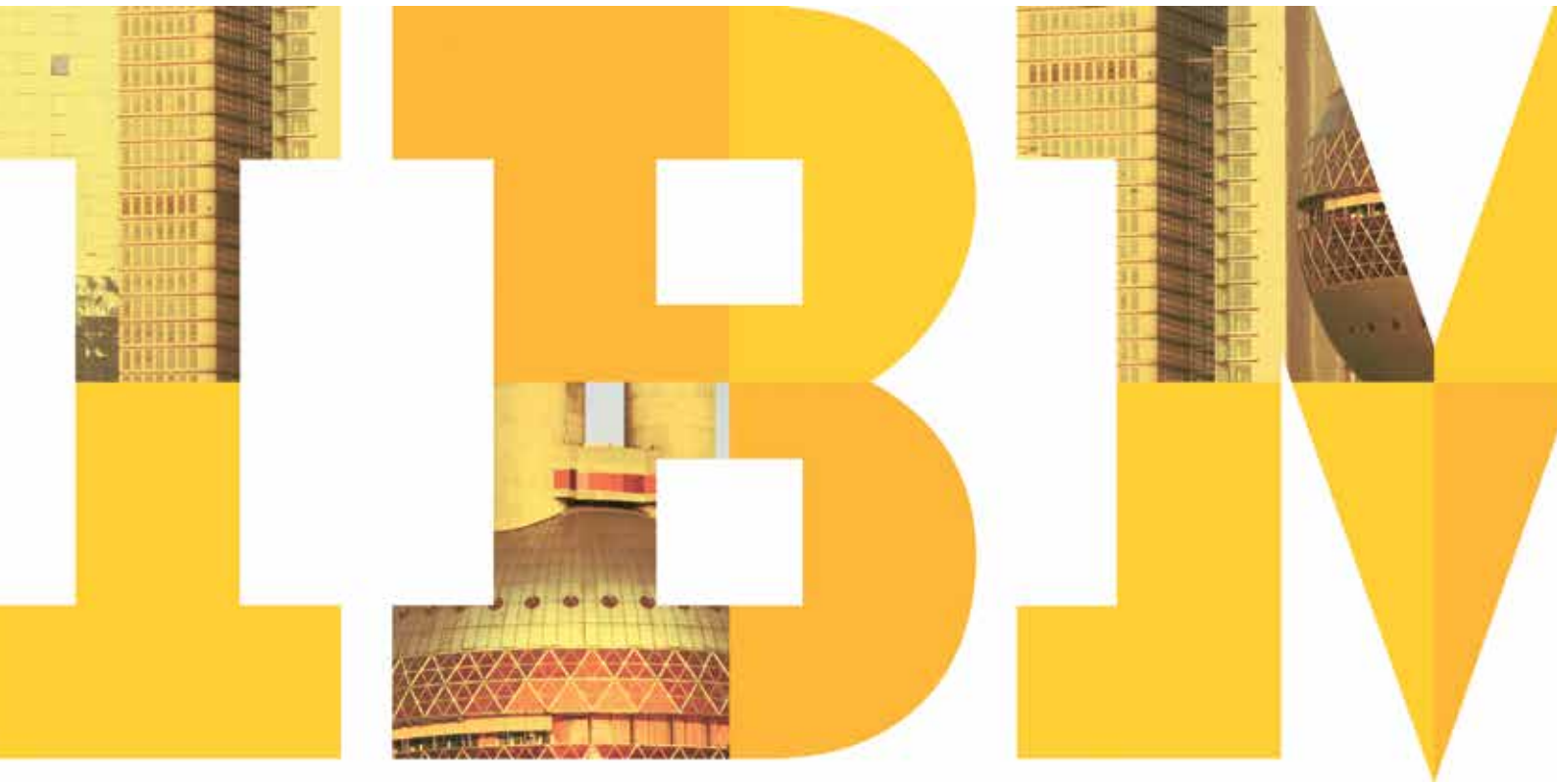
巧妙なセキュリティー攻撃への対応と復旧

組織を常に安全な状態に保つために今すぐできる 4 つのステップ



IBM

目次

はじめに

今日、サイバー攻撃も攻撃をしかける犯罪者も例外なく年々巧妙になってきています。同時に、IT リソースはファイアーウォール外へ移動し、企業はアプリケーションやデータを複数のデバイスに分散するようになっています。今や、組織の周囲を保護するだけでは十分でないことが明らかです。Advanced Persistent Threat (APT)* など、巧妙なサイバー攻撃は従来の防御を迂回するようになっています。

私たちは皆、大規模なセキュリティー・インシデントが企業のデータ、ネットワーク、企業ブランドにどのような影響を及ぼす可能性があるかを十分認識しています。また、重要な情報へ継続的にアクセスしたり、重要なインフラストラクチャーに危害を加えることを目的とした巧妙なセキュリティー攻撃は、重大度が増していると同時に、ますます頻繁に発生し、ますます莫大な損害をもたらすようになっていることも認識しています。

重大度: 巧妙なセキュリティー攻撃には、次のようなものがあります。

- 知的財産の搾取、侵害
- 銀行口座、その他財務資産の窃取
- 各コンピューターおよびシステム全体へのマルウェアの拡散
- 企業や顧客の機密情報のオンライン公開
- 重要なインフラストラクチャーへの危害

頻度: ビジネス・リーダーおよびセキュリティー担当者2,618 名を対象に、米国、英国、ドイツ、香港、ブラジルで 2012 年に実施した調査で、組織は 1 週間に平均 66 件のセキュリティー攻撃を受けていることがわかりました。中でも、ドイツと米国の組織の数値が高く、それぞれ 1 週間あたり 82 件、79 件でした。また、IBM X-Force 研究開発チームは、2012 年の中間レポートで全体的な脆弱性の増加傾向に触れており、年末までには史上最高となる可能性があると予測しました。[2]

