緊急の対応が求められる IT セキュリティのモダナイズ

10 の理由と 10 の方法

目次

はじめに

現実に目を向けましょう。おそらく企業の多くが、自社のユーザーや IT リソースを守るためにできることをすべてやっていないのではないでしょうか。誰もが世間で話題になっているハッカーや脆弱性の悪用を認識しており、間違いなくそれらに対して懸念を抱いています。ところが、企業の限られたリソースを消費しているのはセキュリティだけではないのも事実です。そして実際には深刻な情報漏洩の被害を受けていないのも事実です。少なくとも現時点では…。

他の企業が身をもって学んでいるように、鍵となるのは、企業のセキュリティ戦略のための揺るぎない基盤ではなく、貴重な人材の能力なのです。企業のセキュリティ強化に目を向けるべき説得力のある理由とセキュリティ強化に向け大きな一歩を踏み出すために今すぐできることをご紹介します。これらは企業にとって朗報となるでしょう。

今すぐ IT セキュリティをモダナイズすべき 10 の理由

1.リスクを最低限に抑える：さらに効果的かつ包括的で広範囲にわたるセキュリティは、ユーザーや自社の IT リソースにさらなる保護を提供します。これは、情報漏洩のリスクや監査が不合格となるリスクなど、様々なリスクを軽減します。

2. IT とセキュリティにかかるコストを削減する：IBM の協賛を受けた Ponemon Institute は、IT、コンプライアンス、情報セキュリティに関連する業務を担当している 1,500 名以上の方（11 か国の 350 社）を対象に、「2015 Cost of Data Breach Study」（2015 年情報漏洩にまつわるコストに関する調査）を実施しました。同調査では、「情報漏洩にまつわるコストの平均総額が 2013 年比で 23%増の 38 億ドルである」ことが明らかとなりました。さらに、「損失または盗難された機密情報を含む記録 1 件に対して発生するコストの平均額が 145 ドルから 6%増の 154 ドルとなっている」ことも明らかとなりました。セキュリティを強化することで、悪用された脆弱性を首尾よく修正するために必要な時間とコストを削減できるだけでなく、さらにコストを抑えた自動化を実現できます。

3. マイナス影響なく保護する：モダナイズされた本当に効果的なセキュリティは、広範囲にわたる普遍的で目に見えないものであり、ユーザーの生産性や事業運営にほとんど、もしくはまったく影響を与えないものです。生産性や業務を妨害せずにセキュリティを改善できる機能は、ユーザーの満足度の向上や、広範にわたる新機能やツールの導入に欠かせません。

4. 情報を可視化し、理解を深め、保護を強化する：最大の保護には、自社の IT 環境とセキュリティ体制についての情報を最大限に可視化することが求められます。実現できる最高のセキュリティを自社環境および全社規模で実現するために必要な可視性と知識を提供できるのは、モダナイズされ、統合化されたツールのみです。

5. 企業のアジリティを強化する：競争を生き抜くため企業に求められるのは「アジャイル」であり続けることです。簡単に言えば、包括的で一貫性のあるセキュリティがない所にアジリティはありません。

6. 企業の復旧力を強化する：2013 年に Emerson Network Power の協賛を受けた Ponemon Institute が実施した調査では、データセンターのダウンタイムにより毎分約 7,900 ドルのコストが生じることが明らかとなりました。2014 年に Avaya が実施した調査では、影響を受ける企業の規模と種類によりますが、ダウンタイムのインシデント 1 件あたり、140,000～540,000 ドルのコストが生じることが明らかとなりました。さらに、2015 年に Kaspersky Lab と B2B International が実施した調査では、1 回のサイバーセキュリティ情報漏洩から復旧するために 38,000～551,000 ドルがかかることが明らかとなっています。これらの数値から、復旧力、すなわち定期的なダウンタイムと予期せぬダウンタイムの両方を軽減する企業の能力を強化することが絶対に必要であることは明白です。

7. 企業の信頼性を向上する：世界最大の PR 企業 Edelman は、約 33,000 人を対象に 2015 年信頼度調査を実施しました。回答者の約 63%が信頼していない企業とは取引しないと簡潔に回答している一方、80%が信頼できる人や企業としか取引しないと回答しています。モダナイズされた効果的なセキュリティなくして、信頼性を

