SOPHOS

ランサムウェアを阻止するための エンドポイント保護のベストプラクティス

最適な保護を提供するためのエンドポイント製品の設定に関する実践的なガイダンス

ソフォス ホワイトペーパー 2024 年 10 月

はじめに

ランサムウェアは、最も深刻なサイバー脅威の一つであり、壊滅的な被害をもたらすことも多くあります。ソフォスが実施した調査結果をまとめた「ランサムウェアの現状 2024 年版」レポートでは、回答者の 59% が、2023 年に自社がランサムウェアの被害を受けたと報告していました。これらのインシデントが発生した組織の 70% が、攻撃者によってデータが暗号化されたと報告しています。

全体的に見て、ランサムウェア攻撃の修復にかかる平均コストは 273 万ドルで、前年度と比較して 50% 増加しており、企業に大きな損害を与えていました。さらに、3 分の 1 以上の企業 (34%) が攻撃で受けた影響を復旧するために 1 か月以上を要しており、これらのインシデントが複雑化し影響が深刻になっていることが浮き彫りになっています。

復旧に要する期間が長期化していることから、包括的なインシデント対応が喫緊の課題となっています。インシデントが複雑化していることは、社内のセキュリティチームにも大きな負担を強いており、組織の 95% が基本的なセキュリティ業務を遂行することが困難になったと報告しています [1]。

これらの調査結果からも、ランサムウェアの対策と復旧戦略を強化することが急務であることが明らかです。復旧にかかるコストの上昇、復旧時間の長期化、セキュリティチームへの負担の増大により、ランサムウェアは事業継続に対する恐るべき脅威となっています。適切に設定されたエンドポイント保護ソリューションは、ランサムウェアから最も効果的に組織を守る方法の 1 つです。このホワイトペーパーでは、ランサムウェア攻撃の仕組み、ランサムウェアを防ぐための戦略、そしてセキュリティの効果を最大化するためにエンドポイント保護を最適化するためのベストプラクティスの詳細について解説します。

1 中小企業におけるサイバーセキュリティスキル不足の解消 - ソフォス

ランサムウェア攻撃の展開方法

攻撃者は多数存在し、ランサムウェア攻撃もさまざまな種類が存在しています。非常にターゲットを絞ったものもあれば、日和見的なものもあります。多くの場合、攻撃者 (サイバー犯罪者と呼ばれることもあります) は、企業や組織の環境に侵入するための弱点や脆弱性を見つけるためにネットワークをスキャンします。カナダの教育機関を攻撃したランサムウェアグループのコメントを以下に引用します。

> *「修正されていない深刻な Log4j の脆弱性が Horizon に存在していたため、そこから最初の侵入に成功した。意図的に狙ったわけではなく、一括スキャンで見つけた。」*

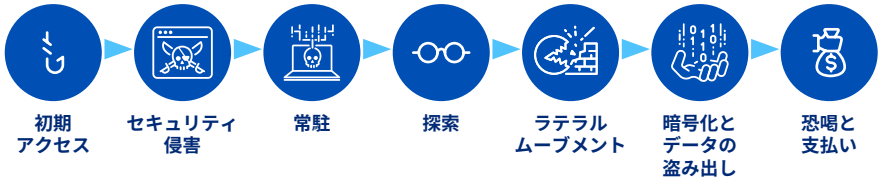
このコメントは、パッチが適用されていない脆弱性が広く攻撃されていることを示しています。パッチ未適用の脆弱性の攻撃は、2024 年のランサムウェア攻撃の最も多い根本原因でした。[2]

この数年ランサムウェア攻撃が増加しているのは、RaaS (Ransomware as a Service) モデルの拡大に起因している可能性があります。サイバー犯罪グループはランサムウェアを作成し、RaaS モデルのもとで、それを他の攻撃者に販売します。RaaS モデルにより、ランサムウェア攻撃への参入障壁が低くなり、これまで以上に多くの攻撃者がランサムウェアを使用できるようになっています。

攻撃者が被害者の環境に侵入すると、多くの場合、何日、何週間、何カ月もかけてネットワークの調査、権限昇格、データ窃盗、マルウェアのインストールを行います。2023 年におけるランサムウェア攻撃の平均滞留時間は 6 日 [3] でした。この期間の中で、防衛側の組織は最終的な攻撃が実行される前に侵入者を特定し、阻止しなければなりません。

