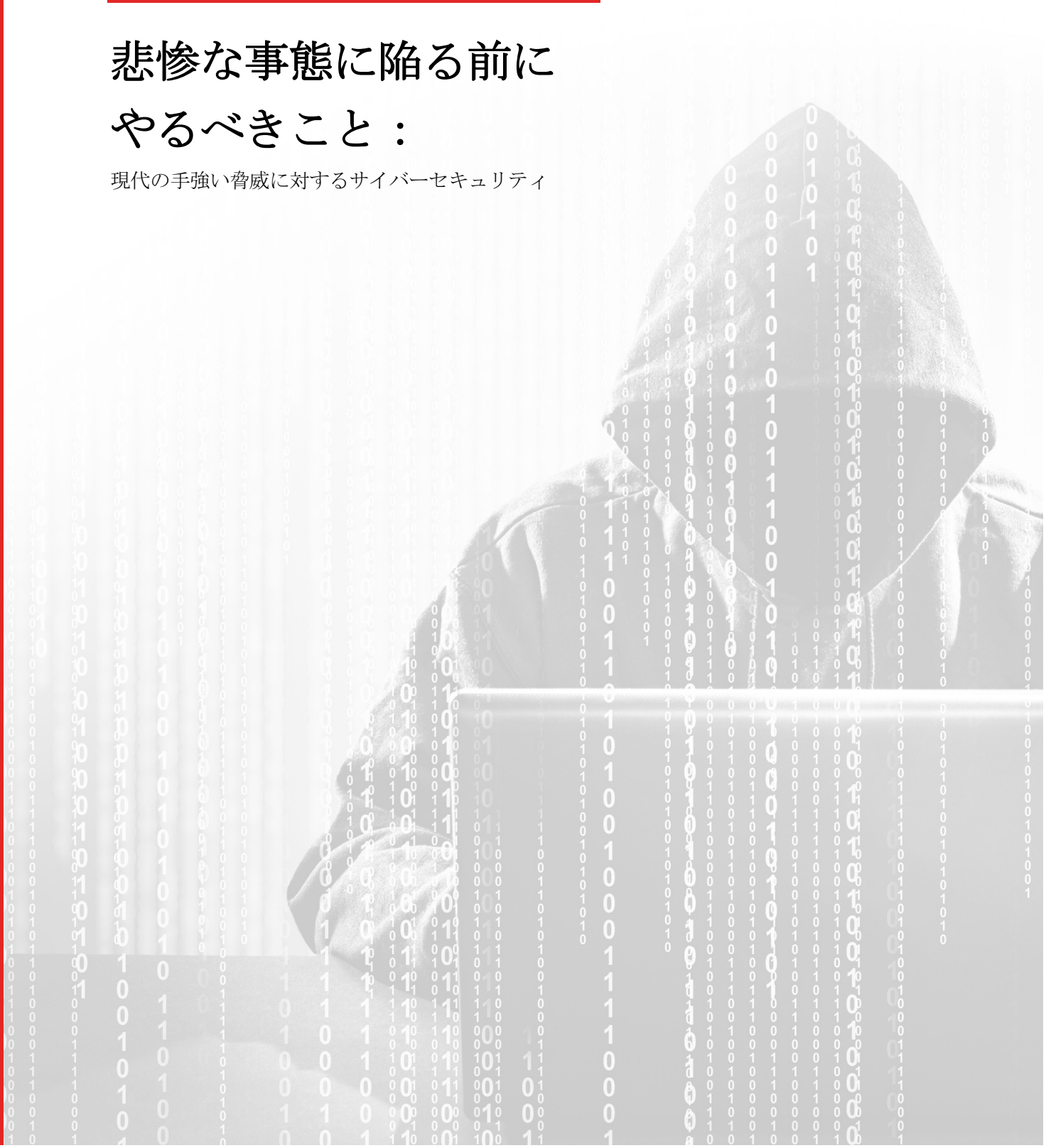
悲惨な事態に陥る前に
やるべきこと：

現代の手強い脅威に対するサイバーセキュリティ



目次

はじめに

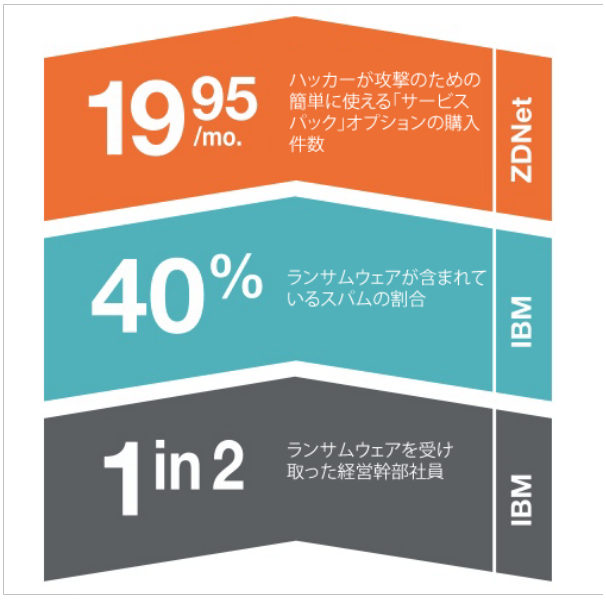
2016 年、公表されている情報侵害の件数はアメリカだけで 500 件を超えていました。これは前年比で約 2 倍に相当する件数です。[1]調査会社の Opinium の 2017 年 2 月のアンケートによりますとアメリカとヨーロッパの IT 責任者の 78%が昨年ランサムウェア攻撃を少なくとも 1 回は受けていると答えました。最悪のランサムウェアとして知られる WannaCry が使用する脆弱性を暴露したハッカー集団 Shadow Brokers（シャドーブローカーズ）は、今後定期的に同じような脆弱性を公開していくと宣言しており、すでに公約を果たしています。事実、史上初となる 100 万ドルの身代金が支払われたことが公表されただけでなく、[2]NotPetya によって今後出現する可能性が高い兵器化されたマルウェアがどんなものかを思い知らされました。そして、Equifax の情報漏洩のニュースは世界に衝撃を与えました。

この流れを阻止するにはどうすればいいのでしょうか？的を絞ったセキュリティ戦略がなければ、デバイスの無秩序な増殖には多大なコストがかかり、管理不能な状態に陥ります。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最適化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的を絞って取り組むことで、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。

情報漏洩の 93%が数分もかからずに企業の評判に傷を付ける状況において[3]、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。

かつてないほど高まっているセキュリティのリスク

上位のサイバーセキュリティの脅威はすべて増加しています。[4]もはや驚くことではありませんが、そのはっきりとした理由が明らかとなっていません。



本書では、その核心に触れずにセキュリティのリスクについて語るつもりはありません。あえて言うなら、脅威の増加はサイバー攻撃者がこれまでやってきたことを別の攻撃者が同じように行うことが簡単であることが少なからず原因だと言えるでしょう。例えば、現代のエクスプロイトキットは経験の浅いハッカーでも使えるようにサイバー攻撃を簡易化しています。これらの悪意のあるツールキットは、事前に書かれたエクスプロイトコードと共に提供されるためにどのように機能するかを理解していなくても使うことができます。多くの場合、シンプルな Web インターフェースにより、ライセンスが付与されたユーザーはログインし、被害者や統計を確認できます。これらのキットには、市販されている合法なソフトウェアのように、サポート期間や更新も含まれている場合があります。