コスト: 2012 年の調査によると、1 件のサイバー攻撃からの復旧にかかる平均コストは約 300,000 ドル (約 3 千万円**) 相当でした。[3] 1 年間では約 10 億ドル (約 1,000 億円) にも相当します。

さらに、こうした巧妙な攻撃を裏で操る人々は、根気強く、長期にわたって計画を立てます。偵察を行い、特定の脆弱性を標的にします。また、焦点を悪用から破壊に向けています。

このホワイト・ペーパーでは、組織を常に安全な状態に保つための事前対策として今すぐ実行できる、そして実行する必要がある 4 つのステップについて説明します。

- **Prioritize:** ビジネス目標に優先順位を付け、リスク許容度を設定する
- **Protect:** 事前対処型のセキュリティー計画で組織を保護する
- **Prepare:** 巧妙なサイバー攻撃という不可避の事態への対応を準備する
- **Promote:** セキュリティー意識の高い文化を促進および支援する

ステップ 1: ビジネス目標に優先順位を付け、リスク許容度を設定する

過去数年間の経験から、「セキュリティー」は相対的な用語であることが明らかになっています。私たちが企業を完全かつ恒久的に安全なものにしたいと考え、対処したとしても、現実は違うからです。それでも、巧妙なサイバー攻撃の脅威が高まる中、情報を守り、人々とインフラストラクチャーを保護するという課題に真剣に取り組むことが求められています。そのためにはまず、優先順位を設定します。

企業のセキュリティーにとって最も重要な事項とその理由を特定する

これは極めて当前のように思われますが、ビジネス目標について真剣に考え、最も重要な事項と許容できるリスクの程度について時間をかけて議論することで、組織全体の独自のニーズを満たすセキュリティー方針の強固な基盤を築くことができます。このような基盤を確立したら、正しい方向へと大きな一歩を踏み出したことになります。

