protiviti®
Face the Future with Confidence

オリンピック開催を迎え、企業はサイバー攻撃にどう対処すべきか

2020
2月4日

今日、サイバー攻撃の脅威は、企業にとっての最大のリスクの一つです。プロティビティとISACAが共同で実施した調査結果[1]によると、2,200人を超えるグローバル企業経営幹部と専門家は、サイバーセキュリティ、およびプライバシー保護を含むデータガバナンスが企業の最大の懸念事項であると認識しています。一方で、年間収益が50億米ドルを超える企業の34％のみが、「事業に関連する情報セキュリティリスク」について、「取締役会による高い関与と理解レベル」を有していると答えています。また、サイバーセキュリティ監査活動を実施していない企業の42％が、的確かつ利用可能なリソースまたはツールが不足していることによりサイバーセキュリティ監査活動を実施していないと答えています。

2020年東京オリンピックを迎えて世界中から注目を集めることから、日本はサイバー攻撃の恰好の標的になります。過去のロンドン[2]、リオ、平昌オリンピックでは、個人データ流出や重要インフラへの侵入の試み、金銭的損失の発生等、オリンピックそのものだけでなく当該国の組織に対するセキュリティインシデントが多発しました。

たとえ一度のサイバー攻撃であっても、企業は金銭的損失や社会における評判の低下、個人情報の漏えい、コンプライアンス遵守違反による制裁金を課せられる可能性があります。警察庁によると[3]、2019年上半期には、1IPアドレスおよび1日あたり3,580件を超える探索行為があり、また、少なくとも2,687件の標的型メール攻撃が検出される等、日々多くの日本企業がサイバー攻撃の脅威に晒されており、個人情報やその他重要な情報が流出する等のニュースが報道されています。

オリンピック開催を目前にし、サイバー攻撃の脅威は今後も増大すると予想されます。企業はこれらのサイバー空間の脅威に備えるため、サイバーセキュリティとサイバーレジリエンスの両方を実現させる必要があります。

企業はどうすべきか？

プロティビティは、企業がサイバー攻撃を阻止、特定、および対応するために、以下の基本的な行動を行うことを推奨しています。重要なビジネスサービス、または多くの顧客や利害関係者に広く影響を与える可能性があるビジネスサービスは、これらの行動について優先順位を付けて検討する必要があります。

1. **セキュリティ意識を高める。** ― セキュリティ強化の最も簡単な方法の1つは、従業員の意識を高めることです。企業は、従業員の関与と意欲を維持するために継続して努力し、現在の脅威の環境を考慮した上でこの問題に関するコミュニケーションの量を増やしてください。また、以下の行動も必要です。

   - **疑似演習により、高度なフィッシング攻撃に対する意識を高める。** 高度なフィッシング攻撃は、多くの防御策を無力化します。技術的な防御策は、人的な防御策を超えることはありません。
   - **企業が最近の攻撃の痕跡情報（Indicator Of Compromise）に関する情報を更新しているか確認する。** IoCには、不審なインバウンド・アウトバウンドの通信パターン、原因不明の設定変更、特定のファイル読み取り時の異常なデータ量、ログにおける攻撃の兆候、特権ユーザーアカウントの異常な活動、システム内の不明なファイルやアプリケーション、プロセスの存在が挙げられます。

1 2019 IT Audit Benchmarking Study - Today's Toughest Challenges in IT Audit: Tech Partnerships, Talent, Transformation, https://www.protiviti.com/sites/default/files/united_states/insights/8th-annual-it-audit-benchmarking-survey-isaca_protiviti.pdf
2 IPA サイバーセキュリティシンポジウム 2014 報告書 https://www.ipa.go.jp/about/news/event/securitysympo2014/lecture.html
3 令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について https://www.npa.go.jp/publications/statistics/cybersecurity/data/R01_kami_cyber_jousei.pdf

2. **重要なビジネスサービスをサポートする重要なシステム、アプリケーション、インフラ、および第三者のニーズを特定する。**— 企業は、環境およびビジネスを機能させる重要な要素を特定していなければ、重大なサイバー脅威、特に国家による脅威に直面しても安全を維持できません。

3. **パッチを適用できない重要な技術は、緩和策を実施して保護する。**— これらの技術には、医療機器や産業用制御システム、レガシーアプリケーション等が含まれます。

4. **システムおよびネットワークへの全てのアクセス権限を評価し、承認されたユーザーのみが会社の資産を使用または管理できることを確認する。**— そのためには、デフォルトのアカウント情報やパスワードが確実に更新されていることが重要です。