2 ランサムウェアの現状 2024 年版 - ソフォス
3 ソフォス「アクティブアドバーサリーレポート」2024 年上半期版 - ソフォス

典型的なランサムウェア攻撃は次のように行われています。



サイバー攻撃者は組織の IT やセキュリティチームが稼働していない、検出されにくいタイミングを狙って戦略的に攻撃を仕掛けていることを、防衛側の組織は認識しなければなりません。ランサムウェア攻撃は、IT チームによる監視が週末に手薄になることを悪用し、金曜日や土曜日に開始されることが多くあります。

Sophos X-Ops のインシデント担当者による分析によると、2023 年のランサムウェア攻撃の 43% は、このような曜日を狙って実行されており、攻撃の 91% は、被害を受けた組織の通常の営業時間 (組織のタイムゾーンにおける月曜日から金曜日の午前 8 時から午後 6 時) を外して開始されており、検出と対応が手薄になる時間帯を狙っています [4]。

リモートランサムウェア

「Microsoft デジタル防衛レポート 2023」によると、人が操作するランサムウェア攻撃の約 60% でリモートから暗号化が実行されています。リモート暗号化はリモートランサムウェアとも呼ばれており、侵害されたエンドポイントを使用して、同じネットワーク上の他のデバイスのデータを暗号化します。

リモート暗号化が広がっている主な要因は、攻撃を広範囲に実行できる能力にあります。他のデバイスに高度なセキュリティソリューションがインストールされていたとしても、管理されていない、あるいは十分に保護されていないエンドポイントが 1 台でもあれば、組織全体が悪意のあるリモート暗号化による攻撃を受ける恐れがあります。

すべてのエンドポイントセキュリティソリューションがリモートランサムウェア攻撃を効果的に防御できるわけではありません。そのため、企業はリモートランサムウェア攻撃の脅威を強く認識しなければなりません。

RDP は、Remote Desktop Protocol (リモートデスクトッププロトコル) それとも Ransomware Deployment Protocol (ランサムウェア展開プロトコル) ?

RDP (Remote Desktop Protocol) は、2023 年にソフォスのインシデント対応チームが調査したサイバー攻撃の 90% 以上に関与しており、前年の 83% から増加しています。[5]

RDP や VNC (Virtual Network Computing) のようなデスクトップ共有ツールは、リモートからシステムを管理するのに便利ですが、適切な防衛策を講じなければ、ランサムウェア攻撃者によって、特権の昇格、認証情報の窃取、ラテラルムーブメント、バックドアのインストール、偽アカウントの作成、検出の回避のために悪用されます。

攻撃者が、外部アクセス、内部アクセス、ラテラルムーブメントのために、RDP を使用しないようにすることが重要です。RDP を外部ネットワークに公開しない対策は進んでいますが、攻撃者は RDP を組織内部のラテラルムーブメントに広く利用するようになっています。

4 アクティブアドバーサリーの阻止：最前線のサイバー防御からの教訓 – ソフォス

5 ソフォス「アクティブアドバーサリーレポート」2024 年上半期版 - ソフォス

ランサムウェア対策のベストプラクティス

ランサムウェアや他の脅威から組織を守るためには、最新のセキュリティソリューションを導入するだけでは不十分です。定期的な社員トレーニングなど適切な IT セキュリティプラクティスが不可欠です。すべての対策を網羅しているわけではありませんが、以下のベストプラクティスに従っていることを確認してください。

1. パッチを早期かつ頻繁に適用

すべてのランサムウェア攻撃は望ましくない結果を引き起こしますが、パッチが適用されていない脆弱性の悪用に起因する攻撃は、特に深刻な損害をもたらします。この方法によって攻撃を受けた組織は、侵害された認証情報を起点とする攻撃を受けた組織と比較して、復旧のコストが 4 倍となり、復旧までの時間も長期化したことを報告しています。

2024 年におけるランサムウェア攻撃の最大の根本原因は、パッチを適用していない脆弱性の悪用でした。[6] マルウェアやサイバー攻撃者は、人気の高いアプリケーションに存在しているセキュリティ脆弱性を悪用します。エンドポイント、サーバー、モバイルデバイス、およびアプリケーションにパッチを少しでも早く適用すれば、サイバー犯罪者が悪用できる脆弱性を少なくすることが可能です。[7]

2. 強力なパスワードを使用

些細な事のように思われるかもしれませんが、実際はそうではありません。脆弱で予測可能なパスワードを使用すると、ハッカーは数秒でネットワーク全体にアクセスできます。パスワードはユニークなものにしてください。大文字と小文字を組み合わせて少なくとも 12 文字で構成し、Ju5t.LiKETh1s! のように特殊文字をランダムに追加することをお勧めします。

