the BULLETIN
Protiviti's Review of Corporate Governance
Volume 7, Issue 11

ランサムウェア：攻撃への予防・対応、攻撃からの回復

ランサムウェア攻撃は、すでに長年にわたって存在してきました。以前の攻撃者は、企業のコンピューターやネットワークシステムに侵入してデータを暗号化するものの、支払いを受ければデータを元に戻すというやり方でしたし、通常、要求する金額も最近の事例よりも少額でした。また、標的組織はバックアップからITシステムを復元して難を逃れたり、支払額をより少なくするよう交渉したりすることもできました。これらの事件のほとんどは金額的にさほど大きなものでもなく、公表もされませんでした。

対照的に、最近のランサムウェア攻撃は、より組織的になり、かつより巨額の身代金要求を伴うようになっています。彼らの意図は、データの単純な「盗難」ではなく、ビジネスを混乱させることにあります。最近報道されているいくつかの事件では、すべてのデータや、ビジネスネットワーク、アプリケーション、データへのすべてのアクセスが流出し、重要なビジネスプロセスが事実上停止することで、組織は完全にロックダウン状態になってしまいました。

ランサムウェアによる攻撃において、攻撃者は被害者に直接連絡してやり取りを図ってくることがあります。要求に応えられない場合はさらにビジネスを崩壊させるという明確な脅迫と共に、具体的な要求のリストが提示されます。攻撃者は、要求に応じれば完全な回復を行うと約束して攻撃の迅速な解決をちらつかせつつ、支払い金額を交渉してきます。

ランサムウェア攻撃を受けた企業への影響は、その企業の事業内容、財務力、ランサムウェア対策のための第三者との取り決めなどによって、さまざまな形で現れます。最近のいくつかの攻撃では、消費財などのB2C関連産業の企業などが標的となりました。これらは、重要インフラ関連や、サイバーセキュリティ規制の対象となっている業種と比べ、サイバーセキュリティへの投資の度合いが一般的により低い業種です。

ランサムウェア攻撃の防止

ランサムウェアキャンペーンの標的企業が被害を受けるのは、攻撃者が組織のセキュリティ上の弱みを見つけ、それを使ってシステムへのアクセスに成功したときです。

攻撃者は、さまざまな手法を使用してシステムにアクセスします。一般的な手法は次のとおりです。

- 盗んだ認証情報を使ってシステムにアクセスし、ランサムウェアをインストールする方法。攻撃者は、フィッシングキャンペーンやその他のソーシャルエンジニアリング手法を用いて認証情報を入手したり、ダークウェブのマーケットプレイスから購入したりします。

- ユーザーをだましてランサムウェアをデバイス（PCやタブレット、スマートフォン等）にインストールさせる方法。この攻撃経路の例としては、リンクや添付ファイルを電子メールで送信し、ユーザーがそれを開いてインストールしてしまうというケースがあります。

- 未修正のシステム脆弱性を悪用する方法。例えば、Microsoft Exchangeサーバには、最近、重大な脆弱性が見つかり、パッチがリリースされました。マイクロソフトは、Exchangeサーバを利用中の顧客に、直ちにパッチを適用するよう呼びかけましたが、残念ながら一部の組織はパッチを即時に適用しておらず、攻撃者が容易に侵入して悪用できる既知の脆弱性が残ったままになっています。

次の表は、企業がこれらの問題に対処するために使用できる対策を示しています。

侵害の局面	防御のポイント	
攻撃者がログインID/PWをダークウェブの市場で購入などして入手	• サイバー脅威インテリジェンス	• パスワードポリシーの管理
フィッシングなどを経由した初期侵入	• セキュリティアウェアネストレーニング	• コンプライアンスの文化
攻撃者が脆弱性を悪用してシステムにアクセス	• ネットワークセグメンテーション • 脆弱性管理	• エンドポイント脅威検知対応エージェント（EDR）
攻撃者が特権アクセスを取得	• 特権アクセス管理	• 多要素認証（MFA）

人的境界は技術的境界と同様に重要であると考えられます。つまり、企業の従業員のサイバーセキュリティに対する意識（アウェアネス）は、ランサムウェアに対する最も重要な防御メカニズムの1つであると言えます。従業員のリスクに対する認識とデータ保護者としての警戒心により、サイバー犯罪者が機密情報を入手したり、無防備なユーザーを騙して感染したファイルをダウンロードさせたりすることが難しくなります。

