protiviti®
Face the Future with Confidence

取締役会のリスク監視：Risk Oversight

パッチ適用に要する時間の考察

最近発生した信用情報会社からの大規模な情報流出は、サイバー脅威から自らの組織を保護するために取るべき行動を、取締役会と経営者が認識しているのかという問題を提起しています。取締役会は、自らが認識していない事柄を把握しようとしているでしょうか。

ISSUE 97

2017年9月、信用情報会社であるエクィファクス社は、米国の人口の40パーセントを超える人々の個人情報が流出したことを公表しました。この公表直後、同社の株価は14パーセント近く下落し、CIOとCISOの交代、そしてCEOの交代が次の3週間の間に行われました。このインシデントが大きく報道されたことは、多くの人々の記憶に残っています。サイバー脅威に関心を寄せる誰もがこの件を話題にしているのです。

エクィファクス社はデータ流出を発生させた無数の会社の一つに過ぎない、というわけではありません。同社は、2015年から2017年まで、フォーブス誌が選ぶ「世界で最も革新的な企業100社」の一つであったのです。一体何が起こったのでしょうか。

2017年7月29日、エクィファクス社のセキュリティ・チームは、同社の米国の申し立て受付ポータルのウェブアプリケーションに関する疑わしいネットワーク・トラフィックに気付いたため、調査を行い、その疑わしいトラフィックを遮断しました。翌日、疑わしい動きが他にも確認されたため、同社はウェブアプリケーションをオフラインにしました。内部調査が行われ、オープンソース・ウェブアプリケーション・フレームワークの攻撃を受けた箇所に脆弱性が発見されました。この脆弱性は、US-CERT（国土安全保障省のサイバーセキュリティ部門）が2017年3月初めに特定・公表していたものでした。同社の調査により、個人情報（氏名、社会保障番号、生年月日、住所、および一部の人々の運転免許証番号）が含まれる特定のファイルへの不正アクセスは、2017年5月13日から7月30日の期間に発生したと考えられています。つまり、セキュリティ上の欠陥は、ハッカーがそれを悪用してセンシティブなデータにアクセスする2か月前に特定されていたということです。同社は問題のウェブアプリケーションにパッチを適用し、オンラインに復帰させました。[1]

このインシデントは、エクィファクス社はなぜ脆弱性が最初に特定された際に、自社のシステムに適切なパッチを適用しなかったのかという疑問を投げかけています。確かに、パッチ適用を適時に行わなかったがためにサイバー攻撃を受けた企業は他にもあり、我々はエクィファクス社の社内状況を詳しく把握しているわけではありません。しかし、どの企業の取締役会と経営陣も、このエピソードによって、自社のサイバーセキュリティ戦略と戦術を理解し、自らが認識する必要がある事柄を現に認識しているかを把握することの重要性を、再認識することでしょう。

主要な考慮事項

サイバーセキュリティに関しては多くの重要な面があり、それらの一部としては、組織の「最も重要な資産」と経営者が回避したい事業上の結果の特定、変化し続ける脅威の状況の理解、および実効性のあるインシデント対応プログラムの整備が挙げられます。しかしここでの論点はより具体的であり、既に認識しているシステムの脆弱性についてです。これは、誰もが認識していながら口にしたがらない問題です。側堡がさらされているのであれば攻撃される前に補強せよ、という賢明な助言が、ここでは適切であるように思われます。非戦闘員であっても、必死の戦闘の中でさらされている側堡を守ることの意味を理解するでしょう。認識されている脆

1 Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes（2017年9月15日）：https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832

弱性がさらされている側堡に相当するものであることは間違いなく、センシティブなデータが関係する場合にはなおさらです。

パッチとは、新たなセキュリティ上の脆弱性やバグの是正、ソフトウェアの安定性に関する問題への対応、あるいは使用しやすさやパフォーマンスを改善する新たな機能の追加を行うために、現行プログラムにインストールされる更新ソフトウェアです。パッチは一時的な対処であることが多く、本質的には急場しのぎです。パッチは必ずしも問題の解決策として最善ではありませんが、製品開発者が次の製品リリースに向けてより良い解決策を設計するまでの間、問題に対応するものです。

複数の複雑なシステムを使用している大規模組織では、ソフトウェアへのパッチ適用に時間を要することは明らかです。脆弱性が特定された場合には、パッチを開発し、本番環境に移行する前に問題がないことを確認するテストを実施しなければなりません。しかし、多くの人々は、パッチの開発と適用における困難があるとしても、エクィファクス社はより素早く行動すべきであったと考えています。エクィファクス社は、多くのセンシティブなデータを持っており、そのようなデータを取り扱うに足る信頼性を有するブランドであることを示唆しているのですから、なおさらです。[2]

プロティビティがセキュリティとプライバシーに関するコンサルティングを提供している企業では、多くの場合、脆弱性の発見から60～90日後までにパッチ適用が行われています。旧来のアプリケーションに不具合を生じさせることを恐れて、高リスクの脆弱性に対するパッチを適用していないケースも見受けられました。このような場合には、組織は事実上、これらのパッチを適用しないリスクを受容し、代替的な方法によりリスクを低減するということです。プロティビティの経験では、標準的な基準として、パッチのリリースから適用までの期間を30日以内とすることが通常です。

