Akamai

ホワイトペーパー

ヘルスケアプロバイダー向けのサイバーセキュリティ

概要

急速に変化する市場で競争に勝ち残るために、ヘルスケアプロバイダー企業各社は、新しいデバイスやアプリケーションを導入し、最高の患者ケアとより高いレベルの体験を提供しようとしています。新しいデバイスやアプリケーションを導入するたびに、患者にとってはメリットとなる一方で、組織にはセキュリティリスクとなります。

保護された健康情報（PHI）の価値が高いことに加え、このような複雑な IT 環境は、システムへの攻撃を続けるサイバー犯罪者にとってまたとない好機となっています。米国保健社会福祉省のレポートと IBM の調査によると、ヘルスケア業界に対するサイバー攻撃は、パンデミックの始まり以降 50% 増加しました。しかも、それらの攻撃によるコストは非常に高く、インシデントあたりの平均コストは 713 万ドルに上ります。IBM レポートによると、最も頻繁に発生した脅威はランサムウェア攻撃で、迅速な復旧を要する医療機関やヘルスケアシステムが攻撃者に狙われました。その次に多かったのはデータ窃取やサーバーへのアクセスです。特にヘルスケアプロバイダーは、ダーク Web 上では電子カルテ（EHR）が 1 件につき 1,000 ドルで取引されることもあり、クレジットカード情報が約 110 ドル、社会保障番号がわずか 1 ドルで取引されるのと比べると、ランサムウェアのターゲットとしては魅力的なのです。

システムに対する脅威は日々増加の一途をたどっていますが、多くの組織では、脅威を緩和するための対策が十分ではありません。さらに深刻なのは、すでに侵入されているにもかかわらず、それに気づいていないケースです。攻撃者はすでにデータを流出させているか、攻撃の絶好のタイミングをうかがっているのかもしれません。

今こそ、デバイスのインベントリを作成し、それらがどのようにインフラに接続されているかを調べ、組織のアタックサーフェスを明確にする必要があります。どこに脆弱性が存在するのかをより正確に把握し、適切な緩和策を導入することで、サイバー攻撃の潜在的な影響を防止または最小限に抑えることができます。

組織にとっての最大のサイバーセキュリティリスクを防ぐ方法

脅威その 1：フィッシング攻撃

フィッシングは、業界を問わず最も一般的なサイバー攻撃の手段の 1 つです。Health Sector Cybersecurity Coordination Center によると、2021 年にはヘルスケアセクターに対するフィッシング攻撃が大幅に増加しました。実際に、2020 年を通して Akamai が観測したところでは、攻撃者が COVID-19 に付け込んで金融支援を謳うなど、財政的苦境に立つ世界中の人々にフィッシング攻撃を仕掛けたことを確認しています。

フィッシングとは、不正な電子メールや Web ページを通じて機微な情報を取得しようとするものです。フィッシングが成功すると、ユーザーはうっかりログイン認証情報を入力してしまいます。これが実質的に、攻撃者にネットワークへの入り口を開放してしまうことになります。

このような被害が、ニューヨークの失業申請者に発生したことがあります。CSO Online の元編集者であり、現在は Akamai のセキュリティ研究者である Steve Ragan のフィッシングレポートによると、2021 年初頭にはパンデミック失業支援（PUA）プログラムを標的としたフィッシングキットが複数存在したとのことです。これらのプログラムは、COVID-19 のロックダウン時に支援を必要とする人々を救済するために設けられたもので、何百万人ものアメリカ人に必要不可欠なサービスを提供していました。

全米で放送されている CBS ニュースのスポット番組で、Ragan はニューヨークの人々をターゲットにした失業者フィッシングキットと、犯罪者が詐欺で入手した個人情報をどのように収集し、販売しているかについて取り上げました。そのニュースが放送されて以降、彼はウィスコンシン、インディアナ、ペンシルバニア、マサチューセッツの人々をターゲットにした PUA 詐欺も発見しました。