トレーニングや、フィッシングメールのシミュレーションテストによる継続的な強化により、従業員は、通常とは異なる電子メールメッセージ、見知らぬ相手からの添付ファイル、インターネットからダウンロードした認識できないアプリケーションの実行などに対する、レジリエンスを持つ防御ラインに生まれ変わることができます。

常に最新の状態に保たれているマルウェア対策ソフトウェアは、悪意のあるファイルを検出・ブロックしたり、疑わしいウェブサイトにアクセスした際にユーザーに警告を発したりすることで、フィッシングやマルウェアの攻撃から保護します。安全な電子メールゲートウェイは、送受信の電子メールをフィルタリングして脅威を特定し、その配信を防止し、ランサムウェアのファイルを未然に防ぎます。機械学習システムや人工知能アルゴリズムを搭載した脅威対策ソリューションは、配信後の脅威を阻止することができます。また、組織はウェブフィルタリングソリューションを使用して、特定のウェブサイトへのユーザーのアクセスを制限することができます。

攻撃への対応

ランサムウェア攻撃の影響は、ますます増加しています。初期のランサムウェアは、データを無作為に暗号化する自動化マルウェアでした。現在では、それだけではありません。現在のランサムウェア攻撃は、事前に計画された戦略的な組織的活動によって編成されており、偵察や組織の攻撃対象領域への侵入、データの迅速な窃取などが行われています。さらに、攻撃者に対する脅迫状を送り付けます。

企業にとって、攻撃を受けていることに気付いた場合、確立されたサイバーインシデント対応計画と運用回復プロトコルに従ってインシデントを管理することが非常に重要です。現代のランサムウェア攻撃は被害を受けた場合の影響が大きいため、対策には、より大規模な危機管理アプローチが必要です。このようなアプローチをとることで、攻撃後の完全な復旧とデータの検証の開始など、攻撃が影響を与える広

範なビジネスプロセスに効果的に対処することができます。

最近のランサムウェア攻撃に対抗するために多くの新しい手順、プロセス、スキルが必要になります。例としては以下のようなものがあります。

- 1つはサイバー保険会社とのやり取りです。保険契約に恐喝補償が含まれていて、ランサムウェア攻撃の調査、犯人との交渉、身代金の支払いにかかる費用がカバーされる場合、企業は攻撃が発生した際に直ちに利用することができます。なお、攻撃の頻度と深刻さが増すにつれ、ランサムウェアの保険金を支払う可能性を最小限に抑えるために、サイバー保険会社は、保険契約者にサイバーセキュリティのベストプラクティスを積極的に導入するよう促します。

- 多くの企業は、ランサムウェア攻撃を受けた場合の支払い交渉のために、ランサムウェアの経験がある外部の弁護士を探します。多くの重要な質問は事前に決定することができますが、企業が支払いを進めるための交渉合意に達した場合の支払い決定プロセスなど、攻撃を受けている最中に経営陣の意思決定が必要な場合が有ります。

企業の従業員のサイバーセキュリティに対する考え方は、ランサムウェアに対する最も重要な防御メカニズムの一つです。

- 攻撃が本質的なビジネス機能に影響を与えた場合、危機に対応する意思決定は混沌としたものになる可能性があります。危機対応計画は、基本的なサプライチェーン管理、財務、人事の要求を満たすための日常業務をカバーすべきですが、危機対応を行っている間は、これらは100％手作業の業務に戻る可能性があります。

- ランサムウェアの攻撃者の多くは、標的組織にビットコインなどのデジタル通貨で身代金を支払うよう要求します。企業は、ビットコイン取引所に積極的に連絡し、口座開設に必要な手続きや時間について相談したり、支払いを安全に管理するためのエスクロー機能（取引に際して信頼できる第三者として資金を預かり支払いを仲介する機能）について問い合わせたりするとよいでしょう。

- 企業が法的執行機関と関与を行うかどうか、いつ行うかの決定は、ポリシー上の懸案事項です。多くの場合、法的処置を行うかは、身代金の支払い額の大きさや、訴訟の機会があるかどうかに左右されます（ただし、訴訟によって損害を回復できる可能性は通常低いです）。最近のランサムウェア事件では、支払額が大きくなり、攻撃者との直接交渉が必要になったものもあり、ランサムウェアの攻撃を防ぐためのベストプラクティスは進化し続けています。米国では、バイデン政権が、ランサムウェア攻撃、重要インフラに影響を与えるサイバーインシデント、および政府や一般市民にリスクをもたらすその他の侵害行為について、連邦政府への情報開示を義務付けることを推進しています。この措置が採用されれば、ランサムウェア攻撃の被害者が法執行機関に通報することを長年にわたって奨励してきたFBIの姿勢を支持するものとなります。[1]

