワスフォーラム・ハードニングプロジェクト）オーガナイザ、グローバルコミュニティ OWASP（オワスプ）のJapanチャプターリーダーを務め、2014年にThe OWASP Foundationより "Best Chapter Leader"を受賞。BBT大学では教員として「教養としてのサイバーセキュリティ」科目を担当している。また、政府・公共機関に協力し、情報セキュリティ10大脅威選考委員、総務省CYDER実行委員。CISA、MBAを保持。