yubico

ホワイトペーパー

ランサムウェアリスクを軽減

強力な認証と最新のMFAの重要な役割

目次

ランサムウェアのリスクを軽減

強力な認証と最新のMFAの重要な役割

ランサムウェアは 2020 年に485% を超えて増加しました [1]

ランサムウェアツールと引き換えに利益を共有する新たなRaaS (サービスとしてのランサムウェア) モデルが有効性が判明しました。

はじめに

パソコンメーカー、食肉業者、メンタルヘルスクリニックの共通点は何でしょう？ いずれもランサムウェアの被害者です。彼らだけではありません。ランサムウェア攻撃は2020年に485%を超えた増加 をみせ、ランサムウェアツールと引き換えに利益を共有する新たなRaaS (サービスとしてのランサムウェア) モデルが活用されました。

米国東部で数百万人の日常生活に支障をきたしたコロニアル・パイプライン社のランサムウェア攻撃 は、メディアで激しく取り上げられました。最近では、ホワイトハウスがさまざまな取り組みやグローバルカンファレンス を発表し、攻撃者を混乱させ、被害者を支援しています。ランサムウェアに関して言えば、問題なのは、組織が標的になるかどうかではなく、いつ標的になるかということです。あなたの組織はその日のためにどんな準備していますか? これは、すべてのビジネスリーダーが考慮すべき問題です。

ランサムウェアとその強力な認証との関係は、今のところあまり理解されていません。結局のところ、ランサムウェアはシステムとそのデータを攻撃し、身代金が支払われるまで暗号化して人質に取るように設計されたマルウェアの一種です。それが認証と何の関係があるのでしょうか？ 強力な認証では、データへのアクセスを承認する前に、ユーザーまたはマシンの信頼できるIDを確認します。強力な認証とランサムウェアの関係の手掛かりは、ランサムウェアを使用するアクターが組織に侵入できる方法を考えることにあります。一般的なのは、ユーザーが偽のリンクをクリックして、知らないうちにマルウェアをシステムにダウンロードするという方法ですが、もう一つの陰湿な方法として、攻撃者が盗んだ認証情報を使ってアカウントを乗っ取り、正規のユーザーになりすましてネットワークに侵入し、自らシステムにマルウェアをインストールして、有害なプロセスが進行するのを監視することが挙げられます。これは非常に意図的な連鎖ですが、組織がパスワードや従来の多要素認証 (MFA) を超越する強力な認証方法を使用して阻止できれば、攻撃者の計画を大幅に撃退することができます。

このホワイトペーパーでは、ランサムウェアとは何か、一般的に誰が関係するか、強力な認証と最新のMFAがランサムウェアのリスクを軽減するために果たす重要な役割、この急速に拡大している憂慮すべき現象から保護するための優れたセキュリティおよびプロセス予防策の推奨事項について、分かりやすく説明します。

ランサムウェアの定義

サイバー攻撃の多くは、標的のシステムに危害を加えたり悪用したりするように設計された、悪意のあるソフトウェア（マルウェア）を利用しています。前述のように、ランサムウェアはシステムとそのデータを攻撃し、身代金が支払われるまでシステムを人質に取るマルウェアの一種です。ランサムウェア攻撃者がよく使うビットコインなどのデジタル通貨は、追跡が困難です。通常、価値のあるデータは攻撃者が管理するシステムにコピーされ、身代金要求の一環としてデータの公開という危険にさらされます。

2021年にランサムウェア攻撃からの復旧に要した平均コストは185万ドル で、これには身代金、業務が中断した時間、売上損失、運用コスト、訴訟費用が含まれます。より機密性の高い、または重要なデータやシステムが関係するランサムウェア

攻撃では、コストは444万ドル 近くに上り、データ漏えいに要した平均コスト (386 万ドル) を上回ります。被害者の57% 以上が、データの復旧や流出防止のために身代金の支払いを終えていますが、実際にすべてのデータを取り戻すことができた被害者はわずか8% にすぎません。