同じように、脅威の増加は元々サイバースパイやサイバー戦争を目的に開発された最先端ツールが、広く普及していることとも関係しています。

例えば単純な脅しのハッキングであったランサムウェアは、国家安全保障局（NSA）から盗んだセキュリティ上の弱点を突くツールをベースに企業を標的としたマルウェアへと進化し、コンピューターを人質に取り、システム全体を機能できない状態にロックするものになっています。これに加え、2016 年に送信されたスパムの約 40%にランサムウェアが含まれていた[5]という事実も合わせて考慮すると、無防備なユーザーがクリックすべきではないものをクリックし、企業を危険にさらすことはいつでも起こり得るということがわかります。

研究開発チーム IBM X-Force は、経営幹部社員の実に 2 人に 1 人が仕事でランサム攻撃を受けたことがあることを明らかにしています。これは実質的に企業の経営陣の半数ということになります。[6]

ユーザー：企業の最大の弱点

Verizon Data Breach Investigations Report（DBIR）は、セキュリティ業界において、最も評価されている年次報告書のひとつです。世界最大の IT 調査期間である Verizon Research, Investigations, Solutions and Knowledge（RISK）チームは毎年、最大の傾向を含むその年のサイバーセキュリティの状態について詳細な情報や見解を発表しています。

2017 年、RISK チームはセキュリティインシデントおよび情報漏洩の 90%以上でフィッシング攻撃が使用されていたことを明らかにしました。[7]

また、これらのユーザーを標的とした攻撃経由で、ランサムウェアやその他のマルウェアの被害に遭っている多くのデバイスを使用しているユーザーが同様に深刻な割合で増加しています。Verizon は、フィッシングメッセージの 30%（前年は 23%）が 2016 年に開封され、うち 12%のケースでユーザーが悪意のある添付ファイルやリンクをクリックしてしまったと報告しています。

Verizon 2016 DBIR では、3 方面からのフィッシング攻撃の増加について重点的に取り上げられています。

- 悪意のある添付ファイルや、悪意のある Web サイトへと誘導するリンクが含まれたフィッシングメールをユーザーが受信する。
- 機密情報や内部情報を検索し、キーロガー経由で複数のアプリケーションの認証情報を盗み、ランサム向けにファイルを暗号化するために攻撃者が使用できるマルウェアをユーザーがダウンロードする。
- 攻撃者は盗んだ認証情報をさらなる攻撃に使用できる（例えば、金融機関やリテールサイトなどサードパーティーの Web サイトにログインするなど）。

現代のサイバー攻撃がもたらす実質的損害

FBI は、犯罪組織が 2016 年の第 1 四半期に集めた額が 2 億 900 万米ドルと推定しており、年末までに 10 億米ドルを超えることを見込んでいます。2016 年の第 1 四半期以降、事態は悪化の一途をたどっています。事実、最近史上初となる 100 万ドルの身代金が支払われたことが公表されました。[8]

ただし、現代のマルウェア、そしてランサムウェアも、単に金銭を目当てにしたものではなくなっています。

実際、金銭を荒稼ぎするという点に関して WannaCry は成功しているとは言い難いですが（2017 年 6 月 28 日時点で約 13 万 5,000 米ドル）、わずか 1 日で、150 か国以上の 23 万台を超えるコンピューターが感染の被害を受けており、被害の拡大という点においては、大きな成功を収めていると言えます。そして企業に対する損害という点においても、企業をまったく屈服させなかったランサムの身代金よりもはるかに深刻になっています。ランサムに対する支払いが功を奏して損失したデータが復旧する保証はありません。にも関わらず、実害は、ダウンタイム、データ破損、生産性の低下、攻撃後の事業妨害、フォレンジック調査、データやシステムの復旧に及び、言うまでもなく企業の風評被害は顧客やパートナー、サプライチェーンにも影響を及ぼし、ずさんなコンプライアンス管理が明らかとなった場合は、罰金が科せられる可能性もあります。

