ivanti

IT セキュリティに関する国の現状：3 本のセキュリティに関する考察

ホワイトペーパー

目次

セキュリティに関する国の現状 – パート 1：国家が支援する活動の増加

言うまでもなく、現代のハッカーは、世界中のクリティカルなインフラストラクチャに甚大な影響を持っています。医療機関、金融システム、電力網をはじめ、多くのエリアが定期的にサイバー攻撃の標的となっており、その脅威の影響を受けています。現在最先端の攻撃ツールが、広く出回っていることがサイバー攻撃の脅威の増加に少なからず関係していると言えるでしょう。

すでにご存知の方もいらっしゃると思いますが、2017 年に発生した NotPetya 攻撃のベースアーキテクチャには、国家機関、すなわち国家安全保障局（NSA）によって開発されたエクスプロイトが使用されていました。悪用されたツールと脆弱性は、NSA のツールを入手したハッカー集団の活動を通して明らかとなりました。

このケースでは、国家のツールを使用した攻撃が、国家が支援するハッカーによって画策されたものでもありました。NotPetya は、ランサムウェアを装った攻撃でしたが、金銭を目的に行われたものではありませんでした。多くのランサムウェアキャンペーンは、関係当局によって支払いが停止されることや、支払いの受け取りが制限されることが絶対にないようにするため、支払いを可能にする様々なメカニズムを提供します。ところが、NotPetya 攻撃において、ランサムウェアキャンペーンに共通するこのような特徴はほとんど、もしくは一切認められませんでした。また、ランサムに身代金を支払ったとしても、NotPetya の攻撃者は被害者に対してファイルを復元する方法を提供しませんでした。

NotPetya 攻撃では、金銭を得るために直接的な影響をもたらすためではなく、社会や経済を混乱させるものとしてランサムが使用されたのです。これはいわばサイバー攻撃の新たな進化だと言えます。NotPetya 攻撃は、国に金銭を要求することではなく、国を破壊する、国を混乱に陥れることを目的とした、慎重に計画された悪意のある行為でした。NotPetya は、金融技術を専門とするウクライナの企業 MeDoc の会計・税務ソフトウェアに不正侵入し、このソフトウェアをダウンロードする可能性のあるユーザー、すなわちウクライナの企業を攻撃するためにこのソフトウェアを悪用することで、ウクライナのインフラストラクチャを標的に実行された攻撃でした。

この攻撃は、標的となったシステム上の記録をすべて破壊し、使用不能の状態にすることに見事に成功し、その脅威を証明しました。ウクライナの企業は、全社規模で何日間も営業できない状態に陥りました。NotPetya は病院にも影響を及ぼし、感染した病院では手術がキャンセルされる事態となりました。また、病院以外にも航空会社や銀行、チェルノブイリ原子力発電所、製薬会社 Merck、FedEx をはじめ、多くの大手企業が NotPetya の被害を受けました。NotPetya に感染した世界大手の運輸会社 Maersk は、ロサンゼルスからムンバイまで、港にあるコンテナターミナルの閉鎖を余儀なくされました。さらに NotPetya は、社内ネットワークが大規模で、攻撃が行われた場所からはるかに離れた場所まで感染が拡大する結果となった、多国籍企業を営業停止させることにも成功しました。世界中の 2,000 社以上の企業が NotPetya に感染したのです。

問題はセキュリティと IT の専門スタッフとして、戦略を練り、この種の攻撃に対してより効果的に防御を行うために何ができるのか、どんな手段を取れるのか、ということです。

ソフトウェア脆弱性の脅威の状況

私たちは何よりもリスクを重視する必要があります。

例えば、今日にいたるまで、ソフトウェアの脆弱性は、脅威の状況全体、すなわち攻撃対象の全領域において極めて重要な役割を担っています。

Forrester が発表したレポート「*Wave: Vulnerability Risk Management, Q1 2018*」（WAVE：2018 年第 1 四半期脆弱性リスク管理）では、昨年最低一回不正アクセスの被害を受けた企業が 58%だったことが指摘されています。この 58%の企業で行われたすべての不正アクセスが、何百万人ものお客様の個人情報が漏えいしたというような新聞の一面を飾る深刻なものではありませんでしたが、この数字が示す最も恐ろしい事実は、昨年一年間で企業の半数以上が最低一回不正アクセスの被害を受けているということです。

