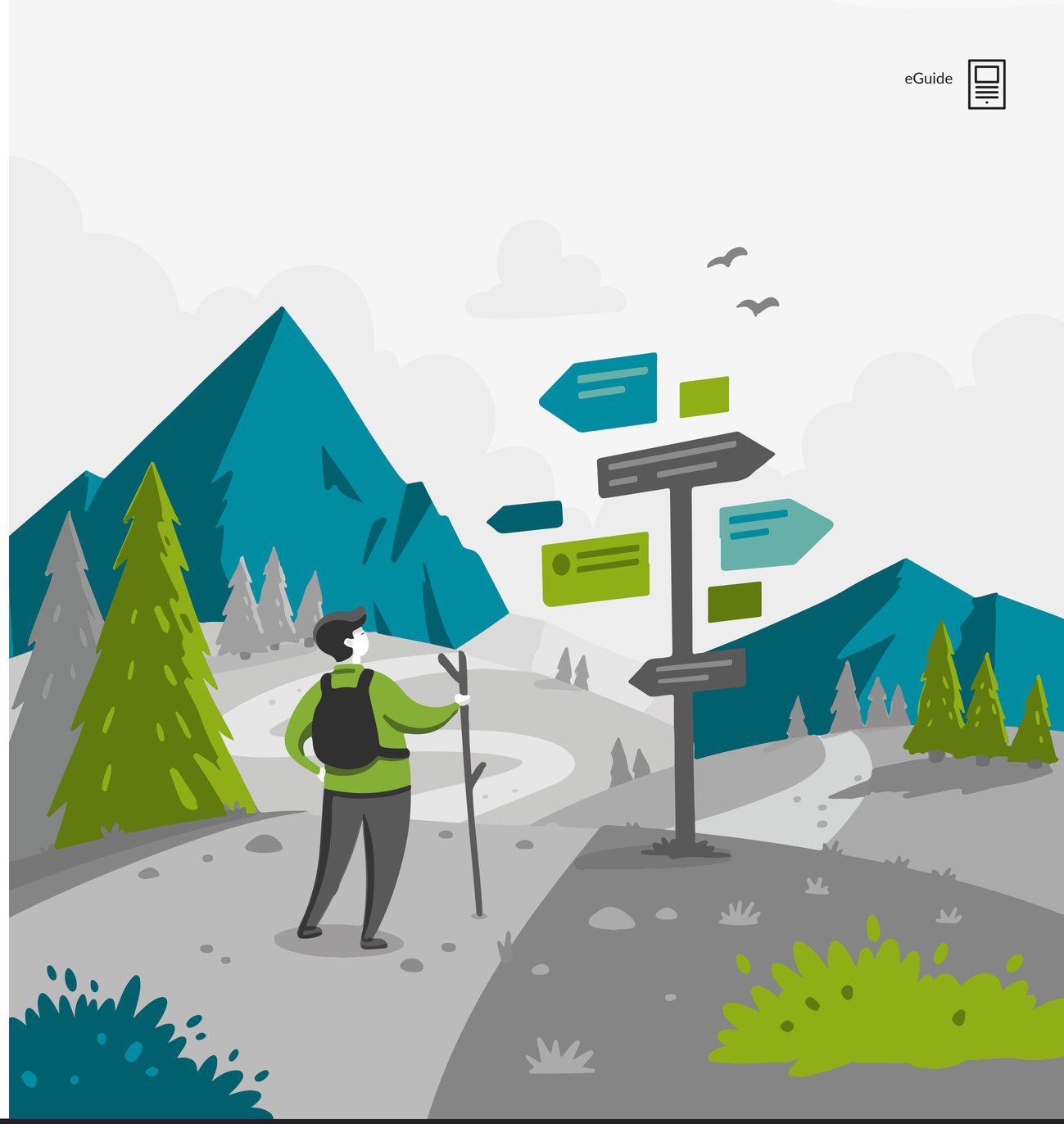
JUNIPER NETWORKS | Engineering Simplicity

eGuide

サイバーセキュリティの基本を理解する

文：トレバー・ポット
テクニカルセキュリティリード、ジュニパーネットワークス



はじめに

この文書では、情報セキュリティの基礎、その役割や重要性を解説します。

情報セキュリティは、原則やツール、テクニック、技術、製品、サービス、実践など、情報保護に関するすべてを指します。情報セキュリティは人に始まり人に終わります。危殆化の発生は、ほとんどの場合何らかの人為的ミスが原因です。