3. 多要素認証 (MFA) の有効化

MFA は、最初の要素 (通常パスワード) の後に追加のセキュリティの追加レイヤーを提供します。MFA をサポートしているすべてのアプリケーションとサービスで MFA を有効にすることが重要です。攻撃者は、ダークウェブから有効な認証情報を購入し、組織の環境に侵入した後に認証情報を積極的に窃取することが多くあります。

6 ランサムウェアの現状 2024 年版 - ソフォス
7 パッチが適用されていない脆弱性 : 最も凶悪なランサムウェア攻撃ベクトル - ソフォス

MFA は、サイバー攻撃者にとって障害となり、追加の本人確認を行わなければ有効なユーザーとして認証されることがなくなります。最後に、アプリケーションが対応している場合は、フィッシングに耐性の高いパスキーを使用します。

4. 内部および外部ネットワークアクセスの制御

ネットワークポートを公開したままにしないでください。組織の RDP アクセスおよびその他のリモート管理プロトコルをロックダウンします。リモートユーザーが、アプリケーション、サービス、その他の組織のリソースにアクセスするときに、ゼロトラストネットワークアクセス (ZTNA) ソリューションを確実に使用できるようにします。

5. 管理者権限を管理

ローカル管理者権限とドメイン管理者権限を常に確認してください。誰に権限があるかを確認し、必要としないユーザーは削除します。必要以上に管理者としてログインしたままにしないでください。

6. データを複数の場所に定期的にバックアップし、復元の手順を定期的に練習する

「ランサムウェアの現状 2024 年版」の調査では、暗号化されたデータを使用している IT 管理者の 68% が、バックアップを使用してデータを復元していました。定期的にデータを複数の場所にバックアップし、クラウドにあるバックアップを保護するために MFA を使用します。バックアップからデータを復元する手順を練習しておき、インシデントが実際に発生したときにスムーズに復元できるようにします。潜在的な脅威からバックアップを保護するために、攻撃が疑われる行動を監視します。

7. 不要なアプリケーションの削除

攻撃者は、一般的にインストールされているアプリケーションを悪意のある目的で使用しています。この手法は「環境寄生型攻撃」と呼ばれ、通常の業務で使用されるアプリケーションが攻撃に転用されるため、正規の目的で利用されているのか、悪意のあるアクティビティなのかを区別することが困難になります。業務のためにアプリケーションを必要としない場合、そのアプリケーションをインストールすべきかどうかを慎重に検討してください。必要であることが確認できなければ、インストールしないようにしましょう。

8. ネットワークで保護されていないデバイスの特定

攻撃者は、エンドポイント保護機能が実行されていないデバイスを探し出し、検出されずに環境に常駐しようとします。これらのデバイスは無防備であり、リモートランサムウェア攻撃に悪用される恐れがあります。

エンドポイント保護のベストプラクティス

予防のための高度な技術と脅威ハンティング機能に対応するエンドポイント保護、EDR、XDR を活用することで、ランサムウェア攻撃から効果的に組織を保護することができます。

セキュリティツールの設定ミスは、組織における最大のサイバーセキュリティリスクと考えられています[8]。正しく設定されていないポリシー設定、除外、その他の要因がある場合、セキュリティポスチャが損なわれる可能性があります。エンドポイント保護機能が正しく設定され、適切な保護機能が有効になっていることを確認してください。

ランサムウェアからエンドポイントデバイスを保護するために、次のベストプラクティスを実行することをお勧めします。

1. 推奨されるすべてのポリシーと機能を有効にする

当たり前のようですが、これはエンドポイントセキュリティソリューションの効果を最大限に得るための確実な方法です。

セキュリティソリューションのポリシーと設定は特定の脅威を阻止するために設計されており、すべての保護オプションが有効になっていることを定期的に確認することで、最新のランサムウェアや新種のランサムウェアからエンドポイントを確実に保護します。ファイルレス攻撃の手法を検出する機能や挙動分析テクノロジーが有効になっていることを確認してください。以下を実行することをお勧めします。

A) タンパープロテクションを有効にします

これにより、エンドポイント保護ソフトウェアが不正に変更または削除されないようになります。サイバー攻撃は、システムにアクセスすると最初に、エンドポイント保護機能を無効化または削除しようとします。

B) フォレンジックデータの記録と保存を有効にします (理想的にはクラウドに記録を保存します)