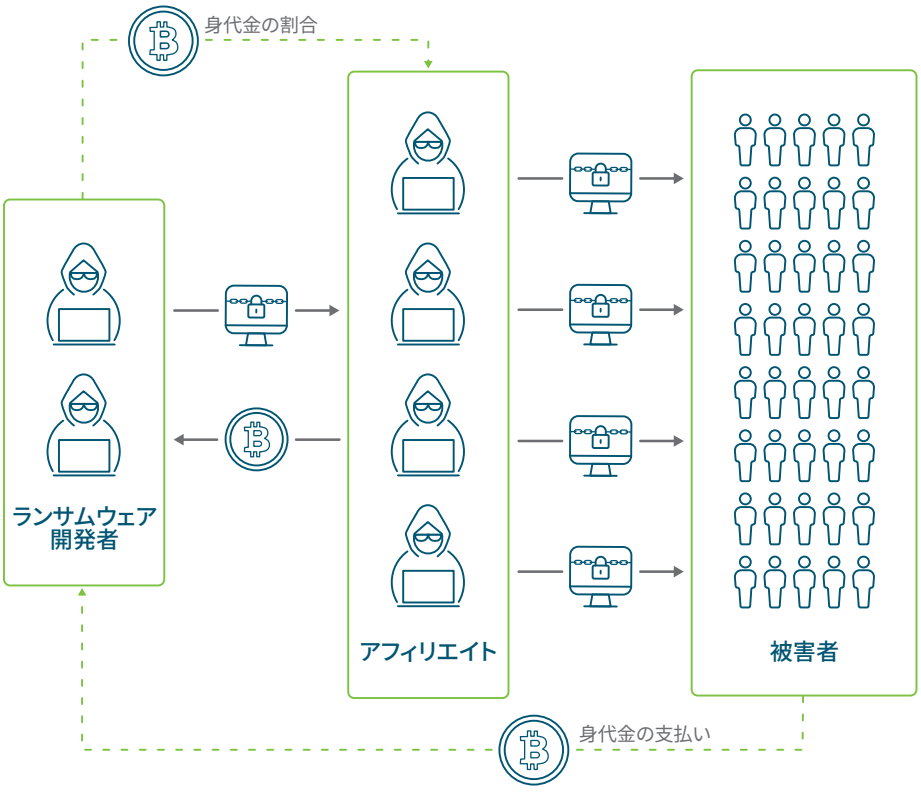
ランサムウェアの背後に潜む悪意のあるアクター

ランサムウェアの増加は、主にロシアや旧ソビエト諸国、中国 を拠点とする組織的な犯罪グループ によるもので、DoppelPaymer、REvil、Ryuk、Darkside、Mazeなどの名前がついています。

これらのランサムウェアグループは、ソフトウェア開発者がランサムウェアを作成し、企業の弱点を見つけてランサムウェアを展開する「アフィリエイト」と呼ばれるオペレーターに引き渡すという、高度な犯罪ネットワークのプレーヤーです。

彼らは被害者から受け取った身代金を分配しています。これらのアクターがさまざまな手法を使用して組織の弱点に侵入し、ユーザーの代わりにランサムウェアをインストールする方法については後ほど説明します。幸いなことに、今日ではアカウントの乗っ取りを防ぐ方法があるので、悪意のあるアクターがユーザーに代わってログインし、マルウェアをインストールしてシステムに侵入することはできません。

犯罪ウェアエコシステム



ランサムウェア攻撃は広範囲に及ぶ

ランサムウェア集団はあらゆる業界や地域を標的にしており、特に大企業や政府機関を標的にしています。2021年3月、REvilはAcerに対して5,000万ドルのランサム攻撃の責任を訴え、侵害された証拠として盗まれた文書の一部を公開しました。この身代金は、単一の要求としてはこれまでで最大規模でした。JBS S.A.はブラジルの食肉複合企業であり、米国子会社は同国の食肉供給の1/5以上を占めていますが、攻撃によりITシステムがオフラインになって業務が停止したことを受け、今年6月に1,100万ドルの身代金 をREvilに支払いました。

1つのパスワードのせいでハッカーがコロニアル・パイプライン社を妨害、とCEOは上院議員に報告

コロニアル・パイプライン社のジョセフ・ブラント最高経営責任者は、米国の 上院の委員会に対し、多要素認証（MFA）が導入されていない従来の仮想プライベート・ネットワーク（VPN）システムを使って攻撃が行われたと述べました。

