IBM Center for Applied Insights

SecurityIntelligence

Executive Series

CIO のための実践すべきセキュリティー対策項目

―確信を持ってイノベーションを採り入れるために―

IBM

日々新しい情報が次々と企業に押し寄せ、最新の分析およびスマートな意思決定の必要性が急速に高まっています。社員、お客様、取引先は、数多くのテクノロジーを介して、かつてないほど強固に連携しています。その一方で、このように不規則に広がる無数のネットワークは、恐ろしいセキュリティー上の課題をはらんでいます。ネットワークの複雑さは目もくらむほどで、常に攻撃対象になる可能性があります。CIO は、危機意識を高めるだけでなく、次のような疑問にも取り組んでいます。このように高度にネットワーク化 された環境でも強固なセキュリティーを確保できるでしょうか? 確かに確保できます。ただし、プロセスおよび考え方を根本的に変えることが必要です。IBM は、社内向けに独自の戦略を実装し、セキュリティー・インテリジェンスを実現するために必要な 10 の必須事項を策定しました。

日の出を迎えたニューヨークで、一人の営業部長はベッドから起き出し、スマートフォンのスイッチを入れ、マレーシアで大きなビジネス・チャンスが浮上していることに気付きました。このニュースがきっかけとなって、次々とコミュニケーションがつながっていきます。朝食前に、グローバル・チームの 6 人のメンバーが電話会議を行っています。その 1 人はストックホルムから Skype 経由で参加しています。3 人の取引先は、携帯電話で参加しています。1 日中、E メールが世界中を縦横無尽に巡っています。その約半数は、企業ネットワークを利用し、その他は Gmail および Yahoo を利用しています。ニューヨークでは、夕方までに取引が終了します。それ以降の時間は、数名の参加者が LinkedIn で親交を図っています。

91%

企業のスマートフォン・ユーザーの 91% は企業メールに接続しますが、モバイル・セキュリティー・ソフトウェアの導入を求められているのは 3 人に 1 人に過ぎないことが報告されています。

出典: Kaspersky Labs
http://usa.kaspersky.com/sites/usa.kaspersky.com/files/Enterprise%20Mobile%20Survey.pdf

今日、マネージャーは知力と何ギガバイトものデータを瞬時に結集し、情報に基づく決定をより迅速に行える ことは明白です。その一方で、相互接続されたネットワークの強みであるスピードと開放性、および世界中のどこでも容易にアクセスできることは、無数の脆弱性をもたらします。また、何千ものデバイスや多数の公共の Web ベース・サービスから情報が押し寄せているため、企業のネットワーク・セキュリティーを保護する作業はこれまでとは比べものにならないほど複雑化しています。Kaspersky Labs による調査では、企業のスマートフォン・ユーザーの 91% は企業メールに接続しますが、モバイル・セキュリティー・ソフトウェアの導入を求められているのは 3 人に 1 人に過ぎないことが報告されています。そのような環境では、すべての関係者がいとも簡単にアクセスできます。多くの場合、その中には犯罪集団も含まれています。

現在、犯罪集団にとって、インターネット接続した PC やモバイル・デバイスは一等地の不動産のようなものです。検出が困難なマルウェアを使ってデバイスを感染させることにより、基地を拡張します。窃盗団にとって、企業ネットワークは、パスワード、ユーザー ID、企業秘密、個人情報など、デジタルの宝の山のようです。また、デジタル窃盗団は、政府省庁から通信ネット

ワークまで、戦略的資産も標的にします。その中は、業務を中断させようと躍起になるものもあります。Gartner の予測によると、一般ユーザー PC の 20 から 30% は、犯罪操作の基盤として使用できるボットネットおよびマルウェアによって危険にさらされています。個人所有のデバイスを社内で使用することを考慮している多くの会社にとって、感染の可能性はまさに現実的な課題となっています。

一般ユーザー PC の 20 から 30%

がマルウェアをホストし、犯罪者の手助けをしています。

出典: http://www.computerweekly.com/opinion/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the-workplace

1 台の感染したコンピューターが、深刻な損害をもたらす可能性があります。これまでで最も大規模な例の 1 つは Stuxnet です。これは、製造業のソフトウェアおよび設備に損害を与えるように設計された、非常に精巧なワームです。2009 年の春に、ワームは多くのマシンに拡散し始め、そのほとんどはイラン国内で発生しました。何者かが汚染された USB メモリー・ドライブを介してワームを導入したものと思われます。