唯一の朗報は、これらの不正アクセスの原因のうち確実な原因がひとつ特定されていることです。これらの不正アクセスのうち、ソフトウェアの脆弱性を悪用したものは 41%でした。昨年一年間という期間の中で最も深刻な不正アクセスの被害は、1 億 4,790 万人の消費者の個人情報（社会保障番号、住所、運転免許証の番号、クレジットカードの番号など）が漏洩した、Equifax の情報漏洩でした。この情報漏洩の原因として、ウェブフレームワーク Apache Struts のソフトウェアの脆弱性が特定されています。

Apache のウェブサーバーに侵入し、機密データにアクセスするために、他の足掛かりが使用された可能性もありましたが、実際にデータへのアクセスとデータの抽出を行うために使われた手段は、ソフトウェアの脆弱性だったのです。また、この脆弱性にはパッチが存在していたことは、特に注目すべき点です。

話を国家が支援する攻撃の調査に戻し、WannaCry について見ていきましょう。WannaCry は国家が開発したソフトウェアを悪用するエクスプロイトおよびランサムウェア攻撃で、世界 150 ヵ国以上の 23 万を超えるエンドポイントに影響を及ぼしました。

NotPetya 同様、NSA が開発し、ハッカー集団 Shadow Brokers が 2017 年 4 月 14 日に流出した EternalBlue エクスプロイトが攻撃者によって使用されました。EternalBlue は、Microsoft のサーバメッセージブロック（SMB）プロトコルの実装の脆弱性を悪用します。

Microsoft は、欠陥を詳述したセキュリティ情報を発行し、パッチ更新プログラムをリリースしました。ところが、Equifax の情報漏洩と NotPetya（WannaCry の後に行われた攻撃）のケースと同様、パッチが利用可能であったにも関わらず、攻撃者は EternalBlue エクスプロイトを使用し、後に WannaCry 攻撃を成功させました。

攻撃に使用されたもうひとつのツールが DoublePulsar でした。DoublePulsar もまた NSA によって開発され、Shadow Brokers によって流出されたバックドアツールで、パブリックネットワークに接続された SMB ポートがない環境を WannaCry に感染させることを可能にするものでした。DoublePulsar は、世界中の何万台ものシステムに事前にインストールされていたため、これらのシステムの管理権限が攻撃者に引き渡され、攻撃者は DoublePulsar を使用し、簡単に WannaCry ランサムウェアを実行することができたのです。DoublePulsar はカーネルモードで実行するため、感染したコンピューターシステムを管理する高いレベルの権限をハッカーに付与できます。

したがって、SMB プロトコルをパブリックネットワークに接続させ、脆弱性を露呈させる手法とエクスプロイトを可能にするバックドアとして DoublePulsar を使用する手法を組み合わせたことが、WannaCry 攻撃の見事な成功につながったのです。また、攻撃を受けた多くの環境に更新プログラムが展開されていなかったため、このエクスプロイトは非常に速いスピードで広がりました。

WannaCry も NotPetya も、現代の企業においてはもちろん、国家が引き起こしている大混乱を踏まえれば国家にとってはなおさら、総合的かつタイムリーなパッチ管理が何より優先すべき対策であることを示しています。

高度な多層攻撃アプローチに求められるのは、高度な多層防御アプローチ

一度環境に侵入した NotPetya によって、さらに感染を拡大させるために追加の機能が使用されました。

管理者の認証情報を入手するために Mimikatz と呼ばれるツールが使用されたのです。そして、PsExec や WMIC といった他の既存のツールを使用するために管理者の認証情報が悪用され、さらには不正に入手した認証情報とそれらのツールを使用して他のシステムへのリモートアクセスを実行し、SMB エクスプロイトが利用できなかった場所にまで、影響を拡大したのです。

最後に、2 回目の攻撃でマルウェアをマシンに導入するために NotPetya が使用したもうひとつの方法がフィッシングでした。実はフィッシングはランサムウェアやその他のマルウェアの脅威の侵入経路として最も多く使用されていることをご存知でしたか。