攻撃に対して最も脆弱な領域を特定する

ビジネスを保護する上で重要な領域とそうでない領域、脆弱な領域とそうでない領域があります。ここでは、責任を追及するというよりは、現状の把握に努め、全体としてより安全な環境を構築できるようにします。

最大の脅威となる攻撃を具体的に特定する

巧妙なサイバー攻撃は、一般に重要なデータの損失や悪用、重要なインフラストラクチャーの破壊など、できるだけ大きな危害を加えることを目的としています。そのため、企業の情報やビジネス上重要なシステムを攻撃者の視点からとらえる必要があります。そして、攻撃者が何をすると損害が最大になるのかを検討します。

攻撃が発生した場合に最も大きな損失を受ける領域を特定する

ここで最悪の事態を想定します。ポイントは、ビジネス上最も打撃が大きい領域に攻撃を受けた場合、被害がどこまで広がるかを把握しておくことです。

企業の情報やビジネス上重要なシステムを攻撃者の視点からとらえる必要があります。

オンライン・ゲーム/エンターテインメント・サイトのハッキングにより、1 億人分の顧客レコードが漏えい

推定コスト: 36 億ドル (約 3,600 億円)

被害者: オンライン・ゲーム・コミュニティーおよびエンターテインメント・サイト

被害状況: ゲーム・ネットワークへの「外部侵入」により、7,000 万人分の顧客アカウントが漏えいし、個人データおよびクレジット・カード・データがリスクにさらされました。この会社は、調査中にオンライン・サービスを停止せざるを得ず、世論の反感を買うと同時に、良くない報道が広がりました。エンターテインメント部門への 2 回目のハッキングによって、さらに多くの顧客データが漏えいしました。

原因: 報道によると、ハッカーはネットワークのセキュリティーを突破し、暗号化されていないアカウント・データやユーザー・データのほか、一部のクレジット・カード・データにもアクセスできたということです。

損害: 広範囲に及ぶ世論の反感に加えて、事業の損失額および対応に要した費用として 1 億 7,100 万ドル (約 170 億円) 以上の損害が発生したと報じられています。また、株価が 12 パーセント下落し、時価総額が約 36 億ドル (約 3,600 億円) 減少したということです。

教訓: 悪用された脆弱性の 1 つは、この会社でも認識していたと伝えられています。企業は、情報資産に関するリスクを管理するためのフレームワークを利用するだけでなく、そのフレームワークをサポートする強力なガバナンス・メカニズムを確立する必要があります。

実例を基に構成したものです。記載されている事実および損害は、実際とは異なる場合があります。*公表されている財務情報、公開されている記事を基にしています。*

ステップ 2: 事前対処型のセキュリティー計画で組織を保護する

優先順位を設定したら、次は計画を策定し、適切なテクノロジーを導入して、実行に移します。ここで、確実に企業が潜在する脅威を認識して、事前に措置を講じておくことで継続的に企業を保護できるようにします。

IT セキュリティーに対する、情報に基づいた事前対処型のアプローチを策定する

セキュリティー戦略に、ステップ 1 で優先事項として特定した資産や情報の保護に必要なポリシーとテクノロジーを導入します。適切な措置を講じて脆弱性を管理することは、事前対処型のセキュリティー対策には欠かせない要素です。ここで策定するセキュリティー・ポリシーは、情報セキュリティー管理戦略の基盤となります。これらのポリシーに基づき、セキュリティー要件、プロセス、テクノロジー標準を文書化します。さらに、スマートなセキュリティー戦略を策定すれば、脆弱性を検出し、取り除くことができるほか、リスクを軽減し、IT セキュリティー管理コストを削減することにより、事業運営を強化することもできます。

既存の脆弱性を特定して修正する

これは、全コンピューターの全オペレーティング・システムに最新のセキュリティー・パッチを適用し、常に最新の状態を維持するという、多くのリソースが必要になるとはいえ単純なものもあれば、ビジネス・アプリケーションの脆弱性など、検出して修正することが難しいものもあります。