このような身代金要求の規模も衝撃的ですが、業務に与える影響は最も破壊的なものであることが少なくありません。アイルランドの公的医療機関ヘルス・サービス・エグゼクティブ（HSE）では、ランサムウェアContiの亜種が蔓延したためITシステムが完全に停止し、患者の予約や電子医療記録へのアクセスが影響を受け、一部のシステムは数週間後もオフラインのままでした。HSEは攻撃者グループ（ウィザード・スパイダー）に身代金を支払うことはありませんでしたが、それでも影響総額は 1億1,800万ドル（1億ユーロ）以上に上ります。フィンランドでは、メンタルヘルスプロバイダーのVastaamoがランサムウェアの攻撃を受けました。攻撃者はVastaamoと個々の患者を脅迫し、治療セッションの記録を暴露すると脅しました。この攻撃の結果、Vastaamoは破産 を申請せざるを得ませんでした。2021年4月には、DarkSideグループが漏洩パスワード を使ってマルウェアを仕込み、440万ドルの身代金が支払われるまでコロニアル・パイプライン社を停止させました。Darksideランサムウェア集団は、非常に単純に、多要素認証を使用していない非アクティブなアカウントを介してコロニアル・パイプライン社に侵入しました。

唯一問題だったのは、ネットワークに入るための仮想プライベート・ネットワーク（VPN）アカウントの、脆弱で弱いパスワードが漏洩した ことです。FBIがビットコイン・ウォレットを押収したことでこの身代金の一部は回収されましたが、Darksideは過去二年間の共同作業によって9,000万ドル以上のビットコインを得たと見られています。

サイバー犯罪者は、しばしばサプライチェーンの穴から侵入してきます。2021年7月、CISAとFBIは、Kaseya VSA（仮想システム管理）ソフトウェアのセキュリティ欠陥を利用した一連のランサムウェア攻撃に対応しました。この攻撃は1か月に 1,500社もの企業 を襲い、最初は約60の直接の顧客から始まり、他の顧客にも波及していきました。このトリクルダウン効果には、スウェーデンの食料品店800店舗がPOSシステムへの侵入を受けて1週間にわたり営業停止した ことが含まれます。犯罪者や日和見主義者は、ランサムウェア攻撃に関連したアップデートと思われるフィッシングメールを送信して、被害企業や利害関係者をさらに追跡します。

ランサムウェア攻撃に対して脆弱なのは誰か?

次に攻撃する場所を計画するとき、攻撃者は常に簡単に達成できる目標を探します。あらゆる犯罪組織と同じように、ランサムウェア集団も最小限の労力とリスクで最高の利益を得たいと考えているのです。最も脆弱なターゲットは、収益が大きい業界（すなわち、多額の身代金を支払うことができる）ですが、これらの業界の環境は複雑で完全に保護することが困難な場合があります。石油・ガス会社、他のエネルギー会社、金融サービス会社はすべてこのカテゴリーに分類されます。

次のような業界の組織は、収益の可能性が高く、テクノロジーなどの業界と比較してセキュリティの成熟度と近代化が比較的低いことから、しばしば「非常に脆弱」であると見なされます。

- エネルギー
- 医療
- 法務（法律事務所）
- 建設業
- 貿易機関
- 教育（学校区）
- 市町村（または小規模な政府機関）

ランサムウェア攻撃は、セキュリティの成熟度が低い従来の環境を標的にする可能性が高いです。「低成熟」とは、情報セキュリティに対する継続的かつ一貫した投資を行っていない企業を指します。このような組織には、専用のセキュリティチームが存在せず、パスワードやパッチの管理方法が不十分な場合があります。そのため、ランサムウェアにとって最も魅力的な標的であるこれらの業界の一部で、サイバー保険の増加が生じていても驚くにはあたりません。実際、一部のサイバー保険証券はMFAの実装を要求している場合があります。実装しない場合は保険料が増加したり拒否されたりする可能性があります。

強力な認証の役割

FIDOハードウェアセキュリティキーの使用など、強力な認証と最新のMFAは、ランサムウェアのリスク緩和に非常に重要な役割を果たすことができます。FIDOハードウェアセキュリティキーはSMSやモバイル認証などの従来のMFAよりもはるかに安全で、より強力なフィッシング防御を提供します

ランサムウェアのリスクを軽減

指定可能な汎用のガイダンスはありません。各組織は、各自の既存インフラと今後の開発・成長計画を確認して、セキュリティ体制を強化しランサムウェアの脅威を軽減するために講じるべき措置を決定する必要があります。一つ明らかなのは、過去の攻撃やパスワード、さらには従来のMFA手法に基づいても、エラーが発生する余地がたくさん残されていることです。なぜなら、これらの認証メカニズムはすべて、フィッシングや中間者攻撃、システムへの侵入を目的とした他のさまざまな手法に対して非常に脆弱だからです。