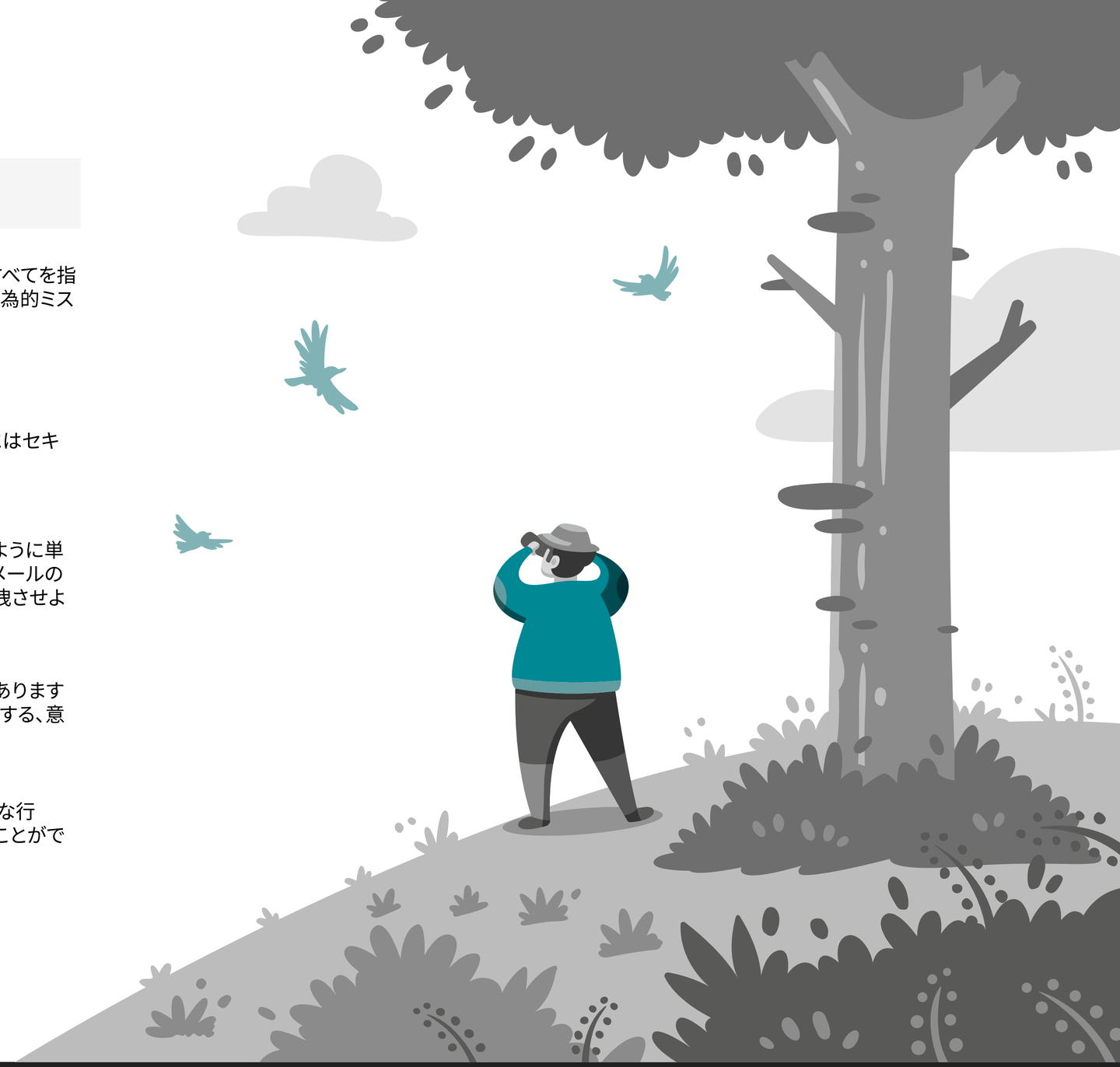
人為的な危殆化は、主に**無知、ソーシャルエンジニアリング、過失の3つに分類されます。**

無知とは知識不足のことですが、知らないことを知っていると思い込んでしまったときにはセキュリティ上のリスクにもなりえます。

ソーシャルエンジニアリングには、「Microsoftの技術者」を名乗る人からの偽の電話のように単純なものもあれば、巧妙に作られた偽のウェブサイトに誘導するスピアフィッシングのメールのように手の込んだものもあります。あなたのアカウントにアクセスするための情報を漏洩させようとすることが狙いです。