セキュリティが侵害された場合、同じ問題の再発を防ぐために何が起こったのかを理解しなければなりません。しかし、サイバー攻撃者は攻撃の痕跡を消すためにシステムログを消去し、攻撃を理解するために役立つフォレンジックデータを削除することが多くあります。また、デバイスにアクセスできなくなる場合もあります。クラウドにアクティビティの記録を保存することで、攻撃を受けた後でも重要な情報にアクセスできます。

C) エンドポイント保護のコンテンツ (データなど) と製品機能のアップデートが有効になっていることを確認します

進化し続ける脅威環境に対応し、新たな脅威を防ぐためには、セキュリティ製品を定期的に更新して新しいデータを利用することが極めて重要です。製品やコンテンツのアップデートを無効にすると、時間の経過とともに保護機能が低下します。

2. 定期的に除外機能を確認する

除外することで、信頼できるディレクトリやファイルの種類がマルウェアのスキャン対象から外されます。この除外機能は、システムの遅延を減らしたり、セキュリティ警告の誤検知を最小限に抑えるために使用されることもあります。

時間が経過すると除外リストが増え、攻撃者に悪用されるセキュリティホールが生まれる恐れがあります。マルウェアが脅威検出の除外となっているディレクトリに侵入すると (おそらくユーザーが知らずにマルウェアをコピーした) は、攻撃が成功する恐れがあります。

ポリシーで設定されている除外リストを定期的にチェックし、除外する必要がないものがあればできる限り除外リストから削除します。削除できない除外については、できるだけ具体的に指定してください。たとえば、データベースのディレクトリやドライブを除外するのではなく、特定のファイルだけをフルパスで除外します。これにより、マルウェアがセキュリティを回避して、同じフォルダから実行されるのを防ぐことができます。

3. セキュリティコンソールで MFA を有効にする

MFA を有効にすれば、エンドポイント保護や他のセキュリティコントロールを管理するプラットフォームへのアクセスを確実に保護できます。これにより、攻撃者がエンドポイントやサーバーを攻撃に対して脆弱にするために意図的に設定を変更したり、保護機能を無効化あるいは削除したりすることを防ぐことができます。

4. 適切な IT プラクティスとハイジーンを維持する

定期的に IT ハイジーンを評価することにより、エンドポイントおよびエンドポイントにインストールされているソフトウェアを最大限の効率で実行できます。これにより、サイバーセキュリティのリスクが軽減され、将来のインシデントを修復する時間を節約できます。

8 中小企業におけるサイバーセキュリティスキル不足の解消 - ソフォス

IT ハイジーンを維持するプログラムを実装することは、ランサムウェア攻撃やその他のサイバーセキュリティの脅威から保護するために特に重要です。たとえば、RDP が必要な場所でのみ実行されていることを確認し、設定の問題を定期的に確認し、デバイスのパフォーマンスを監視し、不要なプログラムを削除します。IT ハイジーンをチェックすることで、ソフトウェアアプリケーションを更新する必要があるかどうかが明らかになる場合があります。また、データを定期的にバックアップする確実な方法でもあります。

5. 環境全体で活動している攻撃者をプロアクティブに追跡する

今日の脅威環境では、攻撃者はこれまで以上に狡猾になり、検出を避けるために正規のツールや窃取した認証情報を展開することが多くなっています。高度な脅威やアクティブアドバーサリーに対するプロアクティブなハンティングは、これらの環境寄生型攻撃を特定して阻止するために不可欠です。脅威を発見したら、すぐに適切なアクションを実行し、迅速に阻止する必要もあります。

社内のセキュリティチームは、EDR や XDR のようなテクノロジーを利用して、脅威をハンティング、調査、および無力化できるようになります。しかし、サイバー攻撃者は通常の営業時間外に攻撃を開始することが多いため、社内のセキュリティチームが攻撃を防ぐことができない場合もあります。多くの組織は、高度なランサムウェア攻撃を防ぐために 24 時間体制で脅威を監視して対応することに苦労しています。そのため、多くの組織にとって MDR (Managed Detection and Response) サービスが重要となっています。

ランサムウェア攻撃を防ぐためにセキュリティテクノロジーを利用し多層防御を実現する

「予防は治療に勝る」という諺は、受けた損害を修復するよりも、問題を早期の段階で防ぐことの重要性を示しています。ランサムウェアから組織を守るには、複数のテクノロジーを連携させて優れた防御と可視化を可能にする多層防御のアプローチが有効です。多層防御のアプローチでは、エンドポイント保護から始め、ニーズの変化に応じてレイヤーを追加し、保護と可視性を強化できます。