これまで述べてきた現実はすべてサイバー攻撃が非常に高度な多層攻撃アプローチであることを物語っています。そしてこの種の攻撃には、それに匹敵する高度な多層防御アプローチが必要なのです。これまで見てきた通り、適切に実行されたパッチ管理は極めて重要な対策ですが、社内でのマルウェアの拡大を阻止するためには権限管理も同様に欠かせない対策となります。また、フィッシングキャンペーンの成功率を下げるために、社員を対象としたセキュリティに関する認識を強化するためのトレーニングを実施することも重要です。

当社の最後の考察では、企業が優先して取り組むべきリスクと、リスクを軽減するために導入すべきセキュリティコントロールについて詳しく見ていきたいと思います。

セキュリティに関する国の現状 - パート 2：SamSam 攻撃＆リスク対策の優先付け

SamSam ランサムウェアファミリー

SamSam は、比較的最近出現したもうひとつの進化型ランサムウェアです。初めてその存在が明らかになってからわずか数年しか経っていないにも関わらず、あっと言う間に深刻な被害をもたらす存在となっています。

SamSam ランサムウェア、そしてこの攻撃を仕掛けている同名のサイバー攻撃集団 SamSam は、間違いなく標的に狙いを定めて攻撃を実行しています。SamSam 攻撃を行うハッカーは、ランダムに金銭を得るための大規模な「Ransomware as a Service（サービスとしてのランサムウェア）」を目的としていません。彼らは標的を絞り込み、攻撃に積極的に関与しています。ランサムウェアを展開、実行する前に標的のネットワークに不正侵入し、入念な調査を行います。また、攻撃中に戦術を変更します。あるアプローチがうまく機能しなければ、方針を変更し、攻撃の効果を最大限に引き上げるために別のアプローチを導入します。セキュリティソフトウェアによって、マルウェアの実行が妨害された場合、彼らはソフトウェアを無効化する方法を模索するでしょう。

エッジサーバーまたは感染サーバー

このサイバー攻撃集団は、これまでインターネットに接続するサーバーを感染させています。これまでに、Red Hat ベースの Java 開発環境である JBoss を狙った攻撃とパートナーやお客様にリ

モートデスクトッププロトコル（RDP）サービスを利用させるために、医療関係の企業において大抵パブリックネットワークに接続されているオープンな RDP を狙った攻撃も検出されていますが、該当するケースは数えるほどしかありません。

サイバー犯罪者は、RDP にブルートフォースアタック（総当たり攻撃）を仕掛けます。もしくは、JBoss のようなプラットフォーム上で一般に公開されているソフトウェアを悪用します。ご存知の通り、従来 RDP のセッションは弱いパスワードで構成されていることが多いため、パスワードのポリシーを強化することがサイバー攻撃者の侵入を軽減するひとつの手段となります。

ただし、一度侵入されると、彼らの高度な技術は警戒レベルになります。サイバー攻撃者は、管理者の認証情報を入手し、他のシステムへのアクセス権を手に入れるため、Mimikatz、PsExec、WMIC などのツールを活用します。攻撃者は、約 10～12 種類のツールが含まれたリストを持っています。このリストには、悪意のある性質のツールもしくは企業の環境に既存しているツールが含まれていることもあり、特定の権限レベルを入手さえすれば様々な方法で使用することができます。

また、すでに指摘した通り、ランサムウェアは特定のアルゴリズムに基づいて何かを悪用するために自動化された単なるソフトウェアではありません。侵入先の環境で活動し、戦術を変更し、新たに直面した障害を回避する新しい方法を開発するのです。

個別のシステムの身代金目的ではない

さらにこの種の攻撃者は個別のシステムの身代金を目的としていません。彼らは大抵、マシンごとの身代金を提案しますが、すぐに全社規模の暗号解読オプションに提案を引き上げます。この額は 50,000 ドル近い金額になることがほとんどです。