FedEx、製薬会社 Merck、配送業界大手の Maersk が良い例です。この 3 社はいずれも今年 NotPetya の攻撃に遭い、それぞれが攻撃を受けてから数週間後、数ヶ月間後も、攻撃から脱するために取り組みを続けていることを認めています。FedEx は、攻撃から 3 ヶ月後にあたる 9 月末までにシステムの完全復旧の目途を立てており、損害額が 3 億米ドルとなることを予測しています。[9]Maersk も FedEx と同様の損害額を予測しており、Merck は重み付けし 2 億から 3 億米ドルの損害額を予測していると発表しています。[10]

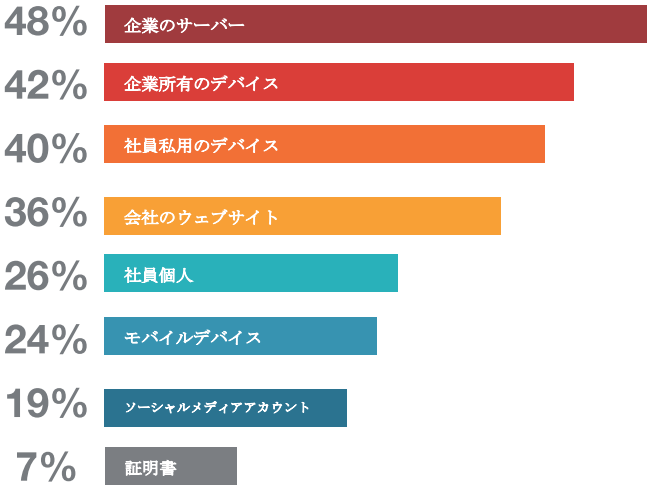
クライアントとサーバーを重視

想像できる限り最高の高性能セキュリティツールを所有している大企業でさえも、これらの攻撃の被害者になり得るのでしょうか？

ひとつ言えることは、導入されているツールの多くが脆弱な資産のほとんどを保護していないということです。

次のうち、この外部からの攻撃の一部として標的となったものをお答えください。

2016 年 Forrester が実施した Global Business Technographics Security Survey



自社の調査 2016 Global Business Technographics® Security Survey のために Forrester は、ここ 12 ヶ月の間に外部組織によるセキュリティの侵害被害に遭った企業（社員数 1,000 人以上）のネットワークセキュリティに関する意思決定を担当している方 192 名を対象にアンケートを実施しました。アンケートの質問の中には、外部組織による攻撃の標的となったインフラストラクチャの側面を回答する質問がありました。このアンケートの結果から、企業が一番重視しなければならないのは、IT 環境周辺ではなく、企業のネットワーク上のクライアントとサーバーであることが明らかとなりました。

的が絞られていないセキュリティ戦略はコストの無駄にしかならない

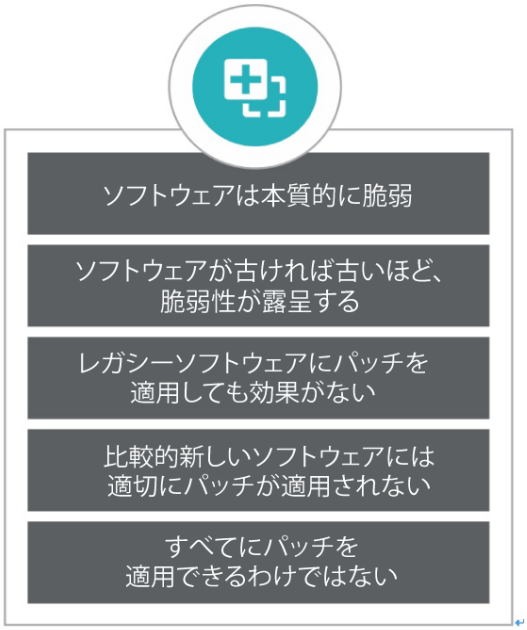
残念なことに、これらの脅威からシステムを保護するための適切なツールを導入しているとしても、それらは企業が設定し、毎日管理しなければならない数多くのツールのほんの一部に過ぎません。