フィッシング攻撃を阻止・緩和する方法

権限の設定やセキュリティ保護対策にもよりますが、たった 1 つのユーザーアカウントにアクセスするだけで、犯罪者はネットワークの重要な部分に自由にアクセスできるようになる可能性があり、組織のネットワーク内に一度入り込んでしまうと、その範囲を広げてしまうことも少なくありません。

マイクロセグメンテーションは、攻撃者のアクセスを最初にアクセスしたネットワークの一部のみに制限し、ラテラルムーブメント（横方向の移動）を防ぐことで、別のエリアに被害を拡大させないようにします。どこを入口としても、犯罪者が組織のより広範なネットワークにアクセスできないようにすることで、侵害の影響を抑制します。

マイクロセグメンテーションに加えて、多要素認証（MFA）はフィッシング攻撃に対する最善の防御策の 1 つです。アカウントへのアクセスを許可する前に追加の本人確認を要求することで、保護レイヤーを増やし、漏えいした認証情報が悪用されるのを防ぎます。

MFA、特に FIDO2 認証ソリューションは、最新の攻撃から確実に保護し、ユーザーのモバイルデバイス上のテキストまたは認証アプリによって生成される固有コードの入力をユーザーに要求します。このようにログインステップを追加することで、犯罪者が正確なログイン認証情報を持っている場合でも、フィッシング攻撃を阻止することができます。

フィッシングのようなソーシャルエンジニアリング攻撃の手口について、スタッフを教育することは非常に重要です。多くの不確定要素が存在するため、フィッシングは決定的な解決策がない問題の 1 つである、というのが現実です。犯罪者が次に何をするか予測するのは困難です。人間がフィッシングの主要な要素であることに変わりはないため、一連のフィッシングの中で最も弱い部分であることに変わりはありません。

つまり、セキュリティを簡単にすることが肝要なのです。Akamai は、最も知恵の回るサイバー犯罪者からも保護する、フリクションレスなフィッシング対抗 MFA ソリューションを提供しています。

脅威その 2：サポートされていないレガシーソフトウェア

ソフトウェアが古くなっていることも、脆弱性に関する重大な懸念事項です。新しいセキュリティアップデート（パッチ）がすぐにインストールされないと、ネットワーク上に無防備に開いたバックドアができてしまいます。特に、サポートが終了し、アップデートが提供されなくなった古いデバイスに当てはまります。

サポートされていないソフトウェアにはゼロデイ脆弱性が存在する可能性があり、組織が独自にパッチを当てるのはためらわれるかもしれません。カスタムパッチを作成すると、デバイスの保証が無効になり、何か問題が発生したときに高額な修理費用が発生することがあります。

医療機器はライフサイクルが長い反面、最新バージョンのオペレーティングシステムにきちんとアップデートされていなかったり、サポートされていないオペレーティングシステムを使用している場合、ハッカーが脆弱性を悪用してデータを盗み、医療機関のネットワークに侵入し、医療に支障をきたす危険性があります。フォーチュンの報告によると、マンモグラフィ装置から MRI 装置まで、インターネットに接続された医療用画像診断装置の実に 83% が脆弱性を抱えています。

旧式のデバイス、特にメンテナンスのライフサイクルを超えているデバイスほど、犯罪者がサードパーティのデバイスを通じて組織のネットワークにアクセスするための弱点を知っている可能性が高くなります。

たとえば、Windows 95 は何年も前にメンテナンスが終了していますが、直接書き込みが可能な最後の OS であったため、MRI の多くの機器（その他）はいまだにこの OS に依存しています。社内の開発者なら脆弱性にパッチを適用できるかもしれませんが、そのパッチによって機械の保証が無効になる恐れがあります。唯一の安全な選択肢は、MRI 装置を全面的に交換することですが、多くの施設ではコスト的に不可能です。

