ランサムウェア対策への5つのステップ

境界を超えて防御を強化するためには

目次

概要

ランサムウェアの増加と広がり

ランサムウェアはこれまで、ファイルやデータを暗号化してアクセス不能にする手段として攻撃者が使用する迷惑なマルウェアの一種にすぎませんでしたが、今では大規模な攻撃手法へと変貌しています。永久的なデータ損失の脅威だけでも厄介ですが、サイバー犯罪者や国家ぐるみのハッカーたちは、ランサムウェアを使用してエンタープライズ、州政府および地方自治体、グローバルインフラ、ヘルスケア組織などに侵入して機能を麻痺させてしまうほど高度になっています。さらに、これらのグループの多くは、サービスとしてのランサムウェア（RaaS）としてサービスを有料で提供しているのです。

2031 年までに、ランサムウェア攻撃は 2 秒に 1 回発生し、それによる損失額は年間 2,650 億ドルに上ると予測されています。

Cybercrime Magazine

ランサムウェアビジネスがもたらす大きな代償

2022 年、セブンイレブンではランサムウェア攻撃により、レジの使用や決済の受付ができなくなり、175 店舗が閉店を余儀なくされました。今年初め、ドイツの石油会社が狙われた BlackCat ランサムウェア攻撃では 233 店舗のガソリンスタンドが影響を受け、Royal Dutch Shell では別の補給所に輸送経路を変更しなければならない事態となりました。2021 年 5 月に発生した Colonial Pipeline への攻撃では、米国東海岸での石油やガスの供給がすべて中断されました。さらに、2020 年の Snake ランサムウェア攻撃では、ホンダの業務が世界中で停止しました。

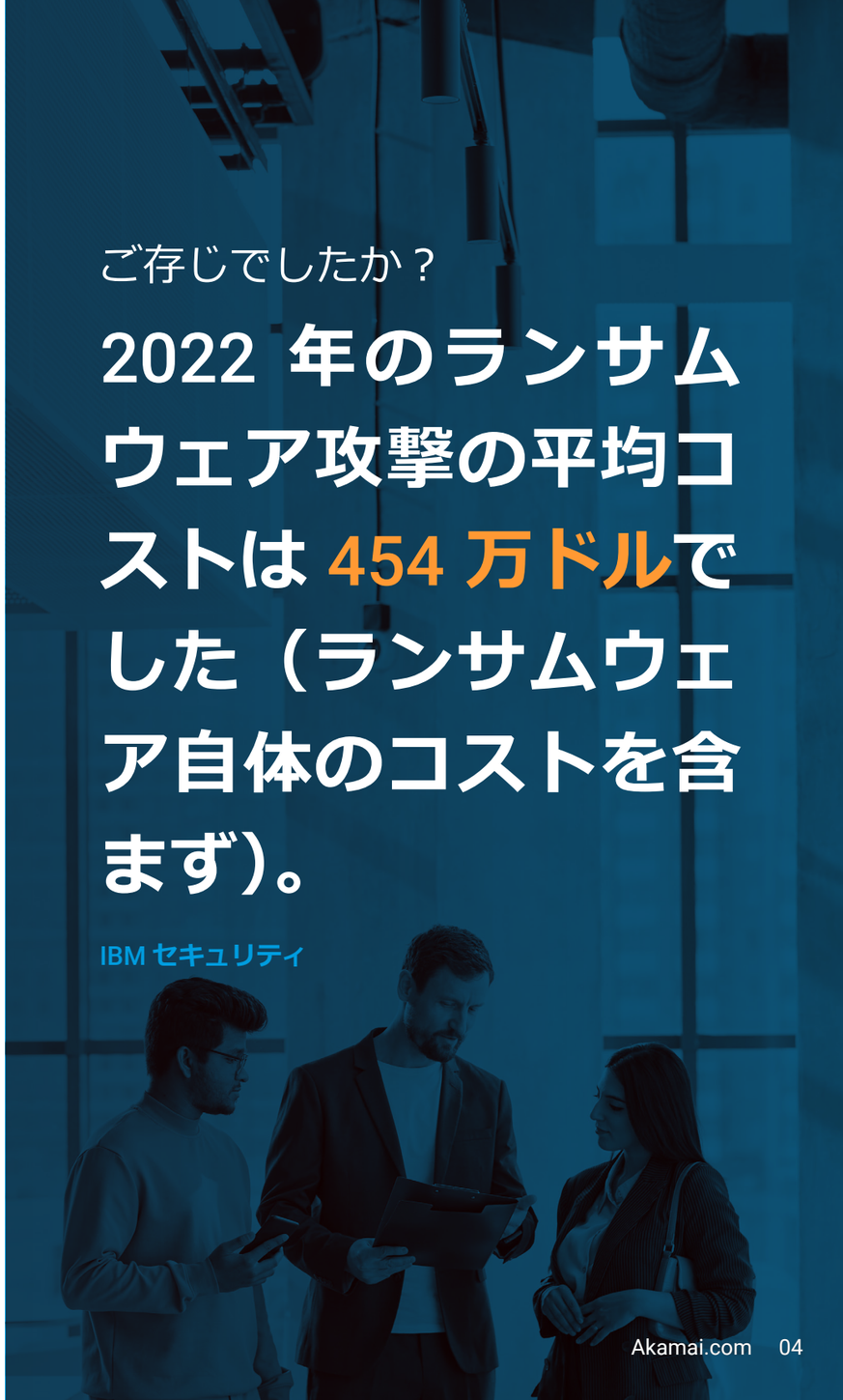
現在、時代遅れのテクノロジー、境界とエンドポイントのみに焦点を当てた「十分な」防御戦略、トレーニングの欠如（および不十分なセキュリティエチケット）、および「特効薬」となる既知のソリューションの欠如により、あらゆる規模の組織がリスクにさらされています。サイバー犯罪者は、企業のネットワークを可能な限り暗号化して、数千ドルから数百万ドルの身代金を要求することを生業としています。