FIDOハードウェアセキュリティキーの使用など、強力な認証と最新のMFAは、ランサムウェアのリスクを軽減するために非常に重要な役割を果たします。悪意のある攻撃者は、システムの脆弱性を探し、さまざまな方法を使用してマルウェアをシステムに侵入させます。よくある手口の一つは、漏洩したパスワードを使ってネットワークにアクセスし、システムにランサムウェアと呼ばれる身代金要求マルウェアをインストールするものです。

コロニアル・パイプライン社の事件と同じように、攻撃者はダークウェブ上で漏洩パスワードを使って、コロニアル社のネットワークにアクセスするために、多要素認証を使用していない仮想プライベートネットワーク（VPN）にログインしました。ネットワークに侵入すると、攻撃者はマルウェアをインストールしました。ダークウェブで盗まれたパスワードを購入するだけでなく、認証情報フィッシングなどの他の手段でパスワードを取得することも可能です。したがって、フィッシング対策用の最新の多要素認証を導入することは、アカウントの乗っ取りを阻止する非常に効果的な方法で、これにより、攻撃者がユーザーの代わりにランサムウェアをインストールすることを防ぐことができます。FIDOハードウェアセキュリティキーは最新のMFAの形式として、SMSやモバイル認証などの従来のMFAよりもはるかに安全です。ユーザーは、これらのランサムウェアのマルウェア詐欺が定着するのを防ぐ強力なフィッシング防御をすぐに入手できます。

システムへの感染に使われるもう一つの一般的な手法はクリックベイトスパムで、これは信頼すべきファイルを装った電子メールの添付ファイルです。ひとたびダウンロードして開かれると、被害者のコンピューターが乗っ取られます。特にソーシャルエンジニアリングツールが組み込まれている場合は、ユーザーを騙して管理者アクセスを許可させます。

重要なことは、可能であれば、ランサムウェアの脅威の影響を大幅に軽減するために、ユーザー認証用の最新のフィッシング対策MFAと組み合わせてデータをクラウドに移動することです。ただし、クラウドは万能ではありません。設定が不十分なクラウドシステムもランサムウェアの被害を受ける可能性があります。どのようなクラウド設定を構成するかを検討する場合は、SAAS (サービスとしてのソフトウェア) ソリューションにはパッチを適用する必要はありませんが、PAAS (サービスとしてのプラットフォーム) システムには定期的なパッチを適用する必要があるため、完全に移行する前にパッチポリシーとガイドラインを設定する必要があります。

クラウドで作業する安全な組織は、通常次のものを備えています。

- すべての証明書利用者を保護するシングルサインオン (SSO) システム
- フィッシング対策MFAを全システムに導入
- ユーザーが相反する責任を持たないようにするための管理統制と職務の分離

さまざまな理由で、すべてのデータをクラウドに移動することはできない場合があります。適切な認証とアクセス制御のすべてを備えた最新のデータベースバージョンを実行するローカルサーバーを使用してインフラを自社運用する組織では、ランサムウェアのリスクを軽減するための適切なレベルのセキュリティを確保することもできます。ただし、自社運用の環境は、長期間にわたり管理して最新の状態に保つのが複雑になる場合があります。

ランサムウェアの攻撃を想定した計画立案

大切なのはできるだけ積極的に行動し、すでに起こった不幸な出来事から学ぶことです。効果的な戦略のためのいくつかの重要な要素にはランサムウェアを事業継続計画とIT災害復旧計画に組み込むことが含まれます。全体的なセキュリティ戦略の評価と全般的なセキュリティ予防策を評価して、ユーザーが強力な認証とさまざまなベストプラクティスを使用して機密データとシステムを保護していることを確認します。

ランサムウェアに関して企業が犯しがちなミスとその回避方法

推奨される全体的なアプローチは、積極的に行動し、組織が健全で最新のセキュリティ戦略と心構えを持つようにすることです。これは、最初の段階でランサムウェアの脅威を緩和するうえで大きな役割を果たします。ただし、ランサムウェア攻撃が発生した場合、侵入が発覚したその日から、「絶体絶命」モード に移行してしまう傾向があります。パニックになる気持ちを抑えてください! ここでは、ランサムウェアの発生を軽減してから管理するための合理的な手順、およびよくある間違いを回避する方法をご紹介します

