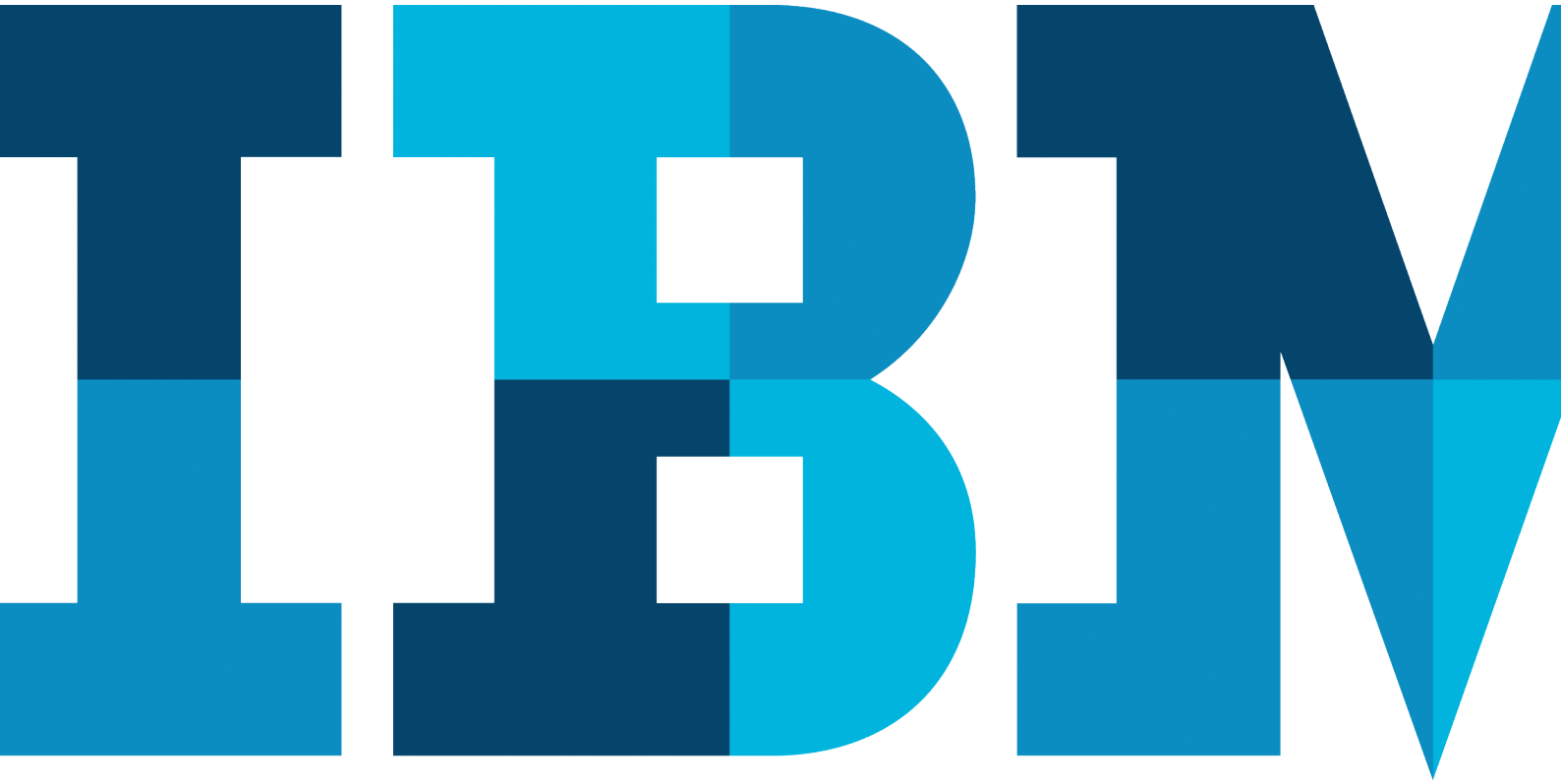
IBM Security
ソート・リーダーシップ・ホワイト・ペーパー

2014 年 10 月

CEO のためのセキュリティー指針

リスク意識が高い企業の 5 つの基本的資質を探る



IBM

目次

近年、ますます多くの企業が自社のコンピューター・システムで大規模なデータ障害が発生したことを明らかにしています。その多くは有名企業であり、攻撃者によって大量の最重要データと顧客情報が盗まれました。低リスクで「うまみ」が大きいと言われているサイバー犯罪が、こうした被害企業の数を一段と増加させています。このような攻撃が頻発してその影響が大きくなったことで、セキュリティーは企業の経営幹部が優先的に取り組むべき課題になっています。