彼らが実際に実現を目指しているのは、月に 6～8 件の攻撃を仕掛け、1 件あたり 50,000 ドルの身代金を得ることです。数年前に現れて以来、彼らはビットコインによる身代金の支払い約 600 万ドルを手に入れ、月に平均して約 330,000 ドルを支払わせることに成功しています。繰り返しとなりますが、彼らは環境に侵入し、気付かれないように動き、攻撃を実際に開始する前に、非常に効果敵意に環境全体にランサムウェアをばらまくのです。

つい先日にも、某医療関連企業を標的にこの種の攻撃が行われました。攻撃が阻止されるまでの最初の 15 分間で、ランサムウェアは約 9,000 のシステムに感染し、実行されました。これが彼らのやり方なのです。

アトランタ市を混乱に陥れた攻撃

ここからは、2018 年 3 月にアトランタ市の 5 つの局を攻撃した SamSam ランサムウェアについて見ていきましょう。これは深刻な混乱を招いた攻撃で、市の職員は任務を遂行するためクローゼットから引っ張り出してきた古いノートパソコンを共有することを余儀なくされました。

裁判所や警察など、影響を受けたシステムの 30%近くが市にとって極めて重要なシステムでした。市当局は、6 台を除くすべてのコンピューターと 10 年分に相当する文書を失いました。警察はドライブレコーダーの録画記録を失いました。約 8,000 人の市職員が数日間パソコンを使えない事態に陥りました。

アトランタ市が被った被害額は約 1,700 万ドルで、その額は今なお増加しています。この額には、業務が妨害された警察の代わりとなる外部の警備サービスやサービスの停止を余儀なくされた緊急電話番号に代わるオンライン救急サービスなどを導入するためのコストなど攻撃の影響をクリーンアップするハードコスト（実際に見えるコスト）約 260 万ドルが含まれています。

ここでもう一度コスト以外の被害に目を向けてみましょう。市内の必要不可欠なサービスの実に 3 分の 1 以上がオフラインもしくは利用できない状態になり、うち約 30%が生活には欠かせないサービスでした。

同様に、NotPetya は、FedEx、Maersk、Merck などの企業に対して、1 社あたり推定 2 億～3 億ドルの損害を与えましたが、その一方で NotPetya により手術がキャンセルされたことや、チェルノブイリ原子力発電所が標的とされたことなどを記憶しておくことが極めて重要となります。データの破損や損失によるコストに加え、事業の中断や生産性の損失、フォレンジック調査、業務の立て直し、株価、生じる可能性のある罰金、失われる可能性のある人命、その他の公共の安全に関する懸念事項などは、絶対的に重視する必要があります。

リスク対策を優先するための第一歩

セキュリティや IT の専門スタッフは、この種のクリティカルな影響を及ぼすことを目的とした高度な攻撃のリスクから企業をどのような方法で保護できるのでしょうか。

とにかくリスクを優先する必要があります。言うまでもなく、考えられるエクスプロイトすべて対して保護を提供することはできません。100%完璧なセキュリティというものは存在しないのです。では、セキュリティの効果を最大限に引き上げるためには、適切なことに注力するにはどうしたらよいのでしょうか。

既知の脆弱性

既知の脆弱性は、依然として多くのセキュリティ侵害の根本的な原因となっているという事実があります。ガートナーは、2020 年末までに悪用される脆弱性の 99%が、悪用された時点でセキュ

リティや IT の専門スタッフにとって既知の脆弱性となるだろうと予測しています。ゼロデイ攻撃も行われていますが、頻発しているとは言えません。ハッカーは、セキュリティを突破し侵入するスキルに頼っています。彼らは、企業のセキュリティ部門や侵入テスト専門スタッフと同じスキルを開発しているのです。ハッカーの潤沢な資金こそまさに、企業よりもハッカーの開発速度が速いことを示す証拠です。

社員：企業の最大の弱点

既知の脆弱性には人的な脆弱性となる社員が含まれています。事実、社員は依然として 1 番の攻撃経路なのです。したがって企業の環境において、社員は最大の弱点となっています。