ネットワークのファイアウォール、Web アプリケーションのファイアウォール、侵入防止システム、脆弱性スキャナ…数えきれないほどのツールがあるのです！デバイスの無秩序な増加にはコストがかかり、IT チームはこれらのデバイス管理にかなりの時間をとられています。このため、環境に実害をもたらす脅威に対する保護を確立し、対応するためのセキュリティに取り組む時間が削られています。

問題の解決にならないパッチ適用

さらに、たとえ適切なツールを導入していても、常に理想通りに機能するように最適化されているわけではありません。

例えばパッチを適用したからといって、問題は何も解決しません。WannaCry と NotPetya は、国家安全保障局（NSA）から盗んだセキュリティ上の弱点を突くツールと Windows ソフトウェアの一般的な脆弱性を組み合わせることで、急速に広がりました。ただし、WannaCry と NotPetya によって突かれた Windows ソフトウェアの脆弱性に対してはパッチが公開されていたのです。



- **ソフトウェアは本質的に脆弱：**何十万ものコードはすべて人間によって書かれています。異常や不具合が生じて当然だと言えます。エラーが一切なく、潜在的な攻撃者からの攻撃を受けないソフトウェアを書ける人はいません。
- **ソフトウェアが古ければ古いほど、脆弱性が露呈する：**Ivanti では、この状況を比喩的に「腐った牛乳」と表現しています。冷蔵庫の中に牛乳を放置している必須が長くなれば長くなるほど、牛乳は古くなります。そして最終的に腐ってしまいます。同様にソフトウェアが世に出てから時間が経てば経つほど、内在していた脆弱性が明らかとなり、露呈され、悪用されてしまいます。
- **レガシーソフトウェアにパッチを適用しても効果がない：**これは鉄の掟ではありません。例えば、WannaCry による攻撃が行われた後、この脅威には拡大する性質があると仮定し、Microsoft は先を見越して自社のサポートされていないオペレーティングシステム向けのパッチをリリースしましたが、概して脆弱なレガシーソフトウェアの更新に期待はできません。
- **比較的新しいソフトウェアには適切にパッチが適用されない：**WannaCry 以前は、サポートされているオペレーティングシステムに対してパッチが公開されていました。そして、先ほど触れた通り、WannaCry による攻撃以降は、サポートされていないシステムに対してパッチが公開されています。このようにあらゆるパッチが利用でき、WannaCry による攻撃を受けたばかりであるにも関わらず、企業はわずか 1 ヶ月後に NotPetya の被害に遭っているのです。おそらく、被害に遭った企業は、自社環境全体にわたって総合的にパッチを適用するツールを導入していなかったのかもしれません。もしくは、限られた人材が速やかに対応したものの、時間通りに対応を取ることができなかったのかもしれません。理由は何であれ、パッチが公開されているからといって、期待されている通りにパッチが適用されているわけではないということです。
- **最後のポイント -すべてにパッチを適用できるわけではない：**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。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。

お客様から寄せられているその他の問題

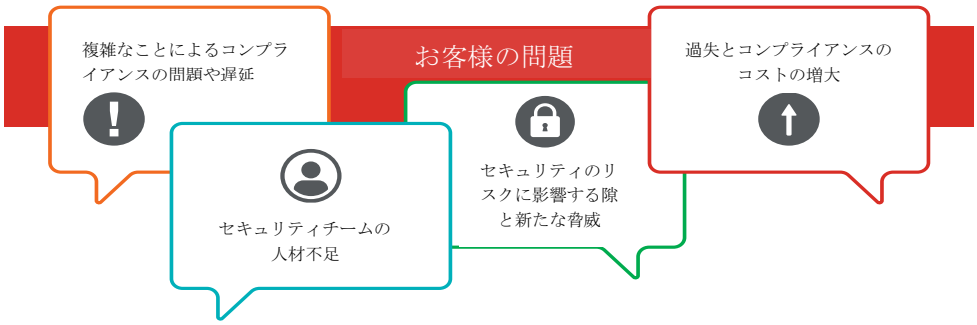
当然これ以外にもサイバーセキュリティに関する問題はたくさんあります。簡単に言えば、IT 部門とセキュリティ部門は懸命に取り組んでいるものの、失敗者に仕立て上げられているのです。