既存の脅威に備えて調整する

巧妙なサイバー攻撃の被害を受けていないという確信はありますか。特に、Advanced Persistent Threat (APT) などの悪質な攻撃は、できるだけ長い間存在を確認できないように設計されており、ネットワーク・トラフィックを生成することなく、侵入を許したホストから別のホストへと次々と移動します。すべてのAPT の中心にあるのがリモート制御機能です。犯罪者は、リモート制御機能を使用して標的の組織内の特定のホストに入り込み、ローカル・システムを操作して、重要な情報への継続的なアクセスを確保します。このような脅威から保護するには、システムと不法侵入者間のリモート制御通信を検出できるツールが必要です。

セキュリティーに関するポリシー、手順、テクノロジーが有効であるかどうかを厳密にテストすることが、これまで以上に重要になっています。

何度もテストを重ねる

セキュリティー攻撃はますます巧妙化しているため、実際に被害を受けるのも時間の問題に過ぎません。そのため、セキュリティーに関するポリシー、手順、テクノロジーが有効であるかどうかを厳密にテストすることが、これまで以上に重要になっています。そうすることが、当然の注意義務に関する法規制上の要件の重要な要素となっているため、特に重要性を増しています。テストを怠れば、執行役員はセキュリティー侵害の結果について責任を問われる可能性があります。

また、セキュリティーの状況はかつてないほどの速度で変化し続けているため、定期的なテストおよびレビューに関するポリシーを導入することも同様に重要です。

セキュリティー・インテリジェンスに対するスマートなアプローチを採用する

IT 部門を常にパニック状態に陥らせることなく、すべてを完全に掌握しておくにはどうすればよいのでしょうか。セキュリティー・インテリジェンスおよびアナリティクス・ツールで、複数のセキュリティー・テクノロジーのデータ・アクティビティーを積極的に監視し、相互に関連付けることで、環境内で何が起こっているかを可視化し、把握することができます。これにより、疑わしいアクティビティーを見分けて、調査することができます。また、マルチベンダー環境でも共通の言語で連携できるため、複雑さが軽減されると同時に、IT 部門の負担を取り除くことができるほか、時間とコストを節減できる可能性もあります。

ガバナンス手順を策定し、リスクの所有権を割り当てる

巧妙なサイバー攻撃などの脅威から企業を保護するセキュリティー・プログラムやポリシーの有効性は、組織の各従業員がどれだけ規則に従って行動できるかによって決まります。そのため、長期的に状況の把握を可能にする計画の導入が必要です。その際、セキュリティー・ポリシーの監視と管理をだれが行うのか、リスクに対する方針が守られていることをどのように証明するのかなどを決定します。必ず重要なビジネス領域全体でセキュリティー・プログラムに所有権およびリーダーシップを割り当ててください。主要な領域全体にリスク説明責任と意識を広げることによって、導入したセキュリティー制御に対する理解を高め、実施を促進することができます。さらには、より安全なビジネス環境を構築することもできます。

セキュリティー投資の価値を示し、文書化する

効果的なセキュリティー・プログラムを策定して管理するには、必要な予算を確保しなければなりません。また、発生していない攻撃を数字で表すことは非常に難しいため、何を行おうとしているのか、それがなぜ重要なのかについて、継続的なコミュニケーションを図ることをお勧めします。例えば、重要なシステムやデータに侵入した、または侵入した可能性のある重大なアクティビティーを報告することによって、セキュリティー・テクノロジーへの投資の価値を示し、ギャップを特定し、進行中の攻撃を阻止し、合理化の機会を明らかにし、このアプローチに対する信頼を引き出すことができます。

49%

の IT 部門のエグゼクティブが、現在のセキュリティーの取り組みの有効性を測定できないことが問題となっていると述べています。[4]