Siemens ソフトウェア・プログラムを導入したマシンを標的として開発されたワームは、数多くの製造業システムに大損害を与えました。

企業のセキュリティー・リーダーにとっての教訓は明確です。ワームがイランや他国の厳重に保護された製造業に侵入できるとしたら、社員がTwitter、Facebook、E メール、および Skype を業務に活用し世界中を駆け回る環境で「隙間」を見つけることはどれほど容易でしょうか。その上、1 つのワームが製造業の設備機能を停止できるとしたら、その惨事の間に、他のワームがサプライ・チェーンを遮断し、データを転送し、さらには配電網に損傷を与えることさえも可能ではありませんか? それは可能です。

これらの増大していく課題に立ち向かうため、企業には**新しいタイプのセキュリティー・リーダーが必要です**。当然、無数のテクノロジーの脅威だけでなく、戦略的な課題にも対応する必要があります。どの情報を広範囲に共有する必要がありますか? 誰が特定の貴重な情報にアクセスする必要がありますか。また、貴重な情報をどのように保護しますか? それだけでなく、技術的および戦略的な課題は、目もくらむほど複雑化しています。これらに対応するため、同じくらい複雑なソリューションを採用しようとする衝動に駆られるかもしれませんが、先見の明のある経営陣は、そのようにエスカレートしていくことに同調せず、費用の負担も大きくなり、最終的には無駄な労力であることに気付いています。

唯一の答えは、企業の運営方法を根本から変化させることです。まず最初に、技術スタッフとそのマシンだけでなく、企業の全社員やすべての取引先に至るまで、**企業セキュリティー確保という使命を拡大**します。これは適合の問題に過ぎません。各人がセキュリティー違反の責任を負う可能性があるため、それぞれが対策を実行する役割を担う必要があるのです。結局のところ、関係者全員にセキュリティーに対する強固で持続的な認識を促せるかどうか? で成功の可否が決まります。**つまり、リスク認識の文化です**。

リスク認識の文化とは、単に最新のテクノロジーを活用することだけや、過去の成功事例をまねすることだけにとどまりません。

それは新しい考え方です。つまり、セキュリティーに対する実践的なアプローチにより、企業のあらゆるレベルに、あらゆる決定および手順を伝達することを意味します。経営幹部からインターンまで、だれもが情報の取り扱い方法を見直す必要があるということです。そのような文化では、データ取り扱いの安全な手順は、シート・ベルトを締めたり、安全な場所にマッチを保管したりすることと同じくらい習慣的なものとなります。

それは新しい考え方です。つまり、セキュリティーに対する実践的なアプローチにより、企業のあらゆるレベルに、あらゆる決定および手順を伝達することを意味します。

これは先延ばしにすべき決断ではありません。企業セキュリティーは、転換点に急速に近づいています。さまざまな要素を考慮してください。犯罪集団で活動しているのは、もはや素人ではなく、プロの犯罪者です。そのことが脅威に拍車を掛けています。同時に、企業は、運営、マーケティング、営業、および顧客サービスに関する大量のデータを幅広く配布することより、従業員の生産性を高め、「やる気」を与えました。このことはぜい弱性に拍車を掛けています。また、現在、企業のビジネスのほぼ全体がデジタルを使って管理されているため、侵入の結果として会社全体が動揺する可能性があります。つまり、窃盗団には高い技術力があり、無数のデジタルのドアおよび窓から侵入できるということです。その中に隠されているものは値段が付けられないほど貴重です。

セキュリティーとは危険な賭けであり、その道のりは困難に満ち、入り組んでいるように思えます。現在、セキュリティー製品やサービスは市場に十分出回っていますが、最近のセキュリティー危機またはコンプライアンスに関する報道を見るにつけ、IBM のお客様は多くの場合、セキュリティー市場に失望していると語っています。多くの人は、セキュリティー対策として、どこから手を付けて、何を信頼すればよいかわかりません。多くの場合、セキュリティーおよびコンプライアンスを、定量化できない価値を伴う投資、疑わしい ROI、高速道路に減速バンプを設置するよう要請するようなものなどと表現します。こうした混乱の結果として、優柔不断な態度をとることになり、さらに悪いことに恐怖心からイノベーションをあきらめるという決断へと至ります。

企業を保護することは、骨の折れる仕事で、決して終わりのない作業であることは、紛れもない事実です。その上、文化を変えることは困難です。しかし、この作業は不可欠です。強固なセキュリティー対策は、事業を継続するために必要なコストであり、その実現は手の届くところにあるのです。

IBM では、イノベーションの前進とリスク・コントロール実施のバランスを見出すよう絶えず努めています。
企業の包括的なセキュリティー対策には、テクノロジー、プロセスおよびポリシーの指標が含まれています。それには、10 の不可欠な実践すべき項目があります。
今後、IBM はそれらについて詳しく説明する一連のホワイト・ペーパーを配布します。このホワイト・ペーパーでは、簡単な要約を以下に示します。