5. **保護および検知の戦略を高度化する。**— システムとデータの保護における重要なステップの1つは、インターネットにアクセスできるシステムのセキュリティイベントの監視を強化することです。さらに、多要素認証（MFA）や積極防御技術（EDRやIPS（侵入防止システム）等）などのより高度な防御を展開すると、環境へのリスクが減ります。

6. **最新のサイバー脅威情報を共有し、取得する。**— 企業間および政府と企業間でサイバー脅威情報を共有することは、他の国家からの攻撃を軽減するのに役立つ可能性があります。共有プロセスを支援する情報共有分析組織（ISAC）は多数あります。企業は、適切なISACに加盟し、最新情報を入手する必要があります。

7. **サイバー脅威に関連するリスク評価プロセスを年に1回以上更新する。**— 脅威は急速に進化しているため、理想的には四半期ごとにリスク評価を実施し、新しい脅威とリスクの有無を確認する必要があります。さらに、リスク評価プロセスでは、機密データの損失より影響が大きいリスクを考慮する必要があります。例えばビジネス中断のリスクが挙げられ、それはサイバー攻撃を通じてリスクが顕在化する可能性があります。したがって、企業は適切なサイバー防御の設計に焦点を当て、これらのリスクが顕在化したときにそれらを軽減する義務があります。

8. **組織が新しい脅威に対処する最新のインシデント対応計画があることを確認する。**— 机上演習等のシミュレーションにより、インシデント対応計画のトレーニングおよびリハーサルを実施します。企業のリスクに応じて、年に1回以上、理想的には四半期ごとに計画を再検討してください。組織の事業継続計画および災害復旧計画をレビューし、特に重要なビジネスの実行に不可欠なシステムに関しては、サイバー攻撃からの業務中断の復旧手順が含まれ、かつそれらが最新であることを確認します。

9. **進化するリスクと脅威に対処するために、サイバー防御に十分なリソースを確保する。**— 蔓延する標的型攻撃を含む脅威環境を効果的かつ包括的に理解することにより、サイバー防御に十分なリソースを理解し、確保することが容易になります。

要約

重要なシステムや資産、知的財産の保護、およびビジネスモデルを維持するために、どのような必要な手順を実行するかはそれぞれの企業の責任です。上記で概説した9つの基本的な行動は、サイバーセキュリティを強化するための枠組みを提供しています。

プロティビティはどう支援するか？

プロティビティは、さまざまな方法で企業を支援することができます。

- **迅速にサイバーセキュリティプログラムを評価します。**— 1～2週間のプロジェクトで、企業のセキュリティ保護機能、サイバー関連のイベントを検知する機能、およびインシデント対応機能を調べます。この評価には経営幹部との机上演習も含み、結果、組織のサイバーセキュリティプログラムの長所と短所を明らかにします。

- **サイバーセキュリティ管理態勢を、評価および監査します。**— 当局が発行したガイドラインや基準も組み込まれ様々な業界の企業に豊富な適用実績を有するプロティビティ独自のフレームワークを用いて、現状のサイバーセキュリティ管理態勢の成熟度を評価します。評価結果と企業のリスクやその許容度等を基に今後のサイバーセキュリティ管理態勢の目標レベルを定め、目標レベルとのギャップ解消に向けた対応策の提言やロードマップを提供します。また、サイバーセキュリティ管理態勢に対する独立した立場からの有効性を確認する「サイバーセキュリティ監査」について、リスクアプローチによる監査計画の立案、監査プログラムの策定、監査のコソース／アウトソース、およびフォローアップ監査の支援も提供します。

- **新しいサイバー機能や技術を実装および管理します。**— サイバー攻撃を避けることはできませんが、並行してサイバーセキュリティ技術も進化しています。企業のサイバーセキュリティ機能を自動化、調整、更に成熟させる必要性が高まっている中、プロティビティは技術（ロボットや人工知能、機械学習など）を活用してサイバーセ

キュリティの効率を改善し、安全に成長させることができます。

- **リスクを評価し、オペレーショナル・レジリエンスプログラムを構築します。**— 定量的なデータ駆動型および根拠に基づいた方法を使用して、サイバーリスクを定義（範囲や規模等）および優先順位付けし、十分な情報とともにビジネス上の意思決定の実施、および継続的な改善を推進するプログラムを設計します。

- **適切な人財やスキルにより、セキュリティチームを補完します。**— プロティビティの親会社であるロバート・ハーフ・インターナショナルとのパートナーシップにより、各企業のご要望に基づいて、適切な人材を適宜に導入します。

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。25ヶ国、85を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、オペレーション、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、Fortune 1000の60%以上、Fortune Global 500の35%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half International（RHI）の100%子会社です。

protiviti®