無知である可能性や、ソーシャルエンジニアリングに騙されてしまう可能性は誰にでもありますが、過失は選択の結果です。自己研鑽やタスクの実行などの何らかの職務をおろそかにする、意図的な選択をしなければ起こりません。

幸いなことに、攻撃をブロックしたり、運用担当者にリマインダーを送ったり、悪意のある行動や異常な行動、過失と思われる行動を検知したりする技術を使って、情報セキュリティの危殆化防止に役立てることができます。



基本的なIT情報セキュリティ

データとメタデータ

情報の多くはどこかのコンピューターにデータとして保存されています。ファイルやデータベースだけでなく、写真やWord文書、記録などの形もあります。

メタデータとも呼ばれる情報についての情報も重要です。

写真には多くの場合、GPS座標や画像を撮影したデバイスの詳細など、関連するメタデータがあります。画像をソーシャルメディアに投稿する際にこうしたメタデータを削除していなかった場合、悪意のある何者かによって、個人を特定できるようにターゲットの位置や、電話の機種を特定するために使われる恐れがあります。

誰かが食べ物と自撮りをして、ソーシャルメディアのメッセージに添付したとしましょう。そこから泥棒は場所と時間を特定できます。簡単な計算で、泥棒が盗みを働く前にその人が家に帰ってこられるかどうかを判断できます。

メタデータから企業秘密が明らかになることもあります。電気技術者が、まだ未発表の新しいデータセンターで完了したばかりの配線工事について写真を投稿した場合、メタデータを見ている人なら誰でも、その場所を簡単に特定できてしまう恐れがあります。同様に、Word文書には過去に編集した人全員の履歴が残されていることが多く、法的な問題につながる恐れがあります。

ファイアウォールやマルウェア対策だけでは不十分

従来のファイアウォールやマルウェア対策は、単体ではあまり効果的ではありません。

従来のファイアウォールは、何者かによるPCの遠隔操作を防ぐことならできまが、クリックしてしまった場合に、ファイアウォールの内部で機能する遠隔操作アプリケーションがダウンロードされたり、PCへの遠隔アクセスを許可するようにファイアウォールの設定が変更されたりするリンクが含まれた、フィッシングメールをフィルタリングすることはできません。

同様に、マルウェア対策のアプリケーションは、すでに知られているタイプの悪意あるファイルに対する防御にはとても効果的ですが、これまでに見たことがないものに対してはあまり効果がありません。また、インターネット ブラウザーを通じてPCに忍び込んでくる様々な脅威に対してはほとんど無力です。

企業では、大半の情報セキュリティ製品やサービスがインフライトデータ、つまり転送中のデータに注力しています。進行中の脅威が何であれ、ユーザーに届く前、またはネットワークを離れる前に認識することが狙いです。

次世代情報セキュリティ

1990年代、アプリケーションと外の世界の間でプロキシとして機能するアプリケーションレイヤーファイアウォールが使われるようになりました。その後、NGFW（次世代ファイアウォール）が登場しました。NGFWは組織のインフラストラクチャにより統合されていて、IPだけでなくユーザー名やグループに基づいたポリシーの適用などの高度な機能を提供します。

一般的にNGFWは、単純な攻撃を使う悪者による外部からネットワークへの侵入を防ぎます。また、フィッシングの試みについてメールをスキャンするなど、インフライトデータを何らかの形でスキャンする機能も提供します。NGFWは、何千人ものユーザーを一度に保護することができ、ウイルス対策による保護を使えないプリンターなどのエンドポイントを防御することもできます。

NGAM（次世代マルウェア対策）またはNGAV（次世代ウイルス対策）は、それがインストールされているホストしか防御できません。そのため、ソーシャル エンジニアリング攻撃に対する防御のためにNGFWと併用されます。

NGFWはPCに脅威が到達すること自体を食い止めようとします。これが最善で最も安全な選択肢です。

NGAM（またはNGAV）は、脅威がPC内部に入り込んだ後、それによる危殆化を防ごうとします。防御の最終の砦（とりで）です。

基本的なIT情報セキュリティ

WAFとアプリケーションセキュリティ

進化の過程における次のステップは、WAF（ウェブアプリケーションファイアウォール）です。WAFはHTTPやHTTPSで提供されるアプリケーションに注目したアプリケーションレイヤーファイアウォールであり、一般的に（ネットワーク内や外部から）インターネットを通じてアクセスされます。