以下のコンポーネントを多層防御に追加できます。

- **ファイアウォール**は、攻撃が疑われるネットワークトラフィックを識別・ブロックし、脅威の侵入を阻止します。ファイアウォールは、外部と送受信されるネットワークトラフィックを可視化しますが、自社環境内のネットワークトラフィックを可視化することはできません。
- **NDR (Network Detection and Response)** 製品は、保護されていないデバイスを検出し、ネットワーク内でラテラルムーブメントを行っている攻撃者を検出できます。NDR は、ファイアウォールでは対応できない社内のネットワークトラフィックを可視化します。
- **XDR プラットフォーム**は、脅威ハンティング、調査、無力化のための機能を提供します。また、他の IT セキュリティソリューションと連携させることができ、共通のプラットフォームからすべてのセキュリティコントロールを可視化して管理できます。
- **MDR サービス**は、テクノロジーソリューションだけでは防ぐことができないサイバー攻撃を検出して対応する専門家が 24 時間体制で監視および脅威ハンティングを提供するサービスです。MDR サービスを検討するときには、追加のコストをかけずに、攻撃を中断および封じ込め、完全に排除できるフルスケールのインシデント対応を提供していることを確認してください。MDR サービスは、環境全体を完全に可視化するために、既存のサイバーセキュリティツールと統合できる必要があります。MDR は、人間が主導する高度なランサムウェア攻撃に対しても、最高レベルの保護を提供します。
- **外部攻撃対象領域管理 (EASM) または脆弱性管理ソリューション**は、優先的に対応すべき脆弱性を特定するために使用できます。これにより、攻撃者に脆弱性が悪用される前に、適用されていないパッチを特定することが可能になります。

ソフォスのランサムウェアへの対策

Sophos Endpoint は、1 つのセキュリティテクノロジーに依存することなく、予防を重視しながら包括的なアプローチに基づいて脅威をブロックします。Sophos Endpoint は、さまざまな攻撃をブロックする以下の高度なテクノロジーを使用します。

- **隙のないランサムウェア対策**によって、新しい亜種を含む、ローカルおよびリモートのランサムウェア攻撃から保護します。悪意のある暗号化をリアルタイムで阻止し、変更されたファイルを自動的に元の状態にロールバックして、ビジネスへの影響を最小限に食い止めます。
- **エクスプロイト対策テクノロジー**は、攻撃チェーン全体のさまざまな攻撃手法を阻止し、ファイルレス攻撃やゼロデイ攻撃にも対応します。
- **適応型攻撃防御**は、業界初の動的な保護機能であり、アクティブアドバーサリーやハンズオンキーボード攻撃にも対応します。攻撃の状況に合わせて動的に高度な防御機能が有効になり、攻撃対象領域を最小化し、攻撃を中断して、その進行を防ぎます。

Sophos Endpoint はセットアップと管理も簡単です。Sophos Endpoint をインストールしてお試しください！推奨される保護テクノロジーはデフォルトで有効になっており、調整せずにすぐに最強の保護設定を利用できます。必要な場合には、詳細にコントロールすることもできます。

Sophos Endpoint は、世界で最も信頼されているサイバーセキュリティプラットフォームである **Sophos Central** から管理できます。Sophos Central は、強力なクラウドベースのサイバーセキュリティ管理プラットフォームであり、ソフォスのすべての次世代セキュリティソリューションを連携させており、アクセスするときには MFA が適用されます。

ソフォスのお客様は、Sophos Central でエンドポイント保護を管理し、「アカウントの状態チェック」機能を利用できます。アカウントの状態チェクは、セキュリティポスチャのずれや例外、そしてリスクの高い設定を特定し、管理者がワンクリックで問題を修正できるようにします。

Sophos XDR – プロアクティブな脅威ハンティングおよび IT ハイジーンツール

Sophos XDR は、Sophos Endpoint の予防重視のアプローチに基づいて構築された統合型の検出および対応プラットフォームです。Sophos XDR を使用すると、すべての主要な攻撃ベクトルに対応でき、短時間で多段階型の脅威を検出・調査して、対応できます。

ソフォスのテクノロジーが Sophos XDR プラットフォームに完全に統合されており、シームレスに最高の成果を実現します。さらに、サードパーティのエンドポイント、ファイアウォール、ネットワーク、メール、アイデンティティ、生産性向上ソフトウェア、クラウドセキュリティ、バックアップおよびリカバリソリューションの広範なエコシステムと簡単に統合でき、既に導入しているサイバーセキュリティ製品を活用しながら、投資収益率 (ROI) を向上できます。