IT 部門とセキュリティ部門がその場しのぎのソリューションを導入しているため、サイバーセキュリティが寄せ集めのような状態になっていませんか？様々なソリューションの寄せ集めでは全体としてうまく機能せず、環境へのリスク全体を集約した形で確認することができません。Cisco 2017 Annual Cybersecurity Report では、セキュリティの専門家の 55%が最低 6 社のセキュリティベンダーを利用していると報告されています。

これは周知の事実となっているサイバーセキュリティ分野の人材の不足によって悪化しています。クリティカルなアラートがどれかを判断し、そのアラートが発生している理由を特定する人材もしくはツールがなければ、セキュリティの専門家は多くの場合すべてのアラートの調査をまとめてスキップせざるを得ないのです。事実、同レポートでは、ほぼ半数のアラートが調査されていないと報告されています。

これらの調査されていない脅威が生産性や顧客満足度、企業の信頼性にもたらす影響を想像してみてください。

そして、複数のベンダーからの様々なソリューションとプラットフォームが混在していることが原因で、実は攻撃を開始できる「隙」ができてしまい、リスクや損害が増大し、すでに働きすぎのチームや IT ガバナンスにさらなる負担を課すことになっているという現実について考えてみてください。



今後見込まれる高い兵器化されたマルウェア

現代のハッカーには、医療機関や銀行のシステム、電力網など、世界中のクリティカルなインフラストラクチャに大きな影響を及ぼす能力があることは間違いありません。特に、レガシーソフトウェアなど経年劣化した技術や脆弱な技術に目を付けた場合、その影響は計り知れません。また、彼らはますます世界中のクリティカルなインフラストラクチャに影響を及ぼそうとしているように見えます。

まさに悪夢のシナリオです。元々最先端のツールはサイバースパイを目的としたものであることや、あらゆる種類のサイバー犯罪に対して戦争を行う体制が整っていることが少なからずサイバー攻撃が巧妙になっていることや、趣旨が変わってきていることの理由となっています。

WannaCry は、世界中の医療機関、銀行、企業のコンピューターの機能を停止しました。イギリスの病院は、人質に取られたコンピューターに対処する間、患者の受け入れを拒否しなければならない事態となりました。NotPetya に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。さらに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など大手企業が NotPetya に感染しました。NotPetya に感染した世界大手の輸送会社は、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。

セキュリティや IT の専門家は、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かつ悪辣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。

IT 部門を成功に導く、的を絞った戦略

満足のいく効果が得られるセキュリティ戦略には、数多くの要素があります。あらゆる状況に対して様々な防御オプションを提供する多層アプローチが最も効果的です。攻撃する「隙」をなくしましょう。

徹底した防御を実現する

- *リスクの全容を把握*
- *攻撃対象領域を軽減*
- *悪意のあるアクティビティを検出*
- *問題解決のための措置を取る*
- *問題を理解するためデータを分析*

セキュリティを簡易化、自動化し
対応時間を改善

- 自社の環境で何が起きているのか全容を把握してください。何が起こっているのか把握していなければ、何も保護できず、何に対して防御が必要なのかわかりません。
- 攻撃対象領域を軽減してください。自社のセキュリティ機能とチームにセキュリティを潜り抜ける脅威を追跡し捉えるわずかなチャンスを提供するため、マルウェアやエクスプロイトの実行を防止してください。
- 実行後悪意のあるアクティビティを検出してください。
- 悪意のあるアクティビティと潜在的な脆弱性に対応し阻止してください。
- 自社のセキュリティ体制とコンプライアンスに情報を提供する豊富なデータを使って自社の取り組みを明らかにしてください。

