多層防御セキュリティで負担を軽減

サイバー攻撃は増加しています。誰もが何度となくサイバー攻撃について耳にしていると思います。それには理由があります。2016 年に公表されたデータ漏洩の件数はアメリカだけで 500 件以上にものぼりました。これは前年の 2 倍近い件数です。[i] 2017 年 2 月には、調査企業 Opinium がアメリカとヨーロッパの IT 関連の意思決定者を対象とした調査の結果として、回答者の 78%が昨年勤務先の企業で少なくとも 1 回はランサム攻撃を経験したと答えていることを発表しています。最悪のランサムウェアとして知られる WannaCry が使用する脆弱性を暴露したハッカー集団 Shadow Brokers（シャドーブローカーズ）は、「ワインの定期購入」と同じシステムで定期的に脆弱性を公開していくと宣言しています。今世界では、史上初となる 100 万ドルの身代金が支払われたことが公表されています。[ii] また私たちは、今後出現する可能性が高い兵器化されたマルウェアを Petya によって経験させられたばかりです。

この流れを阻止するにはどうしたらいいのでしょうか？集中型セキュリティ戦略がなければ、デバイスの無秩序な拡散には多大なコストがかかり、管理ができない状態になります。IT チームは、これらのデバイスの管理に膨大な時間を費やしています。これに加え、サイバーセキュリティの知識を持つ労働力が不足しているため、企業はセキュリティ担当者を削減せざるを得ない状況になっています。つまり、総合的かつ簡易化された管理技術を活用する集中的な戦略を実施し、実際の攻撃に対する最高のバリアを作るセキュリティの基本に集中することで、他のソリューションに勝る強力なメリットが得られることは明らかです。

データ漏洩の 93%が 1 分もかからずに企業の評判に傷を付ける状況において [iii]、企業を守ることについて誤った選択は許されないのです。

まずはパッチ適用から

多くの既存の脆弱性に対してすでに利用できるパッチがあります。2017 年 3 月には、サポートされている Microsoft のオペレーティングシステムの WannaCry が突く脆弱性に対するパッチが公開されました。長年利用できていたセキュリティパッチが一度も適用されていなかったため、このような既存の脆弱性の多くが依然として主に未解決のままとなっています。2015 年 Verizon の RISK チームはこのような脆弱性の多くがは 2007 年まで遡ることができることを発見しました。[iv] また、最も良く知られた脆弱性の上位 10 件を悪用したサイバー攻撃の 85%が成功していたことも突き止めました。[v]

このような状況で、膨大なコストをかけず、IT 部門にとっての悩みの種を生じさせることなく、すべての脆弱性を追跡、修正、レポートするにはどうすればよいでしょうか？

企業に必要なのは、簡単に社内ネットワーク全体を調査、評価、テストし、パッチを適用する方法です。また、脆弱性の大半がサードパーティー製のアプリケーションに影響を及ぼすため、オペレーティングシステムへのパッチ適用や更新だけでは不十分です。

時間やお金をかけず、主力事業の取り組みをサポートすることに集中しましょう。Ivanti のツールは、わずか数分で起動し、お客様が定義したポリシーに基づいて、社内ネットワーク上の Windows、MacOS、Linux、UNIX システムすべてを自動的に特定、評価、修正します。当社のツールは物理システムと仮想システムの両方へのパッチ適用を簡単な操作に変えます。オンラインとオフラインのワークステーションとサーバーを検出し、不足しているパッチをスキャンし、展開します。その後、OS やアプリから仮想マシン（VM）、仮想テンプレートまで、あらゆるシステムにパッチを適用します。さらに、VMware との統合により、ESXi ハイパーバイザーにもパッチを適用します。

また Ivanti は、SCCM コンソールを通してサードパーティー製アプリケーションのパッチを検出、展開するプロセスを自動化し、簡単な操作に変える Microsoft System Center Configuration Manager へのプラグインも提供します。

当社のパッチソリューション向けの高度な API スタックは、セキュリティソリューション、脆弱性スキャナ、Chef や Puppet などの構成管理ツール、そして報告ツールに統合できます。この統合により、パッチに関する業務がセキュリティ製品の大規模なエコシステムのネイティブ（標準）プロセスに変わります。また、この統合は、セキュリティ部門、IT 部門、そして DevOps 間のギャップを埋めることにも役立ちます。例えば、テストを実施するためにパッチの最新の脆弱性評価を自動インポートし、IT 部門がこれまで以上に効率的に企業を保護するパートナーに変えることができます。DevOps の役割は、継続的に改善と自動化を進めることです。また、DevOps にパッチ管理を統合した場合、より回復力があり、一貫性のあるインフラストラクチャやシステムを実現できます。また、Splunk、Reporting Services、Archer、Crystal Reports などのソリューションに重要なデータを入れ、クリティカルなセキュリティインシデントを速やかに分析し、必要な対応をし、解決できます。

パッチが適用できないなら阻止

言うまでもなく、パッチでは、ゼロデイ攻撃に対する保護はできません。また、例えばレガシーシステムを実行している、もしくはパッチを適用することで使用している環境に何らかの支障がでることを懸念していて、パッチが適用できない場合はどうすればいいのでしょうか？アプリケーションのホワイトリストや権限管理などのツールを使用してパッチを適用できないアプリケーションを阻止する必要があります。