事前計画／軽減:

- ランサムウェアを事業継続計画とIT災害復旧計画に組み込み、組織全体で正しく評価されるようにします
- 健全なセキュリティに対する心構えと全般的なセキュリティ予防策を確認します
- パッチ管理によってすべてのシステムに正しくパッチが適用されていることを確認し、エントリーポイントから開始してギャップに対処します
- 攻撃者が代わりにログインしてマルウェアをインストールしないように、最新のフィッシング対策MFA機能を展開し、IAMシステムを導入している場合は最新化します
- 可能な場合はデータをクラウドに移動し、ビジネスをサポートする新しい機能を追加する移行計画を採用します
- バックアップが別の場所で保護および保存されていることを確認します。強力な認証でバックアップを保護します
- 保険会社に相談します。保険会社は、迅速な行動計画を用意している可能性があります
- ランサムウェアについて従業員を教育し、リスクを軽減します

驚異的な身代金の支払額

2021年3月、REvilはAcerに対して5,000万ドルのランサム攻撃の責任を訴え、侵害された証拠として盗まれた文書の一部を公開しました。この身代金は、単一の要求としてはこれまでで最大規模でした。

JBS S.A.はブラジルの食肉複合企業であり、米国子会社は同国の食肉供給の1/5以上を占めていますが、攻撃によりITシステムがオフラインになり業務が停止したことを受け、2021年6月に、1,100万ドルの身代金をREvilに支払いました。

攻撃初日：

- インシデント対応チームと連携して、漏洩と攻撃を阻止し、攻撃が継続または拡大しないようにします。さらに、調査のためにフォレンジックデータが保護されていることを確認します
- インシデント対応計画の一環として、このシナリオで他の組織を支援した経験があり、攻撃への対応で考慮するプロセスと組織に関するガイダンスを提供できる、既に契約済みの外部弁護士に相談します
- 主要なコンプライアンス機関からの情報を参照します（理想的には、この調査がすでに実施され、レビュー済みで、容易にアクセスできる場所にあることが望ましい）。米国 財務省の外国資産管理室 (OFAC) は、ランサムウェア攻撃に対処する際に注意すべき点に関するガイドラインなどを発表しています

回避すべきいくつかの落とし穴：

- 支払いを最初の選択肢にしないでください。まず、適切な精査を行い、ランサムウェアに関するCISAの推奨事項を確認します。場合によっては、政府によって「制裁対象の行為者」としてリストされている攻撃者にお金を払うと、会社が危険にさらされる可能性があります
- ランサムウェアのインシデント対応計画 がないまま、捕まれないようにしましょう。この計画は、攻撃を受ける前に適切に設定し、定期的に更新してテストする必要があります。攻撃時に重要な決定をその場で下す必要がなくなるように、十分に詳細に計画する必要があります。シニアリーダーは計画に関与して責任を持つ必要があり、経験豊富なセキュリティおよび運用担当者には実行可能で実用的な計画を構築する権限が与えられる必要があります。この計画は、事業継続計画や災害復旧計画およびチームと連携し統合する必要があります
- サードパーティのベンダーに依頼して攻撃を管理？ サポートレベル契約が初日の活動をサポートするのに十分であり、コンプライアンス機関によって承認されていることを確認します

攻撃と戦う - ランサムウェアを防御するためのベストプラクティス

ランサムウェアに対する特効薬はありませんが、多面的なアプローチにより、企業のランサムウェア攻撃への対応と復旧を支援することができます。

- すべてのアカウントにフィッシング対策認証を使用します。一度ならず、脆弱なパスワード、再利用されるパスワード、SMS、ワンタイムパスワード（OTP）、プッシュアプリベースの多要素ソリューションによって、ランサムウェアやその他の攻撃が実行されます。Mutual TLSとWebAuthn/FIDO は、どちらもこれらの脆弱性から保護します。YubiKeyは、これら最新のフィッシング対策プロトコルや、OTPなどの従来の認証と連携するように設計されています
- パッチ管理。企業全体ですべてに迅速にパッチを適用するには、多大な労力が必要です。自動パッチ管理を目標として、アクセスポイントにはできるだけ早くパッチを適用する必要があります。すべてのシステムには、制限された例外のないパッチ適用スケジュールが必要です。また、いかなる例外も、CISOとリスクを受け入れる最高位のビジネスリーダーによって承認される必要があります