さらに、セキュリティプロセスを自動化するためのよりシンプルで能率化されたツールも必要です。自動化はすでに多忙極まりない人材から検出や調査の負担を減らす上で役立ちます。

最後に、ユーザーの生産性を保護し、さらに向上させる脅威軽減方法を探す必要があります。なぜなら、自分の仕事が滞りなくできなくなると、ユーザーはヘルプデスクに問い合わせる回数が多くなり、シャドーIT（個人用のデバイスを許可なく使用すること）を選択するユーザーも出てくるからです。これは企業の環境にリスクをもたらすことにつながります。

セキュリティとユーザーのニーズのバランスを取る

- *ユーザーについて理解を深め、ユーザーのニーズを見出す*
- *業務を妨害せずにセキュリティを提供する*
- *アップグレードやリスクを回避せずにユーザーを煩わせずにサービスを提供する*
- *適切なツールで生産性を向上する*

CIS のベンチマークを遵守し目指すビジョンを実現する

このビジョンを実現する最善の方法は、揺るぎないセキュリティフレームワークを利用することです。共通のプロセスと優先される一連のアクションをベースにした的が絞られたセキュリティソリューションを推進するこ

とにセキュリティチームと IT 事業チームが連携して取り組めば、コストが削減され、対応にかかる時間が短縮されます。

米国インターネットセキュリティセンター（CIS）などサイバー環境を監視している機関はこの見解に同意を示しており、サイバーセキュリティのベストプラクティスを特定、検証、推進し、導入を管理するため、持っている知識や専門技術を提供してくれています。NSA での実体験を基に構築されたプラクティスから生まれた CIS のクリティカルセキュリティコントロールは、サイバーセキュリティに関するガイダンスの主な情報源の多くをサポート、反映しています。

クリティカルセキュリティコントロールの最終的な目標は、防御の第一歩を速やかに設定し、すぐに価値の高いメリットを得るため不足している人材をアクションに割り当て、企業固有のさらなるリスクに集中できるよう、企業を支援することです。

- アクションの優先リスト
- すぐに得られる価値の高いメリット
- 規制遵守
- 実際に攻撃された経験から学ぶ

実証されたフレームワークを活用し、企業のすべてのエリアで求められている要件のほぼすべてに対応できる単一ベンダーのソリューションを見つけ、具体的なニーズを特定できたエリアにピンポイントのソリューションを提供することで、企業が求めている徹底した防御を提供する効果的な戦略を実現できる一方、コスト削減にも貢献できます。

研究者と CIS のケーススタディからは、CIS のベンチマークを遵守して IT システムを設定することにより、既知のセキュリティの脆弱性の 80～95%を排除できることが明らかとなっています。

CSC 上位 5 コントロールで速やかにセキュリティを次のレベルへ

特に、CIS のクリティカルセキュリティコントロールの上位 5 コントロールは、企業のセキュリティ体制を抜本的に改善するための揺るぎない基盤を構築します。だからこそ、上位 5 コントロールは、「Foundational Cyber Hygiene」（サイバー攻撃に対する基本的な予防策）と呼ばれています。