「*Verizon 2017 Data Breach Investigations Report*」（DBIR）では、セキュリティに関連するインシデントとセキュリティの侵害の 90%以上に程度の差はあるもののフィッシング攻撃が含まれていることが指摘されています。フィッシング攻撃は依然として一番使用されているランサムウェアや他のマルウェアの脅威の侵入経路なのです。フィッシングに関する情報の普及が進んでいることから、以前に比べて考えずにクリックするユーザーはほとんどいなくなっていますが、いまだにフィッシングキャンペーンを受信しクリックしてしまうユーザーは 4%存在すると言われています。

同様に 2018 年には、DBIR のリスク部門により、メールが侵入経路として最も頻繁に使用され続けていることが認められました。しかも、侵入された責任の実に 96%がメールにあるものの、平然と使用が続けられているのです。マルウェアの 49%がメール経由でインストールされているのです！

メール経由での侵入に必要なのは、1 人のユーザーと 1 つのリンクまたは添付ファイルだけなのです。これを踏まえれば、フィッシングが攻撃においてこれほどまでに重要な役割を担っているのも不思議なことではありません。事実、NotPetya の 2 回目の攻撃においてフィッシングが使用されたことを示す証拠はありません。したがって、管理者としてログインしたユーザーもしくはドメイン管理者が、ブービートラップが仕掛けられた添付ファイルを実行させるメールの罠にかかり、高レベルの権限でマルウェアがインストールされ実行された可能性があります。

ここにもうひとつ人的な脆弱性があります。それは管理者権限です。パート I で触れた通り、最新のサイバー攻撃を企業内に広げるために管理者権限がハイジャックされることがあります。

セキュリティに関する国の現状 - パート 3：CIS のフレームワーク「クリティカルセキュリティコントロール」

CIS のコントロール - 実証されたセキュリティフレームワーク

本書において、最新のサイバー攻撃の主な攻撃経路を考察しているのには理由があります。当社は、企業が不足している可能性のあるリソースを、すぐに得られる価値の高いメリットのある対応に支援することを目指しています。

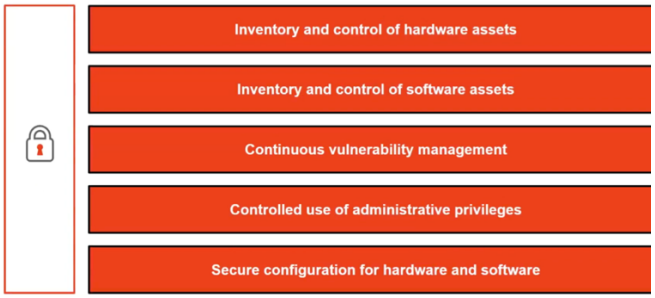
お客様がリスクを最優先できるよう支援するために当社が取っている方法のひとつが、米国インターネットセキュリティセンター（CIS）のフレームワーク「クリティカルセキュリティコントロール」の順守です。CIS のコントロールは、IT システムとデータを最も蔓延している攻撃から安全に守るためのベストプラクティスとして認識されています。米国国家安全保障局（NSA）の実体験に基づく CIS コントロールは、オーストラリア通信電子局（ASD）、米国国立標準技術研究所（NIST）、国立サイバーセキュリティセンター（NCSC）などを含むサイバーセキュリティに関するガイダンスの主要な情報源となっている機関を支援しているだけでなく、それらの機関のガイダンスにも反映されています。

CIS のフレームワークは、20 のセキュリティコントロール（セキュリティ対策）で構成されています。CIS の研究やケーススタディでは、上位 5 コントロールが、現在私たちが直面しているサイバー攻撃の脅威の 85%を占める最も一般的なサイバー攻撃に対し効果的な防御となることが認められています。フレームワークを構成するコントロールの一部を導入することによって、セキュリティ上の弱点の大部分に集中的に取り組み、排除することで、防御効果はさらに強化されます。繰り返しとなりますが、このセキュリティコントロールは効果を優先するためのものです。

自社環境を安全に保護するためにやるべきことの多くが、80/20 の法則に基づいて物事を評価することです。どうすれば 20%の労力で 80%の価値を得ることができるでしょうか。20 のコントロールのうち上位 5 のコントロールを導入すれば、セキュリティプログラムの効果を 85%向上させることができます。25%の労力で、85%のメリットを得られる―したがって、効果を優先する上で、上位 5 のコントロールを導入することは労力に対する効果がかなり高いと言えるでしょう。