WAFは、特定のアプリケーションやアプリケーションの種類に特有の脆弱性を保護します。たとえば、WAFは悪意のあるSQLコマンドをフィルタリングして実行されるのを防ぎます。多くの場合、WAFは内部の脅威から保護するために内部的に使われます。また、あるアプリケーション層が危殆化したことによって別のアプリケーション層に影響が及ぶことを防ぎます。

アプリケーションセキュリティは、セキュリティを提供するにあたりファイアウォールやマルウェア対策、およびその他の外部製品やサービスに常に依存することはありません。

従来型のアプリケーションセキュリティでは、アプリケーション自体の中で直接、保護レイヤーが構築されています。PC上のマルウェア対策アプリケーションと同様に、アプリケーションセキュリティはサーバーベースのアプリケーションにとって防御の最後のとりでです。攻撃がそこまで到達してしまった場合、その過程にある情報セキュリティで何か大きな問題が発生しています。

多層防御

今日の脅威から単独でネットワークを防御できるベンダーはありません。また、新たに出現する脅威に対抗する革新的で新たな手法を模索するには、人手も研究開発能力も足りません。

現代のネットワークを防御するための現実的な唯一の方法は、複数のベンダーから提供される複数の製品を緊密に連携させ、何重にもわたる多層防御を実現することです。

暗号化とDLP

暗号化とDLP（データ紛失防止）はネットワーク内のデータが外部に流出することを防ぐために
設計されています。

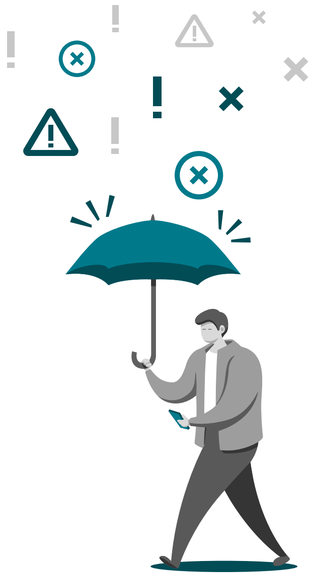
暗号化技術によって、正しいキーを持つ人やアプリケーションだけがデータにアクセスできるようになります。

たとえば、暗号化されていない顧客ファイルが入ったセールスマネージャーのノートPCが盗まれた場合、組織に対する損害はとても大きくなる恐れがあります。

インフライトデータの暗号化は、データが第三者によってのぞき見されないようにするために使われます。インターネットを通じて提供されるサービスにアクセスするときや、無線ネットワークを通じて何かにアクセスするときには欠かせません（インターネットも無線ネットワークも、100%セキュアということは絶対にありえません）。

DLPの基本的な手法では、ネットワークの外に出ようとするデータをスキャンし、外に出るべきでないものであれば遮断します。NGFWやNGAVに組み込まれていることが多く、たとえば、ある種の内容が含まれたファイルがフラッシュドライブにコピーされたり、（Dropboxなどの）クラウド上のストレージフォルダにアップロードされることを防ぎます。

DLPは多くの場合、CASB（クラウドアクセスセキュリティブローカー）やATP（高度脅威保護）製品を含むセキュリティツールに組み込まれています。これらはたとえば、クレジットカード情報が入ったスプレッドシートの送信を検知し、通知を行うかブロックします。



しかし、ネットワークからデータをこっそり持ち出す方法は他にもたくさんあります。Slackやソーシャルメディアなどはいずれも、現代のDLPではうまくカバーできていません。

基本的なIT情報セキュリティによる防御

監視

監視がなければ、IT専門家は何が起きているのか、あるいはどんな問題に対応しなければいけないのかを知ることができません。監視製品の多くは逸脱や相関関係を使ってパターンを発見します。

逸脱は、リアルタイムで作業負荷やシステム間のデータの流れを観察して「正常」な状態を表すベースラインを設定し、その正常な状態から外れた場合に認識します。

相関関係に基づく監視は、問題を示唆する複数のイベントが同時にまたは連続して発生しないかを見張ります。通常は、アプリケーションやインフラストラクチャコンポーネントから生成されるイベントログに基づきます。

理想的な監視ベースのDLPシステムは、組織のITインフラストラクチャ全体にわたるデータアクセスを検証し、異変を発見するものです。つまり、たとえば、普段は1日に数件の取引先情報にしかアクセスしないセールスマネージャーが、その地域の全取引先の情報に突然アクセスしたら、何かおかしなことが起きているかもしれないとシステムが気づきます。この手法では、複数のベンダーから提供される複数の製品を連携させる必要があります。