問題はどれほど深刻なのでしょうか? サイバー犯罪による年間損害額は全体で 4000 億ドル (1 ドル 100 円換算で約 40 兆円) を超えると見積もられ、この数字が国民所得に匹敵する国も少なくありません。[1] 米国単独でも、2012 年半ばから 2013 年までに報告されたサイバー攻撃の件数は 150 万件にのぼりました。[2] 攻撃者はますます巧妙になり、昨年には 5 億件を超える個人識別情報レコードの盗難を許してしまいました。[3] さらにこうしたセキュリティー侵害によって、年間のデータ障害対策コストが 15% 増加し、現在ではインシデントごとの総額が 350 万ドル (約 3.5 億円) を超えています。[4] さらに、顧客離れの増加、企業評価の低下、および信用の失墜といった損害も伴います。

CEO の基本的な職責の 1 つに、事業の安全性を確保することがあります。とはいえ、サイバー・セキュリティーに対しては何に重点を置くべきなのでしょうか? そこで、強固なセキュリティー体制を維持するための鍵を握る 5 つの対策分野を提案します。

1. 全従業員のセキュリティー IQ の向上

鎖の強度はその最も弱いつなぎ目によって決まる、と言われています。ある調査では、セキュリティー・インシデントの 60% が従業員のミスと社内システムの誤作動が原因であると示しています。[4] 社内の一部の従業員のみが正しく行動しているだけでは不十分です。社内の全員がリスク認識を持つ社内風土を構築し、維持することが必要です。常に新たな脅威と危険が生じているため、教育は継続的に実施する必要があります。

ベンダーや契約社員などの社外の関係者も含めた、全従業員の教育を実施し、彼らの学習成果を追跡調査する必要もあります。また、研修プログラムについてテストを実施することも必要です。コース修了を認定するための従来の試験と、攻撃者自身が仕掛ける攻撃に似せた、定期的な組織的プローブ調査の両方を行います。

セキュリティー・ポリシーと従業員教育の策定

問題: あるヨーロッパの銀行グループが、財務安定性の向上、運用リスクの削減、既存のセキュリティー・プログラムの拡張を求めていました。

解決策: IBM コンサルタントが Basel II/III に則した一貫性のあるセキュリティー・ポリシーを定め、従業員の意識向上プログラムの作成を支援しました。

従業員の意識向上プログラムによる利点:
- **統一セキュリティー・プログラムによるリスクの削減。**
- **従業員による、より効果的なセキュリティー・ポリシーの実施。**

例えば、全社的な「スピアフィッシング」キャンペーンの実施を検討してください。正規 e-メールを装い、理論上の「感染」サイトへと誘導するリンクを従業員に送信します。そのサイトへ誘導されると、コンピューターのオペレーティング・システムが乗っ取られ、データベースと最重要資産にアクセスする抜け道が形成されたことになります。誰がこの罠にかかり、誰がかからなかったかを確認してください。そしてそれを教訓にしてください。IBM では、セキュリティー研修を修了していない従業員は、研修を修了した従業員の 2 倍の確率で感染した e-メールの罠にかかってしまうことを確認しています。

全従業員を「訓練し、テストし、そして罠にかけて」みましょう。

2. より迅速な対応のための備え

大手企業へのサイバー攻撃が近年報道を賑わせていることを考えれば、データ侵害は発生するものと想定して対策を行うことが必要です。発生後にいかに対処するかが鍵を握っており、特に対応速度は非常に重要です。巧妙な攻撃は表面上何の「徴候」も表さず、こっそりと長期間にわたって壊滅的な損害を与える可能性があります。攻撃の解決が長引くほど、損害額は増大します。残念なことに、一部の企業では攻撃されたことに気付くのにも何カ月もかかっています。

迅速対応チームを指導するための計画の立案

問題: ある大手の心臓治療センターが、医療保険の相互運用性と説明責任に関する法律 (HIPAA) といった固有の要件にも準拠した対応計画を必要としていました。

解決策: IBM コンサルタントが、サイバー・セキュリティー・インシデントに対処するインシデント対応計画を策定しました。

インシデント対応計画による利点:
- **セキュリティー・インシデントへの迅速な対応を確立するための青写真を作成。**
- **インシデント自体への対処だけでなく、セキュリティー・インシデントの影響を受けるすべての利害関係者への対処についても計画を作成。**