すべてを再検討して、ギャップや不要な重複がないことを確認する

グループで作業を行うと、個人的に責任を負わない要素については、自分がやらなくても他のだれかが代わりにやってくれただろうと考えるという過ちを犯しがちです。同様に、複数の人が同じことをするという事態も起こりやすくなります。そのため、計画に漏れや明快さに欠ける点がないことを最後に確認する必要があります。例えば、セキュリティー・インテリジェンス、アナリティクス、監視に関する条項が導入されていることを確認しておけば、不要な複雑さや支出を軽減できると同時に、継続的な監視、管理、リアルタイムの意思決定をテクノロジー全体で簡素化できる機会を期待できます。

1 年半以上にわたってディスカウント業者から顧客データが盗難 (少なくとも 4,500 万件のレコードが盗難)

推定コスト: 最大 9 億ドル (約 900 億円)

被害者: 全国規模のディスカウント業者

被害状況: 会社のシステムから顧客 4,500 万人分のクレジットおよびデビット・カード番号が盗まれたと推測されますが、インシデントの期間と性質を考えると、実際に盗まれたレコード数を特定することは困難です。この漏えいデータは犯罪者に売られた後、不正な購買取引に使用されました。

原因: この会社では、不必要かつ法外な量の個人情報を長期にわたって収集し、旧式の暗号化テクノロジーを使用して保管していたということです。ハッカーは、安全対策が施されていない無線接続を使用して、ディスカウント業者の中央データベースへアクセスしたと思われます。この会社はその後、支払に関する業界標準に違反していたことがわかりました。

損害: 当時、そのケースでは最大規模のセキュリティー侵害と報じられ、メディアに広く取り上げられました。訴訟、巨額の罰金、復旧のコストに加えて、失われた評判など、その他の間接的なコストは計り知れません。

教訓: 脅威とテクノロジーは変化し続けており、それまでは十分だと思っていたセキュリティー保護機能もいずれ古くなる可能性があるため、インフラストラクチャーおよび情報のリスクを定期的に再評価する必要があります。

実例を基に構成したものです。記載されている事実および損害は、実際とは異なる場合があります。*公表されている財務情報、公開されている記事を基にしています。*

ステップ 3: 巧妙なサイバー攻撃という不可避の事態への対応を準備する

セキュリティーに関するポリシー、手順、テクノロジーを可能な限り導入したら、次は、セキュリティー侵害が発生した場合の対処法を検討します。実際、あるアナリストが述べたように、「ほとんどの大企業のセキュリティー管理者や情報セキュリティー責任者は、セキュリティー侵害を受ける可能性の問題ではなく、いつ受けるのかという問題であると受け止めています」[5]

詳細かつ組織的な対応計画を策定する

インシデントへの対応を管理するには、組織全体で統一されたポリシーとプロセスが必要です。既に計画を導入している場合、定期的に計画をテストしてその有効性を確認することが重要です。

インシデント対応計画には、攻撃を阻止する方法、何が被害を受けたのかを特定する方法 (被害を受けた場合)、財務および評判に対する影響を測定する方法を明記する必要があります。また、メディア、従業員、情報が漏えいした可能性のある個人に危害の実状を伝えるためのガイドラインも提供する必要があります。

迅速な対応に必要なリソースやツールへのアクセスを確保する

攻撃の解決に時間がかかるほど、損害は大きくなり、コストも高くつく可能性があります。さらに、評判に関するリスクについて IBM が最近実施した調査では、回答者のシニア・エグゼクティブの約 78 パーセントが、Web サイトの停止など比較的軽微なインシデントからは半年足らずで回復すると述べています。しかし、サイバー犯罪によって評判に傷がつくと回復には長い時間がかかります。ひとつには、問題が完全に解決したということを信じてもらう方が困難な場合があるためです。[6]