セキュリティーの必須項目

1. リスク認識の文化の構築

考え方は単純です。だれでも疑わしい添付ファイルをクリックしたとか、スマートフォンにセキュリティー・パッチをインストールしていないといった理由で、企業を感染させる可能性があります。そのため、セキュリティーが確保された企業にするための取り組みには、すべての人が関与する必要があります。リスク認識の文化の構築には、リスクおよび目標を設定し、広く浸透させることも含みます。しかし、重要な変化は文化的なものです。子供が道路に走り出しているのに、携帯電話で大声で話し続ける親を見たとき、多くの人が経験する無条件反射的な反応を想像してください。それは恐怖です。それと同様の非許容性が企業レベルで存在する必要があります。同僚がセキュリティーに関して不注意な場合には、同様の反応を示す必要があります。当然ながら、この変化をまさにトップダウン方式で絶え間なく推し進めつつ、進捗を管理するためのツールを導入する必要があります。

2. 問題への対処および対応

2 つの類似するセキュリティーの問題が、1 件はブラジルで、もう 1 件はピッツバーグで発生したと想定します。これら 2 つには関連性がある可能性があります。しかし、それらを関連付けるために必要なセキュリティー・インテリジェンスがなければ、潜在的な問題を指摘する可能性がある重要なパターンは、気付かれずに終わってしまう場合があります。したがって、インテリジェントな分析機能および自動応答機能を実装するための企業規模の取り組みが不可欠です。自動化および統合化されたシステムを構築することにより、企業はその運用を監視して、迅速に対応できます。

3. ワークプレースの防御

サイバー犯罪者は、絶えず弱点を探っています。ワークステーション、ラップトップ、またはスマートフォンなど各デバイスにはそれぞれ、悪意のある攻撃を可能にする「隙間」があります。各デバイスの設定を個人または自主管理グループに任せてはなりません。それらはすべて、一元的な管理および対策が実施される必要があります。また、企業内のデータの流れは個人が持つ固有のリスク・プロファイルごとに分類され、該当するユーザー・グループにのみ送られる必要があります。全従業員を保護することは、混乱を克服し、信頼に変えることを意味します。

4. 設計段階でのセキュリティー

自動車会社がシート・ベルトまたはエアバッグのない車を製造し、恐怖や事故を経験した後に、付け加えた場合を想像してください。それは無分別であると同時に、法外な費用がかかることでしょう。同様に、情報システムにおける最大のぜい弱性の 1 つ (および費用の無駄使い) は、最初にサービスを実装し、後で思い付いたようにセキュリティーを追加することです。これに対し、唯一のソリューションは、最初からセキュリティーを組み込み、定期的な自動テストを実施してコンプライアンス遵守状況を追跡することです。これはコストの節約にもなります。セキュリティー機能をアプリケーションに組み込むために、余分に 60 ドルが必要だとすると、それを後で追加するには、最大で 100 倍の6,000ドルかかる可能性があります。

5. ソフトウェアの確実な管理

よくあることですが、多くの人は古いソフトウェア・プログラムをよく知っており、使い慣れているため、いつまでも使い続けます。しかし、寄せ集めのソフトウェアに対する更新を管理するのは、ほとんど不可能に近いことです。また、ソフトウェア企業は、古いプログラム用のパッチ作成を停止することがあります。サイバー犯罪者はこのことを熟知しています。セキュアなシステムでは、管理者は、実行中のすべてのプログラムを追跡して、それが最新であることを確信できます。また、更新およびパッチをリリースすると同時に導入するための包括的なシステムを整備できます。

6. ネットワーク・アクセスの制御

都市犯罪について考えてみましょう。都市のあらゆる車両が固有の無線タグを搭載し、それぞれがセンサーに従って限られた主要道路のみ走行するなら、治安維持ははるかに容易でしょう。同じことがデータについても言えます。登録済みデータを監視されているアクセス・ポイントを通過するように設定している企業は、マルウェアを発見して隔離するのがはるかに容易です。

7. クラウド内のセキュリティー

クラウド・コンピューティングは、効率性を大きく改善することを確約します。しかし、リスクを伴う可能性があります。企業が特定の IT サービスをクラウド・コンピューティングに移行している場合、クラウドの内部で他の多くのサービスと一緒にまとめられ、そこには詐欺師なども潜んでいることも考えられます。その意味で、クラウドは、一定の割合の宿泊客が感染病を患っているホテルに似ています。この環境で生き残るためには、宿泊客が自分を他者から隔離するための道具および手順を持ち、潜在的な脅威を監視する必要があります。