では上位 5 のクリティカルセキュリティコントロールとは具体的にど

のようなコントロールなのでしょうか？



ハードウェア資産とソフトウェア資産のインベントリと管理

まず 1 番目と 2 番目のクリティカルセキュリティコントロールから見ていきましょう。企業の資産の全体像を把握していない限り、自社環境に存在するすべての資産を保護することや防御することはできません。ビジネスクリティカルなアプリケーションを実行するシステムすべてにおいて管理者権限は縮小されていますか。パブリックネットワークに接続されているキオスクとその他のシステムはすべてアプリケーションとデバイス管理の観点からロックダウンされていますか。同様に、古いオペレーティングシステムを実行しているデバイスや、Meltdown や Spectre などハードウェアの脆弱性に対する防御を行うためのファームウェアの更新プログラムの提供が終了しているハードウェアを実行しているデバイスを使用している場合、古い脆弱性にさらされているデバイスを特定し、新しいデバイスと交換する作業から始めることができます。

すでに触れた通り、2 番目の CIS のクリティカルセキュリティコントロールは、アプリケーションのホワイトリスティングを導入するコントロールです。ユーザーが自身のデスクトップにアクセスする方法や場所を問わず、ユーザーには生産性を向上するために必要なアプリのみを提供し、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軽減し、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。

継続的な脆弱性管理

3 番目のコントロールには、自社環境において既知の脆弱性を評価し、それらに対して継続的に対応を取ることが含まれます。このコントロールを効果的に実践するために、自社環境のソフトウェアをすでに把握している必要があります。同様に、2 番目のコントロールを効果的に実践するためには、自社環境のハードウェアについて正確なインベントリを作成する必要があります。つまり、クリティカルセキュリティコントロールは、上の順位のコントロールが導入された場合に、すべてのコントロールをさらに効果的に機能させるコントロールが続くように優先順位付けされています。

継続的に脆弱性を評価、管理するため、2 つの異なるテクノロジーが必要となります。企業にはセキュリティ部門があり、脆弱性を管理するためのソフトウェア（Qualys、Nessus、Tenable、Rapid7 など企業が使用している脆弱性ベンダーのソフトウェア）があります。これに加え企業には、Ivanti や Microsoft、他のベンダーからのパッチ管理ソリューションが導入されています。

ここで前者と後者は、脆弱性のギャップを埋めるために連携して取り組みを行う必要があります。繰り返しとなりますが、ソフトウェアの脆弱性は攻撃対象領域の大部分を占めています。対象となる領域を制限することは、侵入経路となり得るドアや窓を閉じ、施錠する上で役立ちます。

管理者権限の管理

前述の一部の攻撃に関して言えば、攻撃者は何度もソフトウェアの脆弱性を悪用し、システムに侵入し、企業の環境に存在すべきではない信頼できないツールを起動しています。また、これらのツールを使用して、企業の環境において有効な管理者の認証情報を不正使用します。

攻撃者は、企業の環境から有効な認証情報と社内で活用されているすぐに利用できるツールを活用し、検出がさらに困難な機能や手段を使用できるようになります。ご自身が作成したユーザーである場合やご自身がアクセス権を付与したツールが使われている場合、フィルターを適用し、行動パターンを念入りに調べるにはどのような方法を取れるでしょうか。

ユーザーエクスペリエンスを文字通りロックダウンするだけで問題を解決できた時代は遥か昔に終わっています。今もなおユーザーの権限を完全にロックダウンするポリシーを施行できる企業は存在しますが、ユーザーが業務を遂行する上で必要な一部の機能には、管理者権限をユーザーのシステム上でユーザーに付与することが避けられないものがあるのが現実です。Microsoft は、ユーザー権限と完全な管理者権限の 2 つのレベルのコントロールしか提供していません。この 2 つの権限の間には、いくつかのバリエーションが存在しますが、ユーザーと管理者の両方を満足させるエクスペリエンスを提供するには十分ではありません。