しかし、組織のデータをすべて完全に監視することは不可能です。企業は、オンプレミスとパブリッククラウドの両方において、数千もの異なる場所やシステム上にデータを持っている可能性があります。

組織がすべてのデータアクセスを監視できたとしても、それをどうするかという問題もあります。異常なアクセスパターンはデータを盗もうとしている従業員によるものかもしれませんし、外部の攻撃者による危殆化事象が発生しているからかもしれません。はたまた、単に誰かが自分の業務をこなしているだけかもしれません。こうしたパターンを微調整する手段として、機械学習が使われることが増えてきています。恐らく、この先数年のうちに大きな発展があることでしょう。

SIEMとATP

SIEM（セキュリティ情報・イベント管理）製品は情報セキュリティの中核で、ATP製品と密接に関係するようになってきています。SIEMはいくつもの製品からデータを受け取ります。便利なものの中には、複数のベンダーの主力製品と素早く簡単に統合できるものもあります。

SIEMやATPの中でも最も人気のある製品は、相関関係に着目しています。次の例を見てみましょう。

1. NGFWがメールデータのストリームをATPに送ると、ATPがそのユーザーを標的にした、マルウェアの含まれるメールの数々を検知します。
2. ATPはメールの受信を防ぐようファイアウォールに指示します。
3. その後まもなく、そのユーザーのエンドポイントのNGAVがおかしな挙動を検知します。
4. エンドポイントがクラウドストレージサイトに接続し、文書をアップロードしようとしていることをCASBが検知します。

各イベントに対するアラートの重要性が低いものであっても、ATPが相関関係を見出せれば、恐らく標的型攻撃が行われていると判断でき、最高レベルの脅威を宣言して人間の関与を求めることができます。

SIEMは主にイベントや監視のデータを収集しますが、ベンダーの多くがスキャン機能を追加したり、DLPを組み込んだり、DLPが実装されたアプリケーションとの統合を可能にし始めています。

基本的なIT情報セキュリティによる防御

アクセス制御、VPN、および遠隔アクセス

暗号化をはじめとする情報セキュリティ技術のおかげで、ストレージデバイスに物理的なアクセスができても実際のデータにはアクセスできない、ということが可能になります。同様に、クラウドコンピューティングを使うと、根底にあるハードウェアに一切アクセス権を与えることなく、組織が世界中のどこからでも製品やサービス、データにアクセスできるようになります。

ほぼあらゆるITインフラストラクチャ、オペレーティングシステム、アプリケーションには、何らかのアクセス制御があります。アクセス制御の最も重要な方法の2つに、VPN（バーチャルプライベートネットワーク）と遠隔アクセスが挙げられます。

VPNは2台のコンピューターシステム間の暗号化されたネットワークトンネルです。個人が組織のプライベートネットワークに安全に接続し、サイト間のセキュアなリンクを確立するために使用されます。悪意のある何者かによるのぞき見から保護するために、暗号化も使われます。

遠隔アクセスとは、個人がVPNを利用することなく組織のリソースにアクセスできるようにする技術を総称して使われる用語です。

ブラウザーの防御

メールを除けば、Webブラウザーは恐らく、外部の攻撃者がユーザーのデバイスやエンドポイントを危殆化させるために使う可能性が最も高いルートです。

今日のWebブラウザーはいまだにかなり脆弱です。情報セキュリティ危殆化のうち3番目に多い方法である、ユーザーによるインターネットからのファイルのダウンロードと実行を許可してしまいます。

ChromeやFirefoxなどの人気のWebブラウザーでは、AdblockやGhostery、Privacy Badgerなどの拡張機能をインストールできます。これらの拡張機能はマルバタイジングなどのインターネット上の様々な脅威に対する保護を提供するほか、Webブラウザーによるインターネット上の疑わしいリソースへの接続リクエストの試みを防ぐためのものです。

NGAVベンダーが提供するものをはじめとする、その他のブラウザー拡張機能は、危殆化したリソースへのアクセスを求めるリクエストの完了を防ぐことで、エンドユーザーの保護を試みます。

基本的なIT情報セキュリティによる防御

MDM

MDM（モバイルデバイス管理）製品は、携帯電話やタブレット、ノートPCなど、組織の敷地外で使われるデバイス用に設計されています。遠隔デバイスやモバイルデバイスにセキュリティテンプレート、プロファイル、ポリシーを適用し、会社の敷地内にあるリソースに接続できるようにする前に、組織の情報セキュリティ要件を満たしていることを確認します。