8. 周辺パトロール

例えば、契約社員がシステムへのアクセスを必要しているとしましょう。その担当者が正しいパスワードを持っていることをどのように確認できるでしょうか? パスワードをノートパッド上に残しておきますか? テキスト・メッセージで送信しますか? そのような行き当たりばったりの方法にはリスクがあります。企業のセキュリティー文化は、企業の壁を超えて広がり、取引先やサプライヤーとの間で成功事例を確立する必要があります。これは一世代前に、品質管理を実践していた頃と同様のプロセスです。そのロジックは変わりません。セキュリティーをエコシステム全体に浸透させる必要があります。注意不足から生じる破壊的な結果が、企業の全部門を混乱に導く可能性があります。

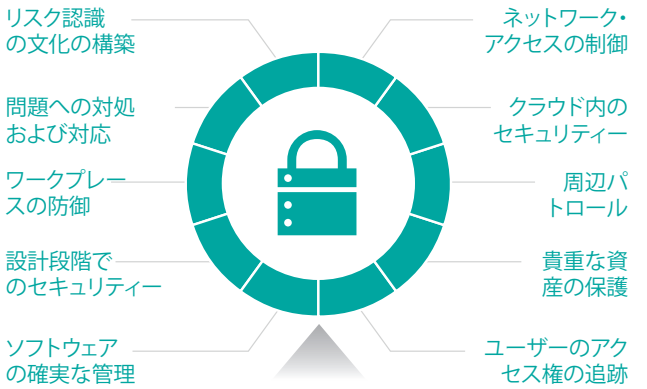
9. 貴重な資産の保護

収集品のどこかに、企業の重要な資産 (合併・買収に関係する文書や顧客の非公開の財務情報といった、科学的データや技術的データ) があるとします。各企業は、データの棚卸しを行う際に、重要なデータは特別な取り扱いをする必要があります。会社の存続に関わることを前提として、重要なデータは保護および追跡し、暗号化する必要があります。現実的に、データ漏洩が会社の存続を左右することもあります。

10. ユーザーのアクセス権の追跡

ある契約社員がフルタイムで雇われるとします。6 カ月経過し、昇進が決まります。1 年後、競合他社が突如としてその人物を引き抜きます。では、時間が経つにつれて、システムはその人物をどのように扱うでしょうか? 最初に、付与されているデータへのアクセス権を制限する必要があります。その後、最終的にその人物を切り捨てます。これは ID ライフサイクルの管理です。必要不可欠な項目です。ID ライフサイクルの管理を誤る企業は、暗闇で作業しているようなもので、侵入者に対してぜい弱である可能性があります。このリスクに対処するには、人物を識別し、その権限を管理し、離職と同時に取り消すといった、細部まで行き届いたシステムを実装する必要があります。

確信を持ってイノベーションを採り入れるためには?



リスク管理とイノベーション実現のバランス

会話への参加

追加の情報や詳細を確認したり、他のセキュリティー・リーダーと考えを共有したりするためには、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

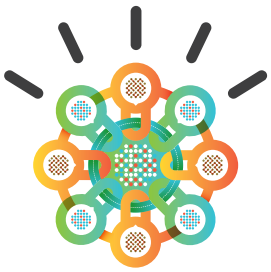
著者について

Kristin Lovejoy は、IBM Office of the CIO の IT リスク担当副社長です。連絡先は次のとおりです。

klovejoy@us.ibm.com

IBM Center for Applied Insights について

IBM Center for Applied Insights は、洞察に富む内容や分析的な専門知識を統合することにより、お客様が新しい価値を提供するための支援を行っています。この Center は、調査を実施し、実際的なガイダンスによって資産およびツールを構築して、組織を行動へと促しています。



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・ページはこちらからご覧になれます。
ibm.com/jp

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。

これらおよび他の IBM 商標に、この情報の最初に現れる個所で商標表示 (® または ™) が付されている場合、これらの表示は、この情報が公開された時点で、米国において、IBM が所有する登録商標またはコモン・ロー上の商標であることを示しています。このような商標は、その他の国においても登録商標またはコモン・ロー上の商標である可能性があります。

現時点での IBM の商標リストについては、次の Web サイトをご覧ください。
ibm.com/legal/copytrade.shtml

本書に記載の製品、プログラム、およびサービスが日本においては提供されていない場合があります。日本で利用可能な製品、プログラム、またはサービスについては、日本 IBM の営業担当員にお尋ねください。

© Copyright IBM Corporation 2012

Please Recycle

CIE03116-JPJA-00