この基準は十分なものでしょうか。企業は事実上、30日間脆弱性にさらされている状態に自らを置いているのです。その一方で、企業はその間に発生した不正な動きを検知する能力を欠いているかもしれません。「サイバーリスク事象は、発生するかどうかの問題ではなく、いつ発生するかの問題である」という使い古された言い回しは、常に攻撃が行われている今の時代の現実に当てはまるものではありません。大部分の企業では、サイバーリスク事象は既に発生し、発生し続けているのです。けれども、多くの企業は、必要とされるより高度な検知と対応における能力を欠いているのです。世界中でデータプライバシーに関する多くの規制が制定され、重大なデータ侵害に関する報道が人々の記憶に留まっていることから、取締役会も経営者も、「サイバー・レジリエンス」の必要性を認識し始めています。

適切に設計された脆弱性管理プログラムを備えている組織では、外部に提供する重要なサービスに関係する認識済みの脆弱性に対して、パッチの適用が迅速に行われています。例としては、サービス内容に関する合意の中で72時間以内という目標値を掲げ、攻撃を受けた場合の損害を押さえようとしている企業が挙げられます。24時間以内、あるいはより短い時間での対応を目指している企業もあります。つまり、経営者と取締役会は、サイバーセキュリティの脆弱性に対応するパッチのリリースから適用までに要する時間を確認し、それに30日（あるいはそれ以上の日数）を要するとすれば、適時性の面で十分と言えるのかを検討すべきであり、外部に提供するサービスに関係するシステムやセンシティブな個人情報に関する脆弱性であれば特にそうです。重大なセキュリティ侵害、企業の受託責任に関する期待、およびレピュテーションとブランドイメージへの影響に対する公衆の視線は、注意深い監視の必要性を示しています。

重大な脆弱性を認識したのであれば、即時に外部に提供するサービスに関係するシステムを検査することが極めて重要であり、脆弱性が認識されたその日のうちの検査実施を目標とすべきです。また、包括的なITガバナンス・プロセスの一環として、パッチの適用状況の追跡と検証を行うべきです。パッチを単にリリースするだけでは十分ではありません。包括的なITガバナンス・プロセスにより、リスクが適時に、真に低減されていることを確認すべきです。

また、取締役と経営者は、重大なセキュリティ侵害が検知されるまでに経過した時間にも関心を寄せるべきです。プロティビティの経験では、発見的コントロールやモニタリング・コントロールの成熟度は、ほとんどの業種において低い水準にあり、セキュリティ侵害を適時に検知できないままとなっています。攻撃側はより高度な手法を用いてきているため、想定される攻撃のシミュレーションを定期的に実施し、セキュリティ侵害の検知とセキュリティ・チームによる適時の対応を確実とすべきです。

インシデント発生後にその影響と拡散を押さえるための組織的準備に課題が存在しています（つまり、攻撃の開始から検知までにあまりにも多くの時間を要しているのです）。多くの場合、疑わしい動きが検知されるまで100日以上を要しており、2件に1件の割合で、組織は第三者を通じてセキュリティ侵害の発生を認識しています。プロティビティが実施したペネトレーション・テストでは、ほとんどすべてのケースにおいて、テストの実施を許可したクライアントが、テストが実施されていることを検知できませんでした。多くの組織は、マネー

2 How the Equifax Data Breach Happened: What We know Now（2017年9月16日）：http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html

ジド・セキュリティ・サービス・プロバイダ（MSSP）[3]への業務委託によって問題をまるごと解決できると考えています。しかし、これが事実ではないことは繰り返し示されてきました。多くの場合、委託元企業とMSSP間のプロセスと協力関係が破綻したことにより、攻撃の検知に失敗しています。セキュリティ侵害を適時に検知できないという発見的コントロールの失敗に十分な焦点を当てている組織は多くありません。

インシデントの発生が認識された際に、組織が即時に対応するための準備ができていなければなりません。注意深く検討された対応計画を整備し、定期的なテストを行うことにより、適切かつ十分に迅速な対応を確実とすべきです。計画は、全ての関係者にそれぞれの具体的な役割を理解させ、データ侵害の公表や関連する開示についてもカバーすべきです。データ侵害を公表する際には、問題をこじれさせないよう注意を払うべきです。例えば、公衆に対して彼らの権利と、彼ら自身を保護するために取り得る行動を伝えるためのサイトを立ち上げるのであれば、そのサイト自体の安全性を確保すべきであり、企業の公式ドメイン内にサイトを置くことにより、詐欺サイトと受け取られ、余計な混乱を生じさせることがないようにすべきです。