MDMは、アプリストアや仮想デスクトップインフラストラクチャ（VDI）といったソリューションを通して、セキュアなアプリケーション配信を提供します。MDM製品はまた、アクセス制御に対応し、承認されたユーザーのみがデバイスを使用できるようにして、盗まれたり紛失した場合には追跡やリモートワイピングを有効にします。

認証

一元化された認証と統合認証（UA）の技術は、LDAP、SAMLやMicrosoftのアクティブディレクトリーなどのディレクトリサービスに依存します。シングルサインオン（SSO）は最もよく知られているUAテクノロジーで、複数の異なるインフラストラクチャ上にある複数のプロバイダーからワークロードやサービスにアクセスするために、ユーザーが一つのユーザー名とパスワードを使用できるようにします。

多要素認証（MFA）システムもまた広く使用されていますが、例えば、国ごとに変える必要がある場合、複雑になる問題を招くことがあります。例えば、SMS検証（よく使用されるMFAアプローチ）は、ユーザーがテキストメッセージからコードを入力してログインする必要がありますが、SMSメッセージに制限を課している国は多くあり、これにより信頼性が失われたり、適切に機能するために追加の統合が必要となる場合があります。

自動化

管理下に置く必要のあるワークロードの量と多様性はますます急増しています。ITが変貌するスピードは衰えることがなく、人間がサポートなしに追いつくことは不可能です。ここで自動化が登場します。

自動化は、最も重要な情報セキュリティーの防御です。

今日の様々な形で接続されているIT、急速に消滅するネットワークの境界線、そして脅威が周囲から起こり得るという事実から、情報セキュリティはITのあらゆる側面の一部となる必要があります。ITインフラストラクチャ、ワークロード、そしてネットワークに接続されているすべてのデバイスが、組織の情報セキュリティ設計の一部とならなければなりません。

攻撃の分析

目的の定義

ハッカーを想像してみてください。ボブと呼ぶことにします（女性のハッカーもいますが、統計的には犯罪者は男性の方が多いのです）。ボブのターゲットは、地元のインターネットサービスプロバイダであるPotatoComです。PotatoComは、何年もの間何度も光ファイバーインターネットの設置を拒否しており、ボブはひどいADSLにうんざりしています。ボブは復讐行為として、PotatoComの金融システムに不正アクセスし、データベースにアクセスできないようにしたいと思っています。

計画を実行すべくシステムを支配するために、ボブは非常に優れた技術者になる必要はありません。目標を達成するために十分に学習するだけで良いのです。

接続性

ボブは、追跡されないように不正のオンラインアクティビティを遂行する方法を見つける必要があります。コーヒーショップで安全でない公共Wi-Fiを使用できますが、そこに向かう途中を含めて監視カメラに映らずに行う必要があります。避けることができない（または検出できなかった）カメラがある場所を通過した場合に備えて、物理的に変装する必要があるかもしれません。

目立ったアクティビティパターンを作ってしまわないように、同じWi-Fiホットスポットは決して二度使用せず、さまざまな無料Wi-Fiがある場所にたどり着くため、さまざまな交通手段を使用します。接続するのに十分に接近できるのであれば、無料のWi-Fiを提供する建物に入る必要もありません。

ボブは、彼自身のアクティビティを彼が使用しているネットワーク上の監視技術からも隠す必要があります。おそらく、VPNか複数の手段を使用する必要があるでしょう。また、攻撃を実行する場所としてVM（仮想マシン）または仮想プライベートサーバーを借りることもできます。インターネットトラフィックをさらに隠すために、おそらくTOR、I2P、またはその他の匿名化と暗号化を行う方法も使用します。

支払い

オンラインにアクセスするたびに、ボブはUSBフラッシュドライブ、ノートパソコン、2つのVPNサービスアカウント、2つの個人用仮想マシンのレンタルを購入する必要があります。そのため、特定されることなくこれを実行できる方法を考える必要があります。これを実行する方法はあります。複雑になるかもしれませんが、可能性はあります。簡単に言えば、ボブは追跡されずにどこででも使用できるプリペイドカードに、現金を何とか（法的に）変換することがでます。