しかも、企業にとってのリスクは収益だけではありません。ランサムウェア攻撃を受けると、次のような悪影響が生じる可能性があります。ダウンタイムが発生し、業務の停止、生産性の低下、データ侵害につながる可能性があります。

その企業が独自に所有するデータが漏洩したり不正にアクセスされたりすると、ブランドの評判が損なわれ、顧客ロイヤルティを失う可能性があります。2020 年の調査によると、データ漏えいのうち、顧客の個人情報（PII）が含まれていたものは 80%、知的財産の侵害は 32%、匿名化された顧客データの侵害は 24% でした。もちろん、このような機微な情報は悪用される可能性があり、機密データが販売されるなど、知らないうちにビジネスが脅かされることもあります。

ランサムウェアの脅威はすぐにネットワーク全体に拡がるため、境界のみの保護では不十分です。

Akamai



ラテラルムーブメントを阻止し、ランサムウェアの拡散を防ぐ

ランサムウェア攻撃は多くの場合、フィッシングメール、ネットワーク境界の脆弱性、穴を見つけるための総当たり攻撃を利用した初期侵害から始まります。その間、攻撃者は自身の実際の意図から防御をそらそうと画策します。

攻撃がデバイスまたはアプリケーションに到達すると、感染させたり暗号化したりするポイントを最大化するために、ネットワーク全体および複数のエンドポイントへとラテラルムーブメント（横方向の移動）が進行します。攻撃者は通常、ドメインコントローラーの制御を奪い、認証情報を侵害し、バックアップを見つけて暗号化することで、凍結されたサービスをオペレーターが復元できないようにします。

攻撃を成功させるためには、ラテラルムーブメントがきわめて重要です。マルウェアが最初の侵害ポイントから拡散できない場合、その攻撃は成功しません。そのため、ラテラルムーブメントを阻止することが不可欠です。

包括的なランサムウェア脅威緩和戦略が必要です。

リスク緩和

鉄壁の防御戦略を構築する

ネットワーク内のラテラルムーブメントを検知して阻止するためには、次の 2 つの領域を重視する必要があります。まず、**最初の攻撃ベクトルを軽減**し、その後**伝播経路を制限**します。

たとえば、インターネットに公開されるサーバー数を制限したり、パッチ管理によってアタックサーフェスを小さくしたり、リングフェンシングによってアプリケーション間の伝播経路を減らしたりすることが可能です。また、データをバックアップしておけば、攻撃が発生しても迅速に復旧できるので、広範にデータが失われる事態を防ぐことができます。

セキュリティ計画を優先させる 4 つの方法

組織の包括的な準備戦略、計画、予算には、セキュリティを含める必要があります。そのためには、経営幹部と取締役会メンバーの意識を高めて、潜在的なリスクや、その緩和に何が必要なのかについて、常に気を配ることが重要です。

1. 組織全体のリスク緩和を管理する機能に、サイバーセキュリティを含めます。さらに、リーダーシップチームにセキュリティに関する専門知識があることを確認してください。
2. バックアップの生成とネットワークセグメンテーションに必ず専用の予算とリソースを割り当ててください。
3. 災害または有害事象（ランサムウェア攻撃など）が発生した場合について、前もって対応計画を作成しておきます。系統立てて準備しておくことで、迅速かつ効率的に対応できます。
4. 新しい製品やサービスの統合、設計、開発の際には必ずセキュリティへの影響を分析します。次の点を自問自答してください。攻撃者のために新たな扉が開かれていませんか？