次の表に、攻撃に対応する際の対策をまとめました。

侵害の局面	防御のポイント	
攻撃者が機密窃取のためデータを収集	• 最小権限原則に従ったアクセス管理	• データ暗号化による保護
ランサムウェアが攻撃を発動	• エンドポイント脅威検知対応エージェント（EDR）	• サイバー保険 • システムとデータのバックアップ
攻撃者からの恐喝要求	• インシデント対応 • 危機管理	• 顧問弁護士との連携

1 “Biden Administration Wants to Require Businesses to Disclose Ransomware Attacks,” Masood Farivar, VOA, July 27, 2021, available at www.voanews.com/silicon-valley-technology/biden-administration-wants-require-businesses-disclose-ransomware-attacks.

当然のことながら、身代金を支払うかどうかは重要な検討事項です。会社が暗号化されたシステムやデータをバックアップしていれば、経営陣はより有利な立場で交渉に臨むことができます。そうでない場合は、要求された身代金に対して、暗号化されたデータの損失の価値を評価しなければなりません。

もう一つ重要なことがあります。身代金を支払っても、サイバー犯罪者が盗んだデータへのアクセスを返してくれるとは限りません。さらに、マルウェアはシステム内に残っているため、攻撃後にはシステムを徹底的に修復する必要があります。

攻撃からの回復

ランサムウェアの攻撃を受けた後は、まずなぜ、どのように起こったのかを事後分析し、今後の攻撃をより効果的に防止・検知するための是正措置を講じましょう。これには、暗号化を行って企業のデータをロックするために必要なアクセス権を、攻撃者がどのようにして取得したかを理解することが必要です。そのためには、ネットワーク上のすべての送受信トラフィックを継続的に監視して潜在的な脅威を発見するEDR/NDRソリューションにより、攻撃がどこで始まり、どのように進行したかを明らかにすることができます。

企業はこれらの情報から、同様のインシデントの再発を防ぐことができます。

企業のシステムからランサムウェアを消去することは、攻撃を受けた後の対応における最優先事項です。しかし、攻撃者が感染したファイルを解読するための鍵を提供しない場合、この対応を完了することは非常に困難です。また、仮に鍵が提供されていたとしても、ファイルやストレージデバイスをすべて消去して新たにやり直すことなく、ランサムウェアが完全に消去されたと経営陣が確信することはできないでしょう。

事前にデータをバックアップしておくことで、攻撃によるビジネスへの影響を軽減することができます。毎日のデータバックアップには、組織のITシステムに接続されていないオフサイトにデータを保存するプロセスを含める必要があります。可能であれば、バックアッププロセスには、ポイントインタイムリカバリー機能を備えることが推奨されます。この機能により、より迅速な復旧が可能になります。とはいえ、一貫したバックアップを行っていなかったり、バックアップをオフサイトに保存していなかったりする企業が多いのが現状です。しかしながら、企業のIT担当者は、継続的なバックアッププロセスの監視と検証を検討する必要があります。

重要な鍵となるレジリエンス

予防、対応、復旧の全ては、組織のオペレーショナル・レジリエンス（運用上の回復力）、すなわち、重要なビジネス・経済機能や基盤となるビジネスサービスの提供に影響を与える可能性のあるサイバー攻撃やその他の運用上の混乱を検知、予防、対応、復旧、学習するための組織の能力を意味します。レジリエンスの主要な構成要素には、重要なビジネスサービスと影響の許容範囲を定義して理解すること、シナリオテスト、定期的な自己評価を行うことなどが含まれており、ランサムウェア攻撃のリスクを管理するための重要な指針となります。

レジリエンスを実現するためには、6つの要素があります。

- **ガバナンスと文化を進化させる。**適切なガバナンス機能を確立し、組織の重要なビジネスサービスのニーズに基づいてレジリエンスプログラムを実装します。たとえば、リアルタイムのダッシュボード、レポート、企業文化への働きかけが該当します。

- **重要なビジネスサービスとプロセスを特定する。**顧客やその他の利害関係者にとって重要な会社の規制、義務または確立された基準に基づき、重要なビジネスサービスとプロセスを理解します。

会社が暗号化されたシステムやデータをバックアップしていれば、経営陣はより強い立場で交渉に臨むことができます。

- **重要なビジネスサービスとプロセスの包括的な対応付けを確立する。**既存の継続的な取り組みをベースに、重要なビジネスサービスやプロセスの提供・実行に寄与する重要なプロセス、アプリケーション、サードパーティ、その他のコンポーネントの包括的なマッピングを確立し、維持します。