セキュリティー・インシデントへの積極的な対応と調査に必要なリソースやスキルを確保することが、インシデントの影響を軽減するための鍵となります。

セキュリティー・インシデントに積極的に対応し、調査に必要なリソースやスキルを確保することが、インシデントの影響を軽減するための鍵となることは明らかです。ビジネスを行う上で評判が重要であり、事業の性質上サイバー攻撃に対するリスクが高いといえる場合、継続的に脅威を監視し管理することをお勧めします。このアプローチでは、防御を強化し、インシデントへの対応を自動化し、問題発生時には証跡から原因を迅速に追及し、法的な対応を可能にするフォレンジック分析を広範な脅威にわたって実施するテクノロジーを使用します。

一貫性のあるアプローチで、組織全体に責任を割り当てる

ほとんどすべての組織がいつかは何らか形で巧妙なサイバー攻撃に見舞われる可能性があるという事実を認めましょう。だれが何をする必要があるのか、どのようにして全員が情報を共有するのかを、インシデント対応計画に必ず明記してください。企業全体の連携が、効果的な検出、復旧、封じ込めの鍵となります。関連する各従業員に役割を割り当て、それぞれ何をするべきかを理解していることが重要です。各利害関係者がどの手順を担当するかを決定してください。各自で担当分野の準備を整えることで、巧妙なセキュリティー攻撃の発生を減らし、被害を限定的なものにできます。

決済代行業者で主要事業へのセキュリティー侵害が発生し、1 億 3,000 万人の顧客に影響

推定コスト: 最大 5 億ドル (約 500 億円)

被害者: 決済代行業者

被害状況: 顧客約 1 億 3,000 万人分のクレジット・カード、デビット・カードの番号が支払処理システムから盗まれ、不正な取引が行われました。

原因: 悪意のあるソフトウェアが処理システムに仕掛けられ、そのソフトウェアを使用して、取引承認プロセスでの処理中に、暗号化されていない送信中の支払データが収集されたとみられています。カード・データには、カード番号、有効期限のほか、支払カード裏面の磁気ストライプに記録されている情報も一部含まれていました。

損害: 注目を浴びた大規模なセキュリティー侵害であり、メディアにも大々的に取り上げられました。この会社は、法的な判決、和解、諸費用など直接経費として 1 億 4,000 万ドル (約 140 億円) 以上を支払ったとされています。また、事件後 3 カ月で株式時価総額が約 5 億ドル (約 500 億円) 減少したということです。

教訓: 直接的かつ真摯な危機対応によって、顧客離れを最小限に抑えました。業界の規格協会からの情報を共有し利用することでセキュリティー体制を強化し、最終的には、失った市場価値を回復することができました。

実例を基に構成したものです。記載されている事実および損害は、実際とは異なる場合があります。*公表されている財務情報、公開されている記事を基にしています。*

ステップ 4: セキュリティー意識の高い文化を促進および支援する

何千ものデバイスから、さまざまな公開 Web サービスを介して情報が流入する中、企業のネットワークを保護するという作業は、ますます複雑になる一方です。ある調査では、企業のスマートフォン・ユーザーの 91 パーセントが会社の電子メールに接続しているにもかかわらず、モバイル・セキュリティー・ソフトウェアのインストールを求められているのは 1/3 に過ぎないと報告されています。[7] このような環境では、犯罪者に限らずだれもが簡単にアクセスできます。

組織全体でリスク意識の高い文化を構築および支援する

企業のセキュリティーという使命を技術スタッフとそのマシンから、企業内の全従業員、取引先のすべての人々にまで広げる必要があります。だれもがセキュリティー侵害をもたらす可能性があるため、それぞれが解決策の一端を担う必要があります。つまり、成功するかどうかは、リスク意識の高い文化の促進と支援にかかっているといえ、セキュリティーの重要性が、企業のあらゆるレベルですべての意思決定と手順に反映されていなければなりません。外出時にはドアに鍵を掛ける – データに関する安全手順もこのように習慣化する必要があります。

するべきことを各従業員に周知する

企業の文化を変革するプロセスは、非常に困難な場合があります。しかし、各従業員にセキュリティー強化の重要性を伝え、セキュリティー上の問題をどのように認識して報告するかを周知できるようにすることから始めると、正しい方向に進むことができます。