この後は、予防対策を開始します。具体的には、インシデント対応計画、その計画を検証するための事前想定訓練、およびインフラストラクチャー内に既に存在する隠れたマルウェアや攻撃を未然に特定するための目標設定型の取り組みです。攻撃を特定して防御するために必要なセキュリティー・データを収集するには、インフラストラクチャー全体で何が発生しているかをモニターする必要があります。

さらに、直接的にセキュリティー侵害を軽減するだけでなく、危機のあらゆる側面に対処できるよう十分に訓練された迅速対応チームも必要です。このチームは、IT、人事、法務、規制管理、販売、広報などの部門から選抜された常設の中核グループであり、セキュリティー・インシデントの影響を受けるすべての利害関係者に対処できます。シミュレート攻撃を定期的に行うことで、このチームを訓練する必要があります。

結論: サイバー攻撃に対応するための計画と実施訓練が必要です。

3. BYOD の保護 – 従業員が新たなセキュリティー境界

標準のワークステーションやラップトップ以外の個人所有のスマートフォン、タブレットなどのデバイスが、任意のツールとして日常的に多用されつつあるのは明らかです。これには専門家も例外ではなく、業務に使用しているケースが数多く見受けられます。わざわざ購入してでも個人所有デバイスを使用したいと考えるのです。

こうした個人向けテクノロジーの利用の急増にともない、個人所有端末の業務使用 (bring-your-own-device: 以下 BYOD) プログラムを機能させるために組織の保護が求められます。ガバナンス、ポリシー、および全従業員の教育はすべて、この分野で役割を果たします。従業員が教育されず、使用方法に関するポリシーが整備されていなければ、利用可能な最高のテクノロジー・ソリューションは機能しません。

どのような使用方法が許され、あるいは許されないのか、および会社が何を行うか、あるいは行わないのかを定義することは重要であり、時間を費やす価値があります。また、会社全体のセキュリティーを実現するための業務活動指針を従業員に通告し、従わせることも重要です。

コンテナー化 (個人所有デバイス上の企業データを隔離する手法) は BYOD で重要なツールとなっています。コンテナー化を行うことで、企業は最重要情報を保護でき、従業員は勤務先である企業が、自分が所有する端末内のプライベートな領域に納められている個人情報などにアクセスしないという確信を得られます。

BYOD のリスクの削減

問題: あるテクノロジー・プロバイダーが、従業員所有のデバイスをより柔軟にサポートできるよう希望しています。既存のポリシーでは、検査および認定が済んでいないデバイス・タイプのネットワーク・アクセスはブロックされます。

解決策: その会社では、Fiberlink, an IBM company, 製の MaaS360 を使用して、会社支給のものか BYOD プログラムの一環かを問わず、自社に入るすべてのモバイル・デバイスの識別、制御、および保護を行うようになりました。

生じた利点:
- **企業のネットワークおよびデータのセキュリティーの強化。**
- **柔軟性を高めた BYOD ポリシーによる従業員の満足度の向上。**

4.「企業の最重要資産」の保護

最重要データ (いわゆる「企業の最重要資産」) は、量としてはわずかでありながら、企業の生き残りと成功に不可欠なデータの最重要部分です。これには、企業秘密、知的財産、機密のビジネス計画と通信内容などのプロプラエタリー・データが含まれます。データ全体の 2% に満たないながらも、その会社の市場価値の 70% を占めることもあります。[5] データの損失は金銭的な損害につながりますが、最重要資産の喪失は事業そのものの喪失につながる可能性があります。

にもかかわらず、多くの企業にはそれらの最重要資産を保護するプログラムが用意されていません。CEO なら、自社にそうしたプログラムが備わっていることを確認する必要があります。企業の最重要資産を特定し、分類していますか? その場合、最重要資産はどこにありますか? どのデバイスまたはデータベース上にありますか? その最重要データを優先順位付けし、喪失のリスクという点で評価していますか?