調査

ボブはPotatoComが使用するデータベースとバックアップシステム、そしてシステムに侵入する方法を見つける必要があります。彼は、PotatoComのITインフラストラクチャを調査する技術的手段を利用できます。さまざまなPotatoComの従業員とチャットするためにソーシャル エンジニアリングを利用し、知識豊富な個人（または内部者）として自身を偽り、従業員から聞き出す機会を得ます。こういったやり方は通常上手く行きます。彼はPotatoComの従業員が使用するツールについて文句を言う従業員を探すことで、ソーシャルメディアで必要なものを見つけることもできます。複数のベンダーのサポートラインに電話してPotatoComの従業員を偽り、PotatoComが顧客であることを確認することもできます。

攻撃の分析

システムへの侵入

システムに侵入する最も簡単な方法は、ログインするための有効な資格情報を提供するように誰かをしむけることです。管理者の資格情報は必要ありません。変更できなくても、インフラストラクチャを見ることができるユーザーなら誰でもかまいません。そこからインフラストラクチャを調査し、ソフトターゲットを攻撃するためにラテラルムーブメントを使用してネットワークスキャンを使用できます。システムに複数のバックドアがあれば、技術的なやり方でデータベースに入り込みエントリーを破損することができますが、これは難しい方法です。

PotatoComのセキュリティを破壊するためにボブが必要なものは、管理者パスワードだけです。

単一のクラウドプロバイダにすべてのインフラストラクチャが保管されていました。ですから、バックアップに使うものと同じ管理資格情報を、本番環境でも使用している可能性があります（セキュリティ上賢い選択ではありませんが、実際にありえます）。

ターゲットを把握する

ボブが管理者の資格情報を持つ誰かを利用できる可能性は低いと考えられます。こういった人物は、セキュリティをより重視する傾向にあるからです。ですから、ボブは適切なターゲットを特定して、物理的な監視を使用します。

ボブはターゲットについて把握し、そこで得た知識を使って、手に入れたい管理者の資格情報を入手できる脆弱性を見つけるために、あらゆる手段を試みます。

例えば、自宅がオフィスほど安全になることは決してなく、自宅にいる人をスパイする機会はたくさんあります。ターゲットが在宅ワークをしていない場合、オフィスはどこにあるのでしょうか？ボブはオフィスに侵入するためになりすますことができ、カメラやキーロガーを仕掛け、Windowsからスパイしたり、無線キーボードから信号を傍受することもできます。

ハッカーのように考える

PotatoComのインフラストラクチャに接続できた後、ボブはレポート機能の変更を無効にし、データベースを破損させます。その後バックアップして古いバックアップを削除し、PotatoComのパスワードを変更して証拠を隠滅します。

PotatoComの財務データベースは今や使えないものとなり、何が起こったか把握するためにアカウントにアクセスすることもできません。顧客に請求したり、サプライヤーに支払ったり、納税することもできません。監査の対象となる可能性もあり、必要なデータにアクセスできない問題が発生する場合があります。倒産する可能性さえあります。

ボブにとって、技術的に難しいことはありませんでした。最も重要なことは発想です。ボブは、特定されないようにするため、大いに時間をかけました。最も簡単な方法を探し求めました。ほとんどのシステムで攻撃に利用できるものは通常人間が担当しています。そのようにハッカーは考えるのです。

ハッカーに対抗するために防御側に必要なことは1つだけです。安全を第一と考える発想です。

防御者はハッカーと同じように考え、セキュリティ上の弱点を探し、技術、ビジネスプロセス、あるいは窓のカーテンなどで、その隔たりを埋める必要があります。守るものを把握できれば、防衛側が使用するべきツールもわかります。ハッカーと同じように、発想が重要です。

高度な概念

規制の順守

単に情報セキュリティ技術を実装したり、チェックボックス方式でITポリシーを適用することで監査をパスするだけでは十分ではありません。組織は基本を実際に理解し、情報セキュリティが必要な理由を実証することを求められています。

例えば、欧州連合（EU）の一般データ保護規則（GDPR）では、大規模なデータを処理する組織に対して、データ保護責任者（DPO）の設置を要求しています。DPOは組織によるGDPRへの遵守を確保する責任を負い、DPOや組織がEU市民のデータ保護を怠った場合、個人的かつ重大な財政上の影響が発生します。

セグメンテーションとマイクロセグメンテーション

ネットワーク管理者は、ネットワークの境界防御を破ることに成功した攻撃者のラテラルムーブメントを防ぐために、セグメンテーションとマイクロセグメンテーションを使用します。　各セグメント（または一つのアプリケーションのみを含むマイクロセグメンテーション）は個別に防御されています。このような制限は、ITインフラストラクチャにクラウドサービスプロバイダなどのマルチテナントがある共有環境において特に重要です。