セキュリティーの必須条件

IBM では常に、ビジネスを円滑に実行しながらも必要なリスク管理を可能にする方法を見いだそうとしています。総合的な対策として、テクノロジー、プロセス、ポリシーをご提供しています。それらを支える「セキュリティーへの取り組み最重要 10 カ条」を以下に挙げます。

1. リスク意識の高い文化を構築する – ずさんなセキュリティーを企業全体で一切容認しません。管理職は、この変革をまさにトップダウンで断固として押し進めると同時に、進行状況を追跡するためのツールを実装する必要があります。

2. インシデントを管理して対応する – インテリジェントなアナリティクスおよび自動化機能の実装など、企業全体の取り組みが不可欠です。統合自動化システムを構築することで、動作を監視し、迅速に対応することができます。

3. ワークプレースを防御する – 各ワークステーション、ラップトップ、スマートフォンから悪意のある攻撃が始まる可能性があります。各デバイスの設定は、すべて一元管理を行い、確実に適用する必要があります。また、企業内のデータ・ストリームを分類し、特定の範囲のユーザーのみにルーティングする必要があります。

4. セキュリティーを考慮して設計を行う – 情報システムの最大の脆弱性の 1 つは、サービスの実装後に、セキュリティーを追加することから生じます。唯一の解決策は、最初からセキュリティーを組み込み、定期的なテストを実行してコンプライアンスを追跡することです。

5. 常にクリーンな状態を維持する – 多種多様なソフトウェアの更新を管理することは、ほとんど不可能です。セキュリティー対策を講じている安全なシステムでは、管理者はすべての実行プログラムを追跡し、最新の状態であることを確信し、更新やパッチがリリースされたらインストールできるようなシステムを整備することができます。

6. ネットワーク・アクセスを制御する – 監視しているアクセス・ポイントを経由して登録したデータを送信する企業は、はるかに容易にマルウェアを特定し、分離することができます。

7. クラウドのセキュリティーを確保する – IT サービスを一部でもクラウド環境に移行すると、他の多くの企業との距離が近くなります。中には詐欺が含まれている可能性もあります。そのため、他社から隔離し、脅威の可能性を監視するツールや手順の確保が重要です。

8. 周囲の安全を確認する – セキュリティーを重視するという文化を企業の外にも広げ、請負業者やサプライヤー間のベスト・プラクティスを確立する必要があります。かつて、品質管理を促進する際に採用されたのもこうしたプロセスです。

9. 企業の重要な資産を保護する – 各企業は、重要な資産を科学的データ、技術的データ、機密文書、顧客の個人情報など、適切に整理し、特別に取り扱うようにする必要があります。重要な資産には企業の存続がかかっていると考え、保護、追跡、暗号化を行う必要があります。

10. 従業員を追跡する – 「ID ライフサイクル」を適切に管理していない企業は、暗闇で業務を行っているのも同然といえ、侵入に対して脆弱である可能性があります。こうしたリスクに対処するには、従業員の身分を確認し、アクセス権を管理し、離職後は速やかにアクセス権を取り消す、周到なシステムが必要です。

図 1. ***セキュリティーへの取り組み最重要 10 カ条****: 組織全体で理解、実践される一貫した安全対策を整備するような、柔軟性とイノベーションを考慮したバランスの取れたセキュリティー・プログラムを策定することが、成功につながります。*

今すぐ始めましょう、被害者になる前に

IBM X-Force は、2012 年の上半期に 4,400 件余りの新たなセキュリティーの脆弱性を報告しました。この傾向が続くとすれば、予測される脆弱性の総数は、2010 年の約 9,000 件を上回ります。さらに、2012 年の上半期における、パッチが適用されていない脆弱性の割合は、2008 年以降で最も高くなっています。