Sophos XDR は、セキュリティアナリストや IT 管理者の効率性を最大化するように設計されたツールと機能を提供します。

- すべての主要な攻撃対象領域にわたって脅威を検出する優先順位を AI が決定し、早急な対応が必要な不審なアクティビティを特定します。
- 検出された問題は自動的に MITRE ATT&CK の戦術にマッピングされるため、防御上の自社の弱点を簡単に特定できます。
- プロセスの終了、ランサムウェアのロールバック、ネットワークの隔離などのアクションを自動化し、脅威を迅速に封じ込め、貴重な時間を節約します。セキュリティアナリストは、セキュリティの強化に焦点を当てた生成 AI 機能を利用して、攻撃をすばやく無力化でき、効率的に業務を進めることができるようになるため、企業に信頼と安心をもたらします。

Sophos MDR - 24 時間 365 日体制の検出・対応サービス

Sophos MDR は、24 時間 365 日体制のマネージドセキュリティサービスで、高度なスキルを持つ専門家がお客様に代わって新しい脅威や高度なアクティブアドバーサリーから組織を守ります。Sophos MDR サービスは、最も優れたランサムウェア対策を提供します。

Sophos MDR Complete サービスを使用すると、追加料金なしで、作業時間に関する制限のないフルスケールのインシデント対応を利用できます。ソフォスの専門家が、お客様に代わって、リモートから攻撃を阻止して封じ込め、完全に排除するための一連の対応策を広範囲にわたって実行します。

Sophos MDR は、Sophos XDR と同様に、すべてのソフォス製品のテレメトリを統合して収集します。また、同じように広範なサードパーティのセキュリティ製品のテレメトリも統合でき、環境全体を包括的に可視化し保護を強化できます。

Sophos Incident Response Services Retainer - インシデントが発生したときに迅速に対応

サイバー攻撃を受ける前にインシデント対応チームを設置しておくことが、貴重な時間を節約し、コストを削減し、ランサムウェアの展開などのセキュリティ侵害の影響を軽減する唯一の方法です。

Sophos Incident Response Services Retainer は、インシデント対応の専門家からなるオンデマンドチームの支援を利用できる年間サブスクリプションで、お客様の環境で迅速に対応して、アクティブアドバーサリーを妨害、封じ込め、完全に排除します。また、組織のセキュリティ体制を改善し、侵害の可能性を軽減する重要なインシデント対策リソースも含まれています。

注：Sophos MDR Complete サービスをご利用の場合、フルスケールのインシデント対応が標準で組み込まれており、Sophos Incident Response Services Retainer は不要です。

Sophos Managed Risk – 脆弱性の管理と外部攻撃対象領域管理サービス

パッチが適用されていない脆弱性は、ランサムウェア攻撃の主な根本原因であるため、脆弱性が攻撃され影響を受ける前に、環境全体で高リスクのエクスポージャーを特定・調査し、優先順位を付けて解決することが極めて重要です。Sophos Managed Risk は、業界をリードする Tenable のテクノロジーを活用し、脆弱性管理のニーズに対応します。

Sophos Managed Risk を使用すると、ソフォスの経験豊富なアナリストがお客様の環境内で優先度の高いサイバーセキュリティの脆弱性や潜在的な攻撃ベクトルを特定し、ビジネスに支障をきたす前に攻撃を防止する対策を講じます。

結論

ランサムウェアは進化を続けており、被害を受けた組織に身代金の支払いを強制させる手段として依然として猛威を奮っています。攻撃者が組織に侵入するのを阻止し、万一侵入された場合は迅速に検出して排除しなければなりません。IT およびエンドポイントセキュリティのベストプラクティスを確実に取り入れ、エンドユーザーへの教育を継続し、自社環境における脅威や攻撃者に対する警戒を怠らないようにしてください。24 時間 365 日体制で検出および対応し、予防を重視した多層防御のアプローチは、ランサムウェアや最新の脅威から組織を守る最善の方法です。

ソフォスがランサムウェア対策の最適化を支援する方法について、ソフォスのアドバイザーにご相談いただくか、www.sophos.com をご覧ください。

© Copyright 2024.Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
ソフォスは、Sophos Ltd. の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。

2024-10-01 (WP-NP)

SOPHOS