最重要情報の保護

問題: 中東のある政府機関において、最重要機密情報を特定し、分類する必要が生じました。さらに、その政府機関はデータの価値を見極め、データに対して適切なセキュリティー管理を適用することも希望しました。

解決策: IBM コンサルタントがその政府機関に協力して、データベースと最重要情報を保護するためのデータのセキュリティー戦略とセキュリティー・アーキテクチャーを構築しました。

生じた利点:
- **最重要情報が特定、分析され、その機密性、セキュリティー脆弱性の評価を実施。**
- **パフォーマンスと可用性を損なうことなく、最重要情報保護のためのロードマップを取得。**

先ほどの質問に回答を終えた後、データのセキュリティー確保と保護を担当する管理者を決定して、その職責を与える必要があります。企業の最重要資産は非常に重要であるため、その保護には十分な時間と多くのテクノロジーを費やす覚悟が必要です。

5. セキュリティー・インテリジェンスの活用

膨大な関連データを保管して分析し、セキュリティー・イベントを検出することは (ましてや予測することは) 非常に困難な作業です。そのデータには、ファイアウォール、e-メール、サーバーなどの従来のソースからのイベントだけでなく、モバイル・ユーザーやクラウド・サービスなどの新たな分野からのイベントも日々数十億件という単位で含まれていくと考えられます。このデータを手作業で調べて、疑わしい動作の徴候を見つけることは、単純に不可能です。こうした作業では、コストがかかるだけでなく、企業は「今後何が起こるか」ではなく「何が起こったか」を確認するだけで精一杯です。

ビッグ・データ・アナリティクス・ツールは、このすべてを変えています。ビジネス・データにアナリティクスを適用することで新たな洞察が得られ、組織の変革を推進する力になります。アナリティクスをセキュリティー・データに適用した場合も、同様に変革を起こす力 (セキュリティー・インテリジェンスおよびセキュリティー対応における「槍の先端」すなわち突破口) になり得ます。アナリティクスにより、インフラストラクチャーのセキュリティー状態に関する情報を自動かつリアルタイムで収集し、どのような状況に置かれているかを認識できるようになるため、攻撃の連鎖を断ち切ることが可能になります。

組織を保護するための拡張モニタリングとアナリティクスの使用

問題: 南アメリカのある銀行で、自行のすべてのシステムとアプリケーションから収集されるデータを統合して、セキュリティー体制を改善する必要が生じました。

解決策: IBM Security QRadar Log Manager および IBM Security QRadar SIEM を使用して信頼性の高い保護を実現し、予測分析を行い、高度な脅威を阻止します。

IBM Security QRadar 導入による利点:
- **優れた脅威検出および企業アクティビティーの多彩な表示。**
- **セキュリティー・イベントの大幅な減少。**
- **調査時間を 99% 短縮。**
- **異常の即時検出と通知。**

インテリジェント・アナリティクスと自動対応機能を実装するための全社的な取り組みが不可欠です。自動化された統一システムを構築することで、企業は自社の業務をモニターして、迅速に対応できます。

最後に、強固なセキュリティー体制を維持するための万能のツールはありませんが、すべての CEO が実行できる共通アクションが 1 つあります。セキュリティーは組織に不可欠であり、組織の中では全員に果たすべき役割があることを、言葉と行動で訴えかけることです。繰り返しになりますが、IBM が推奨する 5 つの基本方針に基づいて行動することを、組織のセキュリティー戦略の中核に据えてください。これらの基本方針に重点を置くことで、企業を保護し、より俊敏に危険から身をかわす動きができるようになります。「物事を済ませてしまうこと」と「物事を安全に実行すること」は違います。

結論

IBM には、セキュリティー分野での豊富な経験と、極めて複雑な企業環境のお客様でも効果的な連携を続けてきた長い歴史があり、お客様のブランドと最重要データの保護を支援するという点で、他社とは違う弊社固有の資質を備えています。IBM は、比類のないグローバル・カバレッジとセキュリティー意識を達成しており、数千人ものアナリストとデリバリー・スペシャリストが日々お客様にセキュリティー・サービスを提供しています。IBM は、セキュリティー・リサーチ・センターを 10 カ所、セキュリティー・オペレーション・センターを 10 カ所、セキュリティー開発ラボを 15 カ所備えています。保有するセキュリティーの特許も 1,000 件を超えています。さらに、数千にものぼる全世界のお客様のために、数万台ものセキュリティー装置を管理しています。弊社のシステムは、133 カ国にわたるお客様のために毎日 150 億件ものネットワーク・イベントをモニターしています。

詳細情報

IBM Security について詳しくは、IBM 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**/security/jp

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

[1] Center for Strategic & International Studies、インテル、2014 年。
[2] IBM サイバー・インデックス・レポート、2013 年。
[3] IBM X-Force 脅威インテリジェンス 四半期報告書、2014 年第 1 四半期
[4] Cost of a Data Breach Study、Ponemon Institute、2014 年。
[5] Commission of the Theft of American Intellectual Property Report、2013 年。

WGW03081-JPJA-00