ランサムウェア検知のチェックリスト

ネットワークで何が起きているのか

多くの組織にとって、ランサムウェアの検知は容易なことではありません。組織のネットワークは、残念ながら攻撃に対して脆弱です。強力な検知機能がない場合、身代金要求のメッセージを受け取った時にはすでに手遅れです。ネットワークのほとんどが同時に暗号化されます。

検知では、拡散中のランサムウェアを把握する必要があります。そのためには次の機能が必要です。

強力な可視性

ネットワークで何が起きているか把握できなければ、ランサムウェアやその他の望ましくないサイバー脅威を検知できません。

セグメンテーションポリシー

すべての通信を定義し、把握することで、標準外の通信が顕在化し、警告が可能となります。

侵入検知（IDS）システムおよびマルウェア検知ツール

既知の脆弱性やエクスプロイトに対して事前定義したルールや署名を使用したり、通常の検知や自動異常検知を増やしたりして、ランサムウェアオペレーターによる拡散の試行を検知します。

ディセプションツール

おとりやハニーポット、または不正なラテラルムーブメントを特定できる分散型ディセプションプラットフォームをセットアップすることで、インシデントの忠実度が向上し、進行中のアクティブな違反を効果的に発見できるようになります。

ランサムウェア防御戦略を構築する

最高の境界防御を構築しても、セキュリティ侵害を避けることはできません。だからこそ、攻撃の効果を最小限に抑え、ネットワーク内での拡散を阻止する防御戦略を確立する必要があるのです。横方向のデータセンタートラフィックの脅威を検知し、ラテラルムーブメントを阻止する包括的なセキュリティソリューションを提供するベンダーを探してください。

準備

IT 環境で実行されているすべてのアプリケーションとアセットを識別できるようにするソリューションを見つけます。このレベルのきめ細かい可視性があれば、重要なアセット、データ、バックアップをすばやくマッピングし、脆弱性とリスクを特定できます。ネットワーク環境の全体像を把握することで、侵入されても対応可能となり、すばやくルールをアクティベートできます。

阻止

一般的なランサムウェア伝播手法をブロックするルールを作成できるソリューションが必要です。ソフトウェア定義のセグメンテーションを使用すれば、重要なアプリケーション、バックアップ、ファイルサーバー、データベースの周囲にゼロトラストのマイクロ境界を作成できます。また、ユーザー、アプリケーション、デバイス間のトラフィックを制限し、最終的にラテラルムーブメント試行をブロックするセグメンテーションポリシーも作成できます。

検知

セグメント化されたアプリケーションやバックアップへのアクセス試行を検知して警告するソリューションを実装します。このようなアクセス試行のブロックは、ラテラルムーブメントの指標となります。さらに、既知の悪性ドメインや悪性プロセスの存在を警告するレピュテーションベースの検知も組み入れる必要があります。境界線の突破に成功した攻撃をすばやく発見できれば、滞留時間を最小限に抑え、ランディングポイントを通過する前に攻撃者を捕まえることができます。

修復

攻撃が検知された場合に脅威の封じ込めと隔離を自動的に開始する機能が不可欠です。隔離ルールを適用して、影響を受けたネットワーク領域をすばやく切り離す一方、セグメンテーションポリシーによって重要なアプリケーションやシステムバックアップへのアクセスをブロックします。

復旧

最後に、ネットワークのさまざまな領域が「完全にクリア」であることを検証しながら、徐々に接続を回復していきます。このような段階的な復旧戦略をサポートできるような可視化機能が必要です。

結論

まとめ

現在の防御戦略に自信はありますか？

ランサムウェアがなくなることはありません。実際のところ、2021 年はランサムウェアに感染した組織は 66% と前年比 78% 増となり、減少する様子はありません。つまり、今後も世界的に攻撃頻度が上昇し、より大規模で価値の高い標的が狙われるようになり、身代金の要求額も高くなると考えられます。これらはすべて、ビジネスに深刻な影響をもたらします。今やこれまで以上に、境界型のみのアプローチを超える高度な計画とリスク緩和戦略が必要とされています。

ネットワークでのランサムウェアのラテラルムーブメントを阻止しましょう。Akamai がその方法をご紹介します。

詳細については、akamai.com/guardicore をご覧ください。

Akamai は、お客様が生み出すもの全てにセキュリティを組み込む取り組みを支援することで、どこで構築しどこへ提供しようとも、顧客体験、従業員、システム、データを守ります。グローバルな脅威に対する可視性を備えた Akamai のプラットフォームは、セキュリティポスチャの適応と進化を後押しして、ゼロトラストの実現、ランサムウェアの阻止、アプリケーションと API のセキュリティの確保、DDoS 攻撃の撃退を支援します。これにより、お客様は自信を持って、継続して、イノベーションを起こし、可能性を広げ、新たな可能性を生み出すことができます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 5 月