多くの組織は、パスワードや個人データの流出によって生じる予期せぬ影響への対処を迫られています。また、これらの攻撃はますます巧妙になってきています。例えば、攻撃者は公開されているソーシャル・メディア・サイトから重要な個人データを取得し、巧妙なソーシャル・エンジニアリングを駆使して対象のアカウントへの無制限アクセスを得ることができます。ユーザーのボイス・メールを転送するようモバイル・プロバイダーに働きかけることによって、2 要素認証を回避した例もあります。つまり、企業が被害者になるかどうかという問題ではなく、いつ被害者になるかという問題なのです。実際、シニア・エグゼクティブの 61 パーセントが、企業の評判への最大の脅威はデータ漏えい、データ盗難、サイバー犯罪であると述べています (IBM が実施した評判に関するリスクと IT に関する調査による)。[8]

企業が被害者になるかどうかという問題ではなく、いつ被害者になるかという問題なのです。

IBM にお任せください

巧妙なセキュリティー攻撃への対策を検討するのは非常に負荷の大きな作業です。話し合うべきこと、検討しなければならないこと、心配なことが数多くあります。しかし、少しずつ進めればよいのです。自社だけで行う必要もありません。

IBM セキュリティー・サービスのコンサルタントが、ほとんどすべての領域にわたって、セキュリティー戦略の計画、実装、管理をお手伝いします。IBM セキュリティー・サービスのコンサルタントは、公共部門と民間部門において、企業のセキュリティー指導およびコンサルティング、政府の調査部門、法執行機関、研究開発などの仕事に携わっているセキュリティーのシニア・プロフェッショナルです。

さらに、IBM は 1995 年以降、マネージド・セキュリティー・サービスで説明責任、信頼性、および保護の標準を確立するお手伝いをしてきました。これらのサービスは、セキュリティー業務の監視と管理を IBM にアウトソーシングすることによって、お客様の情報セキュリティー体制の強化、総所有コストの削減を図るとともに、コンプライアンスを示すことを目的としています。デバイスの種類やベンダーに関係なく、年中無休で、または必要に応じて、お客様をご支援します。

IBM マネージド・セキュリティー・サービスでは、お客様が必要とするセキュリティー関連のインテリジェンス、専門知識、ツール、インフラストラクチャーを提供し、24 時間体制で、しかも、社内のセキュリティー・リソースの何分の 1 かのコストでお客様の情報資産をインターネット攻撃から保護できる場合もあります。

詳細情報

IBM セキュリティー・サービスは、お客様がコストを削減しながら、高度なセキュリティー脅威からの保護を強化できるようご支援します。詳細については、日本 IBM の営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。**ibm.com**/services/jp/ja/it-services/jp-sc-igs-security-privacy.html

日本アイ・ビー・エム株式会社
〒103-8510
東京都中央区日本橋箱崎町19-21

IBM のホームページは以下をご覧ください:
ibm.com/jp/

[1] 米調査会社ポネモン・インスティテュート、「*The Impact of Cybercrime on Business: Studies of IT practitioners in the United States, United Kingdom, Germany, Hong Kong and Brazil sponsored by Check Point Software Technologies*」、2012 年 5 月
[2] 2012 年上半期 IBM X-Force トレンド＆リスク・レポート、2012 年 9 月
[3] 上記の注 1 を参照。
[4] 「*Security Intelligence Can Deliver Value Beyond Expectations And Needs To Be Prioritized*」(IBM Global Technology Services の委託によりフォレスター・コンサルティングによって実施された調査)、2012 年 5 月
[5] ブログの投稿: 「*Okay, Breaches Are Inevitable: So Now What Do We Do?*」、Paula Musich、Current Analysis、2012 年 7 月 20 日
[6] IBM Global Technology Services、Reputational risk and IT、2012 年 9 月
[7] カスペルスキー・ラボ、Enterprise Mobile Security Survey、2010 年 12 月
[8] 上記の注 6 を参照。

* 高度で執拗かつ継続的な標的型攻撃
** 1 ドル = 100円換算 (以下同様)

Please Recycle

SEW03029-JPJA-00