ネットワーク管理者は、サポートされていないシステムをネットワーク外に置こうとしますが、特に患者のケアに必要なデバイスがあり、医師にデータを迅速に提供しなければならない場合、必ずしもそれが可能とは限りません。また、ネットワークに接続されているすべてのデバイスのマップが不完全だと、隔離がうまくいかず、バックドアができてしまいます。見えないものを保護するのは難しいのです。

脆弱でサポートされていないデバイスを保護する方法

これらのデバイスによる組織のネットワークへのアクセスを防ぐには、ゼロトラスト・ネットワーク・アクセス（ZTNA）アーキテクチャに移行することが重要です。ZTNA は、すべての着信リクエストを、安全性が証明されるまで潜在的な脅威として扱うフレームワークであり、たとえソフトウェアが古くても、攻撃者がデバイスにアクセスする前に効果的に阻止します。

ZTNA への移行は、旧来の「城と堀」アプローチ（信頼せよ、されど検証せよ）からゼロトラスト・モデルへの根本的な転換を意味します。ゼロトラスト・アプローチではサイバー攻撃を完全に防ぐことはできないかもしれませんが、潜在的な損害を壊滅的なものから管理可能なものへと制限することができます。HealthITSecurity は、次のように述べています。「攻撃者が認証情報を取得し、1 つのデバイスを操作することに成功したとしても、ゼロトラスト・アーキテクチャを導入していれば、そこから先には進むことはまずできないでしょう」

Akamai では、プロバイダーがダウンタイムを発生させることなく、現在のワークフローに柔軟性を持たせたまま、ゼロトラスト・アーキテクチャに移行できるよう、堅牢なプランを提供しています。この詳細な計画ガイドで、ZTNA を始めましょう。

脅威その 3：在宅勤務と BYOD

21 世紀におけるケアの継続性は分散化されています。患者は自宅で快適にケアを受けられます。プロバイダーは、対面ではなく、モバイルデバイスを介してケアを提供します。しかし、このようなアクセシビリティの向上は、スタッフがオンサイトと自宅の両方でネットワークにアクセスしたり、管理されていないデバイスからログインしたりするため、プロバイダーのサイバーセキュリティリスクが大幅に増大することを意味します。

パンデミック以前にも、チームメンバーが自宅のネットワークからシステムにログインすることはあったかもしれませんが、この期間に組織のネットワークにアクセスする個人所有のデバイスの量が必然的に急増しました。もし、これらのノートパソコン、タブレット、スマートフォンがマルウェアに感染していた場合、ランサムウェア攻撃の入口となる可能性があります。

たとえば、チームの誰かが誤って偽の Web ページにログイン情報を入力してフィッシング攻撃の被害に遭った場合、攻撃者はそのユーザーと同じアクセス権を持つことになり、ファイルを暗号化してチームをロックアウトし、ファイルの復号化に高額な身代金を要求して組織を機能不全に追い込むことができる可能性があります。

ネットワークのエッジを保護する方法

組織のネットワークにアクセスしている人物（場所、IP アドレス、使用しているデバイスなど）を注意深く監視すれば、このような状況が発生する可能性を最小限に抑え、攻撃を未然に防ぐことができます。

あなたのチームが個人所有のデバイスを使用している場合、または自宅で作業している場合、次の質問を自問してみてください。

- 受信リクエストを最大限に精査し、攻撃を未然に防ぐためのゼロトラスト・ネットワーク・アクセス（ZTNA）アプローチを導入しているか？
- マイクロセグメンテーションを確立して、アクセスを制限し、犯罪者が組織のネットワークに侵入した場合のラテラルムーブメントを抑止しているか？
- レイテンシーを最小限に抑え、高速で快適なユーザー体験を維持しながらネットワークを保護するために、セキュア・アクセス・サービス・エッジ（SASE）フレームワークを使用しているか？
- 私たちのチームは、各デバイスとアカウントのログインにアクセスコード、強力で固有のパスワード、多要素認証（MFA）を使用しているか？