例えば、マイクロセグメンテーションは研究病院で有利となります。各研究プロジェクトで各々のITインフラストラクチャを購入するのではなく、マイクロセグメンテーションと組み合わさったプライベートクラウドを使用して、適切な情報セキュリティ対策を講じることで、共有する病院のITインフラストラクチャとして各プロジェクトを個別化させることができます。

すべてを統合

情報セキュリティに対する侵害イベントはもはや生活の一部となっています。侵害が避けられないことは防止技術を無効にするものではありませんが、侵害されたときに何を実行するのかを、組織が計画する必要があることを意味します。

自動化を検知および緩和技術に結びつけることで、侵害されたデバイスを切断や隔離するネットワークスイッチの指示など、緩和手順をトリガーする手段として自動化を利用することができます。これにより拡散を防ぐことができ、企業は各イベント毎に数億、もしくは数十億ドルを節約できます。

組織が注意する必要がある情報セキュリティの責任には、予防、検知、緩和、インシデント対応の4つの領域があり、最も基本的なレベルにおいて、情報セキュリティはすべて発想が重要となることを常に念頭に置いてください。

Juniper Connected Security

セキュリティに必要となる層

今日のネットワークを防御することは、こうしたネットワーク上ですべてを保護することを意味し、ほとんどの組織による実践とは異なる情報セキュリティへのアプローチが必要となります。

ネットワークとセキュリティは相互に結び付けられており、ポイントソリューションを使用してネットワークを構築しようとするとき、事態はひどく間違った方向に進む傾向にあります。効果的なネットワークセキュリティは、複数のセキュリティのベンダーから提供される複数の技術を導入することで達成される複数のレイヤーを相互に結びつけることから生まれます。

スイッチ、ルーター、Wi-FiアクセスポイントはJuniper Connected Securityの一部であり、すべてが一元的に自動化され、統合された方法で、ネットワークの深い可視化と共にネットワークポリシーの実施ポイントを提供します。これにより、組織は達成することが難しい側面の保護が得られます。

特定のセグメントに対する最適なソリューションは、専門家が提供するものであるとするアナリストもいるかもしれませんが、この場合、組織は複数の製品を使用して、互いが上手く機能するように多くのものを入手する必要が生じます。これにより、ネットワーク防衛の自動化と調整が困難になります。ランキングは常に変化し、自動化の実装は多くの場合、自動化される製品のライフサイクルよりも長くなります。

多くのベンダーには、パートナーのエコシステムを含めた情報セキュリティ製品、ネットワーキングからなる多様なポートフォリオが存在します。サービスプロバイダの規模で運営する顧客をサポートし、あらゆる企業の非常に並外れた大規模なネットワークにも対応できるジュニパーのような企業もあります。

ジュニパーを際立たせるものは**Juniper Connected Security**の「接続」、つまり相互接続性への私たちのコミットメントです。ジュニパーは統合とオーケストレーションを支持し、オープンスタンダート、オープンプロトコル、オープンAPIの使用を奨励し、競合製品に対応した構築にも対応します。現在のものを破棄して交換することを要求するのはなく、既存のものを最大限に活用するためのサポートを提供することが私達の目標です。

ジュニパーのポートフォリオに存在する単一のオペレーティングシステムであるJunosを使用することで一元管理をより簡素化し、オンプレミス、クラウドベース、または両方を組み合わた管理プランを持つ多機能の管理プラットフォームを提供します。Junos OSなら、コスト効率の良い方法でポートフォリオ全体に機能を追加できます。

Juniper Connected Securityは、ネットワーク全体のあらゆる接続ポイントにセキュリティを拡大することで、組織にユーザー、アプリケーション、インフラストラクチャを保護する能力を提供します。可能な限り脅威に近いポリシーを実施することで、その脅威のリスクが拡大するリスクを軽減します。また、機械学習、高度な分析、自動化を活用することで、迅速なインシデント対応が実現します。

実際のJuniper Connected Securityの活用例について詳しくご覧ください。

今すぐ読む

「サイバーセキュリティの基本」の完全版はこちらからお読みください

JUNIPER NETWORKS | Engineering Simplicity

PN:7400127-001-EN

米国本社
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
電話: 888.JUNIPER (888.586.4737)
または +1.408.745.2000
FAX:+1.408.745.2100
www.juniper.net

日本
ジュニパーネットワークス株式会社
東京本社
〒163-1445 東京都新宿区西新宿
3-20-2 東京オペラシティタワー 45階
電話番号:03-5333-7400
www.juniper.net/jp/jp