保証し、示すことは極めて難しく、不可能である場合もあります。

8 ユーザー中心のセキュリティを実現する：モダナイズされたユーザー中心の IT 部門は、デバイス、ファイル、ツールよりもユーザーを重視しています。ユーザー中心の IT 部門を実現するには、ユーザー中心のセキュリティ、すなわち、許可されたユーザー、リソース、接続、デバイスすべてを包括的に集約して保護することが必要となります。

9. セキュリティを業務に組み込む：モダナイズされたセキュリティ管理は、問題が発生してから対応する戦術的なものではなく、より業務を重視した主体的なものです。大企業においてはセキュリティ関連の業務に携わる業務担当者が増えているため、セキュリティ業務の担当者はより複雑で戦略的な問題に集中して取り組むことができています。また、大小規模を問わず企業は、問題が発生してから対応する「消火」型の対応から、新しい改善されたセキュリティ対策とより主体的なセキュリティオペレーション（「SecOps」）を継続的に提供する体制にシフトする傾向にあります。

10. 未来に備える：「Verizon 2015 Data Breach Investigations Report」（Verizon による 2015 年情報漏洩に関する調査報告書）では、10 年前はマルウェアアクティビティの約 70%を 7 種類のマルウェアに分類できていたが、2014 年までに、7 種類に分類できていた 70%のマルウェアが 20 種に細分化されたことが報告されています。同じ時期に、マルウェアはメールによる「ワーム」から「コマンド&コントロール（C&C）サーバーを利用し気付かぬうちに攻撃するボットネット、認証情報の盗難、詐欺の手口」へと大幅に進化を遂げました。同調査では、毎日 1 秒あたり 5 件のマルウェアが発生していると予測されています。企業が今すぐ、そして将来必要な保護と適応機能を提供できるのは、モダナイズされた包括的かつユーザー中心のセキュリティだけなのです。

今すぐ IT セキュリティをモダナイズする 10 の方法

1. クリティカルなオペレーティングシステムすべてに、絶えずタイムリーに総合的なパッチを適用する。

2. クリティカルなサードパーティー製アプリケーションすべてに、絶えずタイムリーに総合的なパッチを適用する。

3. ローカルかリモートかモバイルかを問わず自社ネットワーク上のクリティカルなデバイスすべてに、絶えずタイムリーに総合的なパッチを適用する。

4. 非侵入型かつ非破壊型のアプリケーションのホワイトリスト（および必要に応じてブラックリスト）を作成する。

上記の 4 つのステップのみを行うだけでも、自社のセキュリティと保護を強化する大きな一歩を踏み出すことができます。

オーストラリア通信電子局は、ホワイトリストの作成、オペレーティングシステムとサードパーティー製アプリケーションへのパッチ適用、管理者権限の制限を行うことで標的型攻撃の最大 85%を防ぐことができると報告しています。

アメリカの脆弱性情報データベースでは、報告された脆弱性の 86%がサードパーティー製アプリケーションに起因するものであることが明らかとなっています。

「Verizon 2015 Data Breach Investigations Report」（Verizon による 2015 年情報漏洩に関する調査報告書）では、「[2014 年に]悪用された脆弱性の 99.9%が、共通脆弱性識別子（CVE）が公開されてから 1 年以上経過したものであった」ことが報告されています。

情報漏洩の被害にあった約 200 人の顧客を対象に Ponemon Institute/IBM が実施した調査では、悪意のあるアクティビティやソフトウェアに起因する情報漏洩が占める割合が全体のわずか 45%に過ぎず、残りの 55%の原因は業務上の過失や、正規ユーザーの不注意によるミス、システムの問題であったことが明らかとなっています。

ステップ 5〜10 のご紹介

5.できるだけ多くの実証されたパッチとセキュリティ管理プロセスを自動化する：自動化は、一貫したプロセスの実行を可能にし、プロセスのスケーラビリティを最大限に引き上げます。

6.主体的なパッチ管理を自社の重要な IT の取り組みすべてに組み込む：ここで重要な IT の取り組みには、特に IT 資産管理（ITAM）、IT 運用管理（ITOM）、IT サービス管理（ITSM）を重視する取り組みが含まれます。そのような取り組みの成功に欠かせないのが、包括的かつ効果的なユーザー中心のセキュリティです。