業務に壊滅的な影響を与える可能性があるランサムウェア

例えば、アイルランドの公的医療機関ヘルス・サービス・エグゼクティブ（HSE）では、ランサムウェアContiの亜種が蔓延したため、ITシステムが完全に停止し、患者の予約や電子医療記録へのアクセスが影響を受け、一部のシステムは数週間後もオフラインのままでした。

フィンランドでは、メンタルヘルスプロバイダーのVastaamoがランサムウェアの攻撃を受けました。攻撃者はVastaamoと

個人の患者を脅迫し、治療セッションの記録を暴露すると脅しました。Vastaaamoはこの攻撃の結果、破産を余儀なくされた

- 重要なデータは何か、なぜそれが重要なのかを理解します。データ中心のセキュリティ管理戦略に従い、主要なビジネスオーナーと定期的にデータ分類リストを検証します。重要なデータを保持、操作、または転送するシステムを評価します。データを評価するために、業界のデータ分類のベストプラクティスを評価し、データを適切なコントロールに適切に配置します
- 重要なデータを直接処理しない場合でも、他の信頼できるシステムを含めることを忘れないでください。サプライチェーン攻撃により、ITチームが他のシステムへのアクセスを制御または管理するシステムを見過ごしたり、可視化できない場合に、壊滅的な被害を受ける可能性があります。自社運用、クラウド、サードパーティにより操作される場合であっても、これらの一元化された制御ポイントには、非常に高いセキュリティバーが必要です
- それらをテストして、信頼できるバックアップがあることを確認します。重要なデータおよび重要な任務事業システムの復旧に注目します。つまり、バックアップを作成するだけでなく、復旧をテストし、バックアップ・システムの権限モデルを理解して、バックアップを容易に削除できないようにします
- 重要なシステムの隔離を優先します。深層部に焦点を当てた侵入のほとんどは、身代金を要求する前に、可能な限り多くのデータとシステムを漏洩させます。ゼロトラストの原則によれば、すべてを隔離するべきです。ただし、設計と導入に自信をつけた後は、まず最も重要なシステムに焦点を当てるのは良いことです。脆弱性管理とパッチ適用戦略を含めます。システムへのアクセスだけでなく、システムからのアクセスにも注目してください。検知されずにシステムからデータを抽出することが簡単であればあるほど、ランサムウェア集団からの圧力や影響を受ける可能性が高くなります
- 必要なデータのみ残します。データ保存ポリシーと手順を確立し、定期的に見直す必要があります。積極的にオフラインで使用しないデータの保存を検討、または完全に破棄することを検討します。そこにないものは、盗まれて、お客様やお客様の情報を信頼しているユーザーに対して使用されたりすることはありません
- 専門家にシステムの定期的なテストを依頼します。「これを破ることを証明する」式の進入テストだけを対象としないでください。1つ以上のシステムに「ゼロデイ」脆弱性が存在すると想定し、侵害を検出して隔離し、迅速に復旧できるかどうかを判断する、共同の机上演習を使用します
- 身代金の支払いは避けてください。支払いをしてもランサムウェア攻撃がさらに増えるだけで、完全なデータやアクセスが戻る可能性は低いです。場合によっては、支払いを受け取るエンティティが制裁対象である可能性があり、違法になる可能性があります。攻撃に対して適切に準備するための時間と労力を費やすことで、その影響を最小限に抑えることができるのです

ランサムウェアのリスク軽減計画を作成するための主要なアクションアイテム

- 健全なセキュリティに対する心構えと全般的なセキュリティ予防策を確認します
- パッチ管理に穴がないことを確認します
- 最新のフィッシング対策MFA機能を展開し、IAMシステムを導入している場合は最新化します
- 可能な場合はデータをクラウドに移動し、ビジネスをサポートする新しい機能を追加する移行計画を採用します
- バックアップが別の場所で保護および保存されていることを確認します。強力な認証でバックアップを保護します
- ランサムウェアについて従業員を教育し、リスクを軽減します

YubiKeys、YubiHSM

ランサムウェア軽減戦略の重要なコンポーネントとしての最新の認証

Yubicoのフィッシング対策ハードウェアセキュリティソリューションであるYubiKeyは、ゼロトラストアプローチ「何も信用せず、すべてを検証する」をサポートします。YubiKeyは強力なユーザーIDおよびデバイス認証ソリューションであり、セキュリティ専用に設計されており、フィッシングやその他の形式のアカウントの乗っ取りを阻止し、強力な認証を大規模に提供します。