Akamai は、テレワーカー・セキュリティ・ソリューションにより、ネットワークアクセス管理を容易にするお手伝いをいたします。

脅威その 4:不十分なデータ・フロー・マッピング

片足はオンプレミス、もう片足はクラウドという状態では、データがどこにあり、どのように流れているのかを理解することはほぼ不可能です。これにはいくつかの理由があります。

1 つ目は、量です。ベンダー、業務委託先、コンサルタントがそれぞれ異なるデバイス、ツール、ソリューションを使用しているため、1 時間単位とは言わないまでも、毎日ネットワークに追加されたり削除されたりするデバイスやアプリケーションの数を把握するのは至難の業です。

2 つ目は、チームメンバーの入れ替わり、プロセスの変更、優先順位の競合などの理由で、ハードウェアとソフトウェアを追跡するシステムが機能しなくなり、正確性や信頼性が低下している場合です。

目に見えないものを保護することはできないのですから、理由は何であれ、ネットワークとコネクテッドデバイスを可視化することは重要です。

コネクテッドデバイスのフローをマッピングする方法

コネクテッドデバイスのロードマップを作成できる可視化ツールを持つことは非常に重要です。特に、HIPAA Journal（HIPAA ジャーナル）の 2019 年の記事には、ヘルスケア組織の 82% が過去 12 か月間にコネクテッドデバイスへのサイバー攻撃を受けたことが挙げられています。

ネットワーク全体のデータの流れを追跡し、ネットワークに接続されていないデバイスも含めて、データの送信元と送信先を教えてくれるソリューションを選択することは、コネクテッドデバイスのマッピングの第一歩です。マッピングができれば、情報の流れをリアルタイムにネットワーク図で把握できるようになり、ネットワーク上に存在する悪性のデバイスを探索しやすくなります。コアシステム、資産、データ（PHI など）の周囲にソフトウェア定義のマイクロセグメンテーションリングを設置することで、攻撃者のネットワーク内でのラテラルムーブメントを制限することができます。Akamai のマイクロセグメンテーションツールで、必要な可視性を確保してください。

脅威その 5：ネットワーク、アプリ、システムの複雑性を管理する

自分のデータを読み取ることができるアプリケーションやソフトウェアを把握していますか？ソーシャル・メディア・プラットフォームのように、プライバシーステートメントや利用規約の中で、その侵害性を明示しているソフトウェアアプリケーションもあります。また、電子メールプロバイダーのように、目立たないものの、重大なリスクをもたらすものもあります（たとえば、写真に PHI が含まれている場合、デバイスの写真にアクセスできたりします）。

また、クリップボードにコピーされた項目（患者識別情報やパスワードなど）をアプリが閲覧することも許可されている可能性があります。デバイス上に患者情報がある場合、サードパーティ（または攻撃者）がそれを見る（記録する）可能性もあります。

チームの教育、ネットワーク全体の表示、エッジの保護

私物のデバイスを使用するリスクと、患者の個人情報を保護するために必要なことについて、プロバイダー組織の全員を教育することが極めて重要です。

また、アタックサーフェスと潜在的な攻撃ベクトルについて、組織がどのような見解を持っているかを考慮することも重要です。セキュリティチームは、複数のクラウド・サービス・プロバイダーやオンプレミスのデータセンターを横断するネットワーク全体を監視していますか？それとも、組織のインフラの異なる側面に焦点を当てた複数のグループに分かれているのでしょうか？特に攻撃を受けている間は、組織のネットワーク全体とその活動の全体像を把握することが不可欠です。

「脅威その 4」と同様に、ネットワークのエッジを保護するための最善の防御策は、マイクロセグメンテーションとアカウントログイン用の MFA を組み合わせた、ゼロトラスト・アーキテクチャです。所有者が誰であるか、クラウドかオンプレミスかに関係なく、1 つのプロバイダーを採用してすべてのシステムを保護することで、ユーザー体験を妨げることなくネットワークを保護することができます。