ユーザーから完全な管理者権限を除去し、担当業務に必要なタスクのみにアクセスできる昇格権限をユーザーに付与することで、エンドポイントの安全性を簡単に確保し、サポートへの問い合わせ電話の件数を軽減し、TCO（総所有コスト）を削減できます。完全な管理者権限を一般ユーザーから取り戻し、アクセス権から、アプリケーションのインストール、プリンターのインストール、PowerShell の使用、その他ユーザーが必要な操作を実行する権限まで必要な場合に権限の昇格を提供しつつ、ユーザーに付

与すべきではない権限は付与しないようにすることか、もしくは、完全な管理者権限を管理者のみに付与し、一般ユーザーがアクセスすべきでないコンテンツへのアクセス権を剥奪するか、それとも例えばPowerShellを使用する権限をはく奪するか、その他の特定の機能へのアクセス権のみを提供するか…すべてはお客様次第です。管理者権限を特定のコンソールやアプリケーション、サービスやコマンドに制限し、管理者に起因するマルウェアのリスク、基幹サービスの中断、ミッションクリティカルなサービスのパフォーマンスへの影響を軽減しましょう。

ハードウェアとソフトウェアのセキュアな設定

オペレーティングシステムとアプリケーションのデフォルト設定は通常、セキュリティではなく展開しやすさと使いやすさを念頭に置いた設定です。結局、5 番目の CIS のコントロールにおいてユーザーが求めるのは、最低限の構成基準を維持することなのです。

構成を理解するためにチェックリストに隈なく目を通していただくこともできますが、ここでは 3 本の考察で触れた内容と紐づけてみていきましょう。例えば、弱い RDP のパスワードは、サーバーのドアを開けっぱなしにし、通りかかったスパイに室内を公開しているようなものです。ハッカーは、RDP パスワードを入手すると、ログオンし、新しい管理者アカウントを作成します。これによりハッカーは、後で気付かれないように使用できるバックアップアカウントを持つことができ、かなり高い確率でこのアカウントを使用して破壊的なランサムウェアのアップロードや展開などの操作を実行します。

このような脆弱性に対応するパッチをタイムリーに適用することに加え、不要な場合には、RDPをオフに設定すればSamSamなどの攻撃を食い止める役に立ちます。また、パスワード類推攻撃を制限するため、ロックアウトポリシーを設定することもできます。

さらに、WannaCry攻撃が実行されて以来、IT部門にはSMB（サーバメッセージブロック）バージョン 1 サービスを無効に設定することも推奨されるようになりました。概して、5 位のコントロールは、十分なファイアウォールルールと複雑なパスワードが設定されているかを確認する対策です。また、設定を強化することで、企業の環境で実行されている脆弱な暗号スイート、プロトコル、アプリケーションをロックダウンする対策でもあります。ロックダウンの対象には、自社の IIS サーバーや SQL サーバーなども含まれます。

繰り返しとなりますが、上位 5 コントロールすべてを組み合わせて活用することで、現存する脅威の 85%を軽減または排除できます。

常に警戒する

IT セキュリティの専門スタッフにとっては、常に脅威、脆弱性、業界の動向に関する最新情報を把握していることが極めて重要となります。Ivanti は以下のリソースを通して、企業がこの目標を達成できるよう支援しています。

- **セキュリティに関するブログの更新（週 1 回）** – 当社の研究者が毎週金曜日にブログを投稿しています。また、広範囲に及ぶマルウェア攻撃発生時には緊急の最新情報が提供されます。こちらをクリックしてご確認ください。もしくはIvanti.com/blog にアクセスしてください。
- **ウェビナーシリーズ「Patch Tuesday」** – 毎月ライブ配信されるウェビナーにぜひご参加ください。「Patch Tuesday」は、更新プログラムや脅威に関する情報などをご確認いただける受賞歴のあるウェビナーシリーズです。
- **IT セキュリティに関するリソース**– お客様のセキュリティ体制を強化するお手伝いをさせていただければ幸いです。Ivantiの専門スタッフや当社のお客様、ガートナーやフォレスターなど業界のアナリストからの見解や方法をご確認ください。当社のリニューアルされたセキュリティに関するサイトで、活用できるコンテンツをお探しください。

詳細はこちら

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