FIDO2/WebAuthnおよびスマートカード認証標準を活用することで、YubiKeyは自社運用環境またはクラウド環境でシームレスに動作し、登録済みサービス間での秘密共有に依存せず、携帯電話の接続を必要としません。つまり、YubiKeyはオフラインでも、いつでもどこでも動作することができ、ユーザーとそのIDに常時セキュリティを提供します。また、最も厳しい認証保証レベル3 (AAL 3) 要件を満たすFIPS 140-2認証済み製品ラインアップでは、FIPS要件を満たす必要がある組織に、直感的なユーザーエクスペリエンスと強力なセキュリティを提供します。

YubiKeyは企業や個人の住所に関わらず、簡単にユーザーに配布でき、リモートワーカーやハイブリッドワーカーを効率的に保護します。また、セキュリティキーを使用すると、ユーザーの自己登録が容易になり、既存のセキュリティインフラ、ID/アクセス管理プラットフォーム、その他の数百ものサービスとすぐに統合できるため、ユーザーIDをわずか数分で保護できます。YubiKeyを使用すると、組織は強力なセキュリティ、高速で簡単なユーザーエクスペリエンス、およびTCOの削減を実現します。

「誰も」「何も」信頼しないゼロトラストの世界では、組織は内部システムで使用される資格情報を保護して、攻撃者が特権アクセスを取得するために使用できないようにする必要があります。この点において、YubiHSM 2は、FIPS 140-2認証取得済みのLevel 3のソリューションまたはFIPS認証未取得のソリューションとして、いずれも同じ機能が装備された強力なソリューションを提供します。どちらのソリューションも、従来のHSMと比べてわずかなコストとサイズで、アプリケーション、サーバ、およびコンピューティングデバイスの妥協のない暗号化ハードウェアセキュリティを妥協なく保障します。

YubiKey 5 シリーズ
左から右へ：YubiKey 5 NFC、YubiKey 5C NFC、YubiKey 5Ci、 YubiKey 5C、YubiKey 5 NAno、YubiKey 5C NAno

YubiKey 5 FIPS シリーズ
左から右へ：YubiKey 5 NFC FIPS、YubiKey 5C NFC FIPS、YubiKey 5Ci FIPS、YubiKey 5C FIPS、YubiKey 5 NAno FIPS、YubiKey 5C NAno FIPS

YubiKey Bio シリーズ - FIDOエディション
左から右へ：YubiKey Bio - FIDO Edition、YubiKey C Bio - FIDOエディションn

YubiHSM 2 シリーズ
左から右へ：YubiHSM 2、YubiHSM 2 FIPS

ランサムウェアの未来

ランサムウェアに終わりはありません。当面の間、私たちと存在し続ける可能性があります。これまでの成功を考えると、ランサムウェアはあらゆる規模の業界や組織で拡散し続けるでしょう。ランサムウェアには複数の侵入ポイントがあり、さまざまな手法で脆弱性を悪用します（例：フィッシング）。これに対応するために、組織は、人、プロセス、およびテクノロジー間の脆弱な繋がりに光を当てセキュリティ体制を強化する必要があります。これは、セキュリティの全体的な態勢は、最も弱い部分の強さによってのみ決まるからです。パッチ管理とデータ復旧プロセスを緊密に調整する必要があります。さらに、強力な認証、クラウドへのデータの移行、最新のMFAのインストールは、次のランサムウェア攻撃を阻止するための重要な工程です。企業の最高位に承認され、定期的に実行される堅牢なインシデント対応計画を持っていると、起こりうる攻撃に対処する準備となります。

yubico

Yubicoについて

YubiKeyの発明者としてYubicoはセキュアなログインを簡単に、そして誰でも利用できるようにします。弊社はコンピュータやモバイル機器などへの安全なアクセスのための世界標準を設定するリーダー的存在です。YubicoはFIDO2、WebAuthn、FIDO Universal 2nd Factor (U2F)、およびオープン認証規格の開発者であり、コアコントリビューターです。

1つのデバイスで数百の一般向け、企業向けのアプリケーションやサービスに対応することができ、フィッシングに強い多要素認証(MFA)のゴールドスタンダードです。

Yubicoは株式非公開企業であり、世界中に事業所を有しています。詳細については次のリンクをご覧ください。 www.yubico.com.