生産性を向上するために必要なアプリのみをユーザーに提供し、不正アプリを導入させないようにすることが極めて重要となります。不正アプリは

デスクトップの安定性を損ない、セキュリティに影響を及ぼし、ライセンスのコンプライアンスの違反となり、ユーザーのダウンタイムにつながり、デスクトップ管理コストを引き上げる原因となることがあります。

一方で、デスクトップをロックダウンすればリスクを軽減できるものの、ユーザーエクスペリエンスの質も大幅に低下してしまいます。パフォーマンスが低下するためユーザーの生産性は下がり、結果としてヘルプデスクに多くの問い合わせの電話がかかることになります。また、ユーザーはシャドーIT（個人用のデバイスを許可なく使用すること）でシステムロックダウンに対処する可能性があり、これが新たなセキュリティリスクにつながります。

Ivanti は、IT 部門に膨大なリストを手作業で管理させることなく、また、ユーザーの生産性に障害をもたらすことなく、不正コードの実行防止に役立つ革新的なソリューションを提供します。Trusted Ownership™は、既知のコードであっても、信頼できない所有者（例えば一般的なユーザーアカウントなど）が導入したすべてのコードの実行を自動的に防止します。簡単な操作でユーザー権限やポリシーを詳細に管理できるだけでなく、例外が発生した場合に自己昇格機能を使用できます。担当業務を履行するために必要な権限のみをユーザーに付与することで、プロセスをシンプルにします。

さらに、当社は SCCM 環境でのサポートをアプリケーション管理にまで広げています。集約化されたコンソールを使用してエンドポイントでのアプリケーションとエンドユーザーの操作を管理しましょう。また、System Center Operations Manager（SCOM）を使用して、Application Control のイベント/監査の詳細を収集しましょう。

セキュリティ管理をレベルアップ

Ivanti のエンドポイントセキュリティプラットフォームは、自動化されたパッチ管理とアプリケーション管理を、統合された強力なエンドポイントセキュリティ管理と結びつけます。エンドポイントセキュリティ管理には、グローバルポリシー、セキュリティ診断、リモートエンドポイント管理、セキュリティダッシュボード、レポートなどが含まれます。

このレベルで Ivanti は、高度なウイルス対策とマルウェア対策機能をお客様のセキュリティソリューションに追加できます。また、デバイス管理（リムーバルデバイスの使用の管理、リムーバルデバイスおよびハードドライブ上での暗号化の施行）とファイルレス攻撃に対する高度な保護（インターネットからダウンロードされたスクリプトの無効化、アプリの挙動の検出、信頼できるアプリのスクリプト実行のみを許可、メモリ内攻撃に対する保護など）も提供できます。さらに、許可されたネットワークや IP アドレスにアクセス権を制限することや、個別のシステムやシステムグループに対してファイアウォールの設定（最新の Windows ファイアウォールを含む）をカスタマイズすることもできます。マルウェアをブラックリスト化して効果的に攻撃を阻止するため、ローカルマシンのファイルを暗号化しようとする試みを検出し、暗号化プロセスを阻止し、ネットワーク上の他のすべてのコンピューターにインシデントを通知できます。

簡便な単一のインターフェースにより、統合されたセキュリティコンポーネントとサービスの設定やタスクを簡単に管理できます。また、リモートコントロールの機能が充実しているため、ネットワーク上のエンドポイントを隔離し、調査し、クリーンアップできます。

動作の遅いマシンや、セキュリティに関する懸念があるマシンを管理しましょう。問題の根本的原因を速やかに特定するため、アプリの評判に関する情報、ディスカバリ/実行時間、その他のメタデータを表示してリアルタイムの情報を入手し、同じコンソールから問題を修正しましょう。システム管理ツールを統合すれば、IT 環境の効率と管理を向上できます。

リアルタイムダッシュボードのレポート

Ivanti はお客様が結果を把握できるよう支援します。

実環境の実態を把握していなければ適切な防御はできているとは言えません。そこで Ivanti Xtraction は、経営陣や取締役、事業部門（LOB）やアプリケーション所有者に適切なデータを提供できるようにするため、オンデマンドのデータと簡単に新しいダッシュボードやレポートを作成できる機能を使い、レポートをチェック機能に変えます。

お客様が使用しているほぼすべてのツール（サービスデスク、モニタリングと ITAM のツールセット、電話システムなど）向けに事前構築されたコネクタが提供されるため、プログラミングやビジネスインテリジェンスのエキスパート、スプレッドシートは不要です。また、データのサイロ化の心配もありません。また、社内での連携をさらに強化するため Xtraction をカスタマイズすることもできます。これにより、誰もが膨大な量のデータからクリティカルな意味のある情報を抽出して、全社規模で状況に沿ったデータを確認できるようになり、簡単かつ速やかに賢い判断を下すことが可能となります。

i Privacy Rights Clearinghouse
ii https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/
iii Verizon 2016 Data Breach Investigations Report (DBIR)
iv Verizon 2015 DBIR
v Verizon 2016 DBIR

03-5226-5960
www.ivanti.co.jp
Contact-Japan@ivanti.com