取締役会は、サイバーリスクの監視において、これら2つの面－パッチの適用に要する時間とセキュリティ侵害の検知－を考慮すべきです。どの組織も、サイバーセキュリティに関する具体的なインシデントの影響と、経営者の対応計画の方向性が適切であり、十分に実行可能な状態にあるかを改めて見直すべきです。この見直しには、社内プロセスと能力を評価し、短期的および長期的に、必要な改善を行うために主体的ステップを取るべきであるのかを判断することが含まれます。組織がクラウド・サービスやより新しいアーキテクチュアを利用するために旧来のインフラを刷新することにより、適時に脆弱性を是正することがより容易になるはずです。それまでの間、認識されているシステムの脆弱性と検知されたデータ侵害に対して適時に対応することにより、企業は自社の側堡を注意深く守る必要があります。

取締役会の考慮事項

以下は、事業体の活動に内在するリスクに関連して取締役会が考慮すべき事項です。

- 取締役は、自社の脆弱性に対する管理を理解しているか。例えば、取締役会は、以下の項目の対応に要する時間を確認しているか。
  - 特定されたシステムの脆弱性に対するパッチ適用に要した時間
  - 攻撃の開始から検知までに要した時間
  - セキュリティ侵害の検知から、その拡散と影響を押さえるための対応計画の発動までに要した時間
  - 重大なデータ侵害の検知から、関連する法規制に基づく一般公衆、規制当局、および執行当局に対する所定の開示を行うまでに要した時間
- サイバーセキュリティは、取締役会において適宜状況を把握しておくべき、組織の中核的リスクの一つと捉えられているか。取締役会は、セキュリティ・インシデントのリスクを受容可能な水準まで低減するための自社の戦略は、釣り合いが取れており、最も重要な情報資産と事業上の結果に向けられていることを確認しているか。取締役会は、セキュリティ・プログラムの現状に関する客観的な指標または報告を受領しているか。
- 取締役会は、インシデント発生後の対応、復旧、および通常業務再開に関する規定の行動をまとめた計画について、データ侵害によるレピュテーションの棄損を最小限に留めるための顧客と従業員への対応を含めて、その十分性を確認しているか。

3　MSSPとは、ネットワーク・セキュリティに関する管理サービスを提供するインターネット・サービス・プロバイダです。そのようなサービスには、ウィルスやスパムの遮断、侵入の検知、ファイアウォール、および仮想プライベートネットワーク（VPN）の管理が含まれるかもしれません。

プロティビティの支援

プロティビティは企業と共に、以下の様な根本的な情報セキュリティの課題に焦点を当てています。

- 何を保護する必要があるのかを認識しているか（例えば、最も重要なデータと情報システム資産）、それらはどこに存在するか。それらの資産について以下の事項を考慮しているか。
  - それらの資産を十分に保護しているか。何によってそのことを確認できるか。
  - 誰からそれらの資産を保護しているのか、誰に対してそれらの資産へのアクセスを許可すべきか、アクセスを許可すべき者とそうではない者をどのように区別できるか。
  - 保護の仕組みは有効であるか。設計されたとおりに機能しているか。
  - 計画どおりに物事が行われていない場合に、どのようにしてそのことを把握するのか。
- 自社の環境に対する新たな脅威の認識と想定される攻撃手法の検知を適時に行い、脅威に合致するよう保護の仕組みを見直しているか。
- よからぬことが起こった際に対応する準備ができているか。そのようなインシデントを管理する能力を有しているか。インシデントが発生した際に、その再発を防ぐことができるか。

プロティビティは、幅広い種類のセキュリティとプライバシー評価 、アーキテクチャ、トランスフォーメーションと管理に関するサービスを提供し、セキュリティとプライバシーに関するエクスポージャー（例えば、顧客データの喪失、収益の喪失、あるいは レピュテーションの低下）を未然に特定し対応する上での企業の支援を行っています。プロティビティは、全ての業種の企業と共に、情報セキュリティ・プログラムの成熟度や統制の有効性を評価し、必要である場合には改善策の策定と実施を支援しています。セキュリティ・インシデントへの対応、主体的なセキュリティ・プログラムの確立、個人情報とアクセス管理対応、および業種に特有のデータセキュリティとプライバシーの課題への対応における企業の支援に関して、プロティビティは、確たる実績を有しています。世界クラスのインシデント対応における経験と専念により、プロティビティはセキュリティ戦略、対応実施、フォレンジック分析、および対応計画策定における深い専門知識を有しています。

Board Instituteが取締役会のリスク監視の新たな評価ツールを公開

TBI Protiviti Board Risk Oversight Meterは、取締役会が自らのリスク監視プロセスを見直し、真に重要性のある機会とリスクに焦点を絞ることを確実にする機会を提供するものです。プロティビティは、企業が自信を持って未来に立ち向かうための継続的なプロセス改善を促進することにコミットしており、柔軟で費用対効果に優れたツールを提供するためにBoard Instituteと協力しています。このツールは、取締役会が自らのリスク監視について行う定期的な自己評価を支援するものであり、多くの取締役が好ましいと考える自己評価のあり方を反映したものです。

詳しくはこちら：www.protiviti.com/boardriskoversightmeter