1. **許可されたデバイスと不正デバイスのインベントリ**
   CIS の通り：[11] “Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.”
2. **許可されたソフトウェアと不正なソフトウェアのインベントリ**
   上記の通り。ただし、ソフトウェアの場合：「許可されたソフトウェアのみがインストールされ、実行できるようにし、さらに、管理されていないソフトウェアを見つけ、インストールや実行を妨げることができるように、ネットワーク上のすべてのソフトウェアを積極的に管理（インベントリ、追跡、修正）してください」
3. **ハードウェアとソフトウェアのセキュアな設定**
   「攻撃者による脆弱なサービスや設定への攻撃を妨げるため、厳しい設定管理と変更管理プロセスを使用してノートパソコン、サーバー、ワークステーションのセキュリティ設定を構築、導入、積極的に管理（追跡、報告、修正）してください。（メーカーやリセラーから提供された通りのオペレーティングシステムとアプリケーション向けのデフォルトの設定は通常、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。）」
4. **継続的な脆弱性の評価＆修正**
   「脆弱性を特定し、修正を行い、攻撃者にとって攻撃の機会を最小限に抑えるため、継続的に取得、評価、措置を取ってください」
5. **管理者権限の制限された使用**
   「管理者権限の誤用は、標的としている企業の社内で感染を広めるために攻撃者が主に使用する方法です」「コンピューター、ネットワーク、アプリケーション上で管理者権限の使用、割り当て、設定を追跡/管理/防止/修正するため」のプロセスとツールを提供してください。

徹底した防御を実現する当社のソリューション

重要事項：必ず自社のビジネスクリティカルな資産すべてについて、CIS のクリティカルセキュリティコントロールと照らし合わせて既存のセキュリティコントロールと比較してください。すでに実行しているサブコントロールと、まだ実行できていないサブコントロールを正確に特定してください。その後、特定した「隙」と具体的なビジネス上のリスクや懸念事項を基に、速やかに上位 5 コントロールを実行するための措置を取り、他のコントロールを実行するための戦略的な計画を立ててください。

当社がサポートいたします。Ivanti は、お客様が IT 事業部門とセキュリティ部門の足並みを揃え、顧客のサイバーセキュリティのニーズに応えることができるよう、上位 5 コントロールおよびそれ以外の CSC コントロールに対応する的を絞った総合的な製品ポートフォリオを提供しています。

Ivanti のソリューションを支えているのは、ディスカバリ、パッチ管理、アプリケーション、デバイス管理、管理者権限管理、セキュアな設定など自動化された機能、すなわち CIS の上位 5 コントロールに欠かせない要素です。さらに、Ivanti はこれらのコントロールを首尾よく、経済的かつ簡

単に、ユーザーの生産性に及ぼす影響を最低限に抑えて実行できるようお客様を支援します。したがって、ユーザーはアクセス権を付与してもらう

ために 5 分毎にサービスデスクに問い合わせる必要がなくなります。また、不正な、安全でない、シャドーIT（個人用のデバイスを許可なく使用すること）が排除されます。ただし、事業はこれまで通り滞りなく進めることができます。

当社は状況把握も支援します

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するため、オンデマンドのデータに加え、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ボックスに変えます。

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。

結論

無駄なことにお金を使わないでください。また、セキュリティ部門や IT 部門は必要なリソースや専門知識・技術がない状態で企業を保護するために必要な対策を提供するために懸命に取り組んでいますので、彼らを悩ませないでください。大きな変化をもたらすために最も重要な業務に集中できるように、効果的なサイバーセキュリティプログラムを導入しましょう。そして、主なセキュリティのニーズを満たすソリューションを選択し、巧妙かつ広範な影響をもたらす現代のサイバーセキュリティから自社環境を防御するための保護を強化しましょう。

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

1 Privacy Rights Clearinghouse

2 https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/

3 Verizon 2016 Data Breach Investigations Report (DBIR)

4 EY’s Global Information Security Survey 2016-17

5 2016 IBM X-Force research, http://www-03.ibm.com/press/us/en/pressrelease/51230.wss

6 Op. cit.

7 Verizon 2017 DBIR

8 https://arstechnica.com/security/2017/06/web-host-agrees-to-pay-1m-after-its-hit-by-linux-targeting-ransomware/

9 https://www.infosecurity-magazine.com/news/fedex-notpetya-cost-us-300-million/

10 http://files.shareholder.com/downloads/ABEA-3GG91Y/5005768664x0x954059/3E9E6E5C-7732-4401-8AFE-F37F7104E2F7/Maersk_Interim_Report_Q2_2017.pdf

11 https://www.cisecurity.org/controls/