7.効果的なセキュリティに対する自分達の重要性を理解させるため、ユーザーを関与させ、教育を提供し、後押しする：ユーザーは企業にとって最初で最後の防御線となります。包括的かつ効果的なユーザー中心のセキュリティは、犯罪の被害者になることや、不正行為のルートになることからユーザーを保護することを目的としています。また、インシデントや疑わしい行動を IT サポート部門やセキュリティ部門、もしくはその両方に速やかに報告することをユーザー（顧客を含む）に推奨するものにもなります。

8.「サイロ化」しない：IT 部門とセキュリティ部門のみに委ねるには、IT セキュリティの重要度は高すぎていること、そして IT セキュリティが広く必要とされていることについて理解を示す企業が増えています。多くの企業が、セキュリティのための予算やアクティビティを IT 部

門から切り離しており、全社規模で予算を割り当て、取り組みを導入し、意識を高めています。一部の高く評価されている有名企業は、セキュリティに関する情報やインテリジェンスを「クラウドソーシング」していることを公表しています。すぐにできることとしては、社内の異なる部署の社員同士を交流させることがあげられます。

9.脅威を特定し優先するため、セキュリティの取り組みのサポートを促進し後押しするため、そしてセキュリティ関連の意思決定を促し支援するため、自社の環境に関するインテリジェンスとカスタマイズされたレポートを活用します：インフラストラクチャに関するインテリジェンスと自社環境から得た「事実」に基づくレポートを活用することで、多くの場合、最も広範にわたる効果的なコミュニケーションツールを IT 部門とセキュリティ部門の枠を超えて他の部門の社員にも提供できるようになります。

10.セキュリティに関する継続的な学習とセキュリティを進化させることを社員全員の最優先事項にするため尽力する：ガートナーのアナリスト、ローレンス・ピングリーは 2015 年 10 月『ニューヨークタイムズ』誌で次のようにコメントしています。「問題がないことが確認されている既知のファイルが 6 億件あり、約 4 億件のマルウェアファイルがあります。ただし、この他にさらに望ましくないアドウェアである可能性があるものが 1 億件あり、不明なソフトウェアパッケージが 2 億件あります。何が正常で何が危険かを見極めるには相当な才能が求められます」

4 億件の既知のマルウェアファイルのいずれかが自分達を標的とするかどうか、いつ標的とされるか、もしくはすでに標的とされているかを確認する術はありません。さらに、セキュリティツールに 300 億ドルほどを毎年費やしているとしても、脆弱性とセキュリティは毎日攻撃の対象となるのです。IT セキュリティツールとプロセスをモダナイズすることで、現在の保護を拡大し、今後待ち受けているものが何であれ将来に向けて効果的に備えられる方法で、自社のセキュリティを大幅に改善できます。

Ivanti Endpoint Security for Endpoint Manager：モダナイズされた IT セキュリティ

Ivanti® Endpoint Security for Endpoint Manager（旧 Landesk Security Suite）は、最も巧妙な脅威からユーザーと IT リソースを守る多層保護を提供します。機能には、自動パッチテスト、展開、Microsoft Windows および Mac OS システムの管理、選択した Linux のエディションの脆弱性の検出とレポート作成、アプリケーションとネットワークのアクセス管理、アンチウイルスの統合などが含まれます。

さらに、エンドポイントセキュリティとエンドポイント管理を集約化するため、このソリューションを Ivanti®Endpoint Manager（旧 Landesk Management Suite）と統合することもできます。これにより、セキュリティポリシーと IT 管理ポリシーの両方を速やかに自動化し、IT セキュリティと管理に関連するすべてのアクティビティで比類なき可視化を実現できます。また、統合することにより、Ivanti® Workspaces for the Security Administrator の集約化されたカスタマイズ可能なインターフェースと Ivanti® Mobile Security Suite の強化されたモバイル保護が追加されます。

Ivanti Endpoint Security for Endpoint Manager は、包括的かつ設定可能なレポートとダッシュボードのオプションも提供します。これらは、リスクと脅威の可視性を強化し、規制や方針遵守を容易にし、全体的なセキュリティ体制を強化する上で役立ちます。詳細は Ivanti の担当者までお問い合わせいただくか、オンライン（http://www.ivanti.co.jp/）にアクセスしてご確認ください。

http://www.ivanti.co.jp/

03-5226-5960

Contact-Japan@ivanti.com