- **「許容できない損害」を定め、影響の許容レベルを設定する。**オペレーショナル・レジリエンスに関する事象が企業のさまざまなステークホルダーに与える影響を理解し、最も影響度の高い重要な領域を特定します。重要なビジネスサービスの影響許容度を設定します。影響許容度は、従来から使われている復旧目標時間（RTO）を拡張する概念で、サービス中断の影響がステークホルダーにとって許容できない損害の水準に達する状態・時点を表します。

- **シナリオのテストと改善。**「極端だが現実的な」シナリオをテストし、現実的な復旧時間と確立された影響の許容範囲をよりよく理解しましょう。テストを行うことで、確立された許容範囲内に収めるために企業が技術やプロセスに投資すべき箇所がわかります。テストを通じて得られた発見事項は、レジリエンスを継続的に向上させるために考慮し、行動する必要があります。

- **自己評価（セルフアセスメント）の実施。**主要なレジリエンスリスクを特定し（テーマ別、機能別、ドメイン別など）、業界標準や規制当局の期待に沿った結果を導き出すために、詳細かつ深く掘り下げた自己評価を設計しましょう。変化とレジリエンスの向上を実証するための測定メカニズムを構築します。

成熟した組織に対して市場が期待するのはレジリエンスであり、それはランサムウェアの攻撃を受けた場合も当てはまります。ランサムウェアにより、外部のステークホルダーや経済全体が被る損害の影響を最小限に抑える方法をしっかりと理解し、組織の脆弱性がどこにあるのかを知り、サイバーレジリエンスを向上させることが、攻撃への対応と回復を迅速に行い、顧客の被害を最小限に抑えることにつながります。

成熟した組織に対して市場が期待するのはレジリエンスであり、それはランサムウェアによる攻撃にも当てはまります。

経営陣からの質問

ランサムウェア攻撃のコストは増大しています。システムのダウンタイム、従業員の時間、評判低下の懸念など、ビジネスへの影響は、身代金の支払いによる金銭的コストとは比べ物になりません。ランサムウェアによる攻撃が継続し、より多くの企業が標的となる現在、経営者が発すべき厳しい質問には以下のようなものがあります。

- ランサムウェアの影響を防止または制限するために設計された、効果的なセキュリティ管理が行われているか。これらの対策はどのくらいの頻度でテストされているか。

- 重要なデータがどこにあるか把握しているか。オペレーショナル・レジリエンスを高めるためのプロセスやコンポーネントを導入しているか。

- ランサムウェアの影響を効果的に定量化できるか。

- ランサムウェアの発生に対して、24時間365日体制で防御と監視を行っているか。

- 特権アクセスアカウントを保護するための対策システムが施されているか。

- ランサムウェアを軽減するためのバックアップ戦略はどうなっているか。一貫したバックアップ体制をとっており、バックアップはオフサイトに保存されているか。

- ランサムウェア攻撃の標的となった場合のインシデント対応計画はどのようなものか。その計画は、組織内でどの程度広く共有されているか。

- インシデント対応能力はどのようなものか。

プロティビティの支援

プロティビティでは、急速に進展するサイバーセキュリティの潮流にお客様が対応できるよう、CISO、CIO、CAE（最高監査責任者）、CDO（最高データ責任者）の皆様をご支援しています。サイバーセキュリティとプライバシーの実践における強化されたランサムウェアへの対応は、悪意のある攻撃者によるビジネスへの脅威レベルを抑えます。機能が拡張され、より専門化されたランサムウェアアドバイザリおよびリカバリ製品は、壊滅的なランサムウェア攻撃の短期的な危機を管理し、ビジネスと長期的な回復力に役立ちます。

プロティビティのクロスソリューションチームは、クライアントがランサムウェアの復元力を強化することを支援しています。3つの主要なフェーズを介して、ビジネス全体でサイバーセキュリティに対する強化体制を拡大します。

1. 予測：積極的な防御により、脅威を予測、理解、および対抗します。

2. 対応：ランサムウェア攻撃が発生した場合の危機を管理し、ビジネスを止めないまま、経営層や、法務、技術の利害関係者を含めて対応します。

3. 回復：攻撃を受けた後、業務が確実に復元され、セキュリティシステムが強化され、組織の回復力が再構築されます。

取締役会や経営層にとって、オペレーショナル・レジリエンスは、継続した最優先事項であるため、強力な危機管理計画と最新のデータ保護は、日常業務の維持や、復旧の効率性を改善し、より安全な組織になるために重要です。

protiviti®