何もしないことの影響とは

コストはさまざまな形で発生します。最もわかりやすいのは金銭的なもので、IBM の「データ侵害のコストに関する調査」2021 年版によると、米国のヘルスケア企業では 1 件のデータ漏えいに伴う総コストは平均で 923 万ドルに上ります。その他のコストは、患者の安全性や信頼性など、質に関わるもので、ヘルスケア組織に与える影響は同等かそれ以上です。

患者の安全性の低下

サイバーセキュリティにおいて、患者の安全は最も重要なターゲットです。攻撃によって IT システムがシャットダウンを余儀なくされると、患者の治療が中断されます。治療や予約が延期され、患者の健康状態が悪化する可能性があります。実際、最近の訴訟では、ランサムウェア攻撃が直接の原因となって患者が死亡したという史上初の申し立てがありました。

一方、患者の遠隔モニタリング（心拍数やグルコースレベルなど）に使用される医療用のコネクテッドデバイスは、ケアに対してより直接的な脅威をもたらします。たとえば、患者の血圧計測が阻害されると、危険な状態が見過ごされ、治療を受けることができないままになり、警鐘事象を引き起こす可能性があります。

顧客の信頼の喪失

信頼できる医療を提供できず、患者情報を保護できなければ、患者の信頼を失うことにつながります。患者の 90% 以上が、データ漏えいによって個人情報が危険にさらされた場合はプロバイダーを変更すると回答しています。実際の数字はもっと低いかもしれませんが、計算してみてください。仮に半減した場合、あるいは 10 分の 1 だけだったとしても、患者数にどのような影響が出るでしょうか？そして、新たな患者を少しずつ獲得しながら、どのくらいの期間、継続的な損失を被ることになるのでしょうか？

収益の損失

38% に上る事業損失は、データ漏えいに関連する最大のコスト要因です。プロバイダーの基幹システム（EHR や電子メールサーバーなど）がダウンすると、医療機関の業務はピタリと止まってしまいます。つまり、予約、来院、面会ができなくなり、収入もなくなります（患者ケアへの影響は言うまでもありません）。

米国サンディエゴを拠点とする Scripps Health は、2020 年 5 月に大規模なサイバー攻撃を受け、主に救急外来での治療や待機的手術の件数を減らしたことにより、9,160 万ドルの減収となりました。

ヘルスシステムのネットワークの一部がまだ稼動していたとしても、攻撃ベクトルを特定し、脆弱性にパッチを適用し、フォレンジック分析を完了するまでは、すべてが安全であるとは断言できません。

諸経費の増加

優秀なサイバーセキュリティエンジニアを採用し、雇用し、維持するためにはコストがかかりますが、真のコストはそれだけにとどまりません。サイバーセキュリティチームを自前で組織内に雇用すると、高額な補償の不足が生じる可能性があります。

一般的に、組織が攻撃者を特定し、ネットワークから排除するのに長くかかるほど、コストは高くなります。Ponemon Institute のレポートによると、サイバー攻撃を最初の 200 日以内に検知できれば、組織は 126 万ドル以上を節約できるそうです。残念ながら、同レポートによると、攻撃を特定し、封じ込めるまでに要する日数は平均 287 日です。*287* **日も！**この日数が意味するのは、攻撃者は 9 か月以上にわたってネットワークインフラ内部に潜伏し、その医療機関の評判と収益に最大の損害を与え得る攻撃を画策していることが多いということです。

このため、セキュリティチームが攻撃を特定し、対策を講じるために必要な時間を明確に数値化することが不可欠です。セキュリティベンダーを、マネージドサービスを提供し、スタッフの緊急事態に対応できるエンジニアリングサポートを提供するベンダーに統合することで、大幅なコスト削減が可能になります。

規制当局からの罰金

価値のある個人情報が大量に管理されているため、データ漏えいが発生すると、規制当局から多額の罰金が科される可能性があります。2021 年 11 月 30 日時点で、米国保健社会福祉省の公民権室は、106 の HIPAA 対象事業体に対し、総額 1 億 3,100 万ドル以上の和解金もしくは罰金を科しています。これは、1 件あたりにすると平均 120 万ドル以上の罰金です（ここに挙げた追加費用に加えて）。

ヘルスケア組織のサイバー攻撃への最善の備え方

今日のサイバー脅威は、プロバイダー組織に業界トップレベルのセキュリティを要求しています。患者さんとビジネスがかかっているのですから、何もしないことの代償は非常に大きいのです。

財政的な制約、競合する優先事項、またはリスクの不確実性によって、過剰なリスクを背負うことになるかもしれません。しかし、セキュリティへの取り組みは、徹底的かつ戦略的で、注意深く、俊敏でなければなりません。

今日適切に保護されたエコシステムが、明日も保護されているとは限りません。脅威は急速に進化するのです。脅威が新たな脆弱性を悪用するのに必要な時間は、1 日（あるいはそれ以下）です。

脅威対象範囲を縮小し、連邦政府の勧告で推奨されたバックアップ方法（3 つのコピーを作成し、そのうち少なくとも 2 つを異なる形式で保存し、1 つをオフラインにする）を採用したいと考えるプロバイダーの多くは、ハイブリッドアプローチを模索しています。オンプレミスのデータストレージは、セキュリティを制御しやすい一方、コストがかさみ、規模の拡大も難しくなりがちです。特にパンデミックが拍車となって健康データが爆発的に増加し、治療のデジタルトランスフォーメーションが急速に進みつつある現状では、これが大きな問題となる可能性があります。パブリック・クラウド・データ・ストレージは、コスト効果は高いものの、サービスの停止やデータ保護方法に関する透明性の欠如といったリスクが生じます。

ハイブリッドアプローチであれば、機微な情報はオンプレミスに保持しながら、機密性の低いデータはクラウドに保存することができます。もちろんこれでも完璧ではありません。2 つのストレージタイプ間のデータ転送を保護し、データの転送と表示を許可されている者だけにアクセスを制限するようなセキュリティを整備する必要があります。ZTNA アーキテクチャを実装するために必要な 7 つの主要要件を満たすことで、各機関は、ユーザーがそれぞれの職務に必要なアプリケーションのみにアクセスできるようにし、MFA によってさらにセキュリティを強化することで、データを保護することができます。

Akamai は、「もし攻撃が発生したら」ではなく、発生することを前提として、お客様をサポートします。攻撃を迅速に察知し、被害を効率的に緩和するために、お客様のネットワークの全体的なビューを、ともに構築しましょう。当社は、分散型サービス妨害攻撃やランサムウェア攻撃からネットワークを保護し、シームレスでセキュリティが確保された Web 体験（アプリや API を含む）を提供することを基盤としています。

ネットワークのエッジを強化することで、侵害の可能性を最小限に抑えるだけでなく、侵害が発生した場合の影響範囲を縮小します。また、ユーザーアクセスの柔軟性を維持しながらこれを実現することで、日々変化する業務やケアに対する要求の中で、組織が最適な医療成果の提供に集中できるようにします。

増え続ける巧妙なサイバー犯罪や、拡大するクラウドベースのアタックサーフェスから患者の情報を守ることは、かつてないほど重要な課題となっています。患者を中心に考える組織や政府機関は、Akamai のエッジプラットフォームを信頼し、患者にデジタル体験を近づけ、脅威を遠ざけています。

サイバーセキュリティをいつまでも続く重荷から競争力へと変えるパートナー、Akamai にお任せください。

詳細については、当社までお問い合わせいただくか、+81-368979452 までお電話ください。