ハンドアウト

opentext™

ランサムウェアに対する防御を強化する 2 つのステップ

ランサムウェアが猛烈な勢いで世界中に広がっています。CyRiM (Cyber Risk Management) の 2019 年のレポートによると、ランサムウェアによる経済的な被害は 1,930 億米ドルにも上っている可能性があります。

FBI の推定によると、ランサムウェアは全世界で 1 日あたり 10 万台以上のコンピューターに感染しています。EUROPOL (欧州刑事警察機構) が 2018 年に発表したインターネット上での組織犯罪の脅威に関する評価によれば、「ランサムウェアは、捜査機関と業界両方の報告において、主要なマルウェア脅威であり続けています。」2017 年に世界中に被害を広げ、推定で 50 億米ドルを超える損害を与えた WannaCry ワームを覚えているでしょうか[1]。実は WannaCry ワームの脅威は続いていて、「WannaCry による感染はアジア太平洋地域で現在も拡大しています。」[2]

企業は 2 ステップのアプローチで、ランサムウェアの脅威を容易に無効化することができます。まず、侵入に対する保護を強化します。そしてウィルスが侵入してしまった場合は、システムを正常な運用へと復元するために用意されている最新のデータコピーを使用して問題を迅速に解決します。

変化し続けるランサムウェアの状況

ランサムウェアはその登場以来、攻撃の様態を進化させ続けており、ますます巧妙で手の込んだ手法により、さまざまな IT システムの脆弱性を標的としています。それはなぜかと言えば、ランサムウェアがサイバー犯罪者に大きな経済的利益をもたらすからです。ZDNet のレポートによると、「SamSam ランサムウェアを仕掛けたサイバー犯罪者集団は、2015 年後半にこのファイルをロックするマルウェアをばらまき始めて以降、600 万米ドルにも及ぶ利益を上げており、現在でも毎月 30 万米ドルもの利益を上げ続けています。」

実のところ、豊富なソフトウェア開発経験を持たないサイバー犯罪者でも攻撃を行うことができる RaaS (サービスとしてのランサムウェア) をダーク Web から簡単に入手できるようになっています。そのため、ランサムウェアの拡大がさらに進むと予想されています。さまざまな形での攻撃が激化しているため、企業はその対策に悪戦苦闘しています。

2017 年 5 月に攻撃を開始した WannaCry は、Windows の脆弱性を悪用するランサムウェアですが、Microsoft は 2017 年 3 月にはこの脆弱性に対応するセキュリティパッチ (MS17-010) をリリースしていました。セキュリティアップデートをしっかり行っていなかったシステムが被害を受けたのです。SynAck は、プロセスドッペルギャンギングと呼ばれる、正規のプロセスに成りすまして侵入し攻撃を隠ぺいする手法を使用して、マルウェア検出を回避します。

この 2 つ以外にも、ランサムウェアに対する包括的な防御のアプローチが必要であることを示す事例には枚挙にいとまがありません。

ランサムウェアはその登場以来、攻撃の様態を進化させ続けており、ますます巧妙で手の込んだ手法により、さまざまな IT システムの脆弱性を標的としています。それはなぜかと言えば、ランサムウェアがサイバー犯罪者に大きな経済的利益をもたらすからです。

巧妙さを増すランサムウェアを無効化するための 2 つのステップ

1. 継続的なデータ保護

ランサムウェアの被害に遭い、身代金を要求された場合、要求された金額を支払ったとしてもデータが元に戻らない危険性があります。FBI によるインターネット犯罪に関するレポート[3]にはこのように書かれています。「FBI では攻撃者に金銭を支払うことを推奨しません。要求どおりに金銭を支払ったとしても、データが元に戻る保証はありません。実際、金銭を支払った後も復号化キーを提供されなかった個人や組織の事例が存在します」

では、企業としてはどのような対策が必要でしょうか。IDC は『**Ransomware Defences Require Backup and a Comprehensive Security Strategy**』という文書の中で次のように述べています。「調査によると、数秒前あるいは数分前など、任意の時点から情報を復元できるようデータを追跡し、ディスクに保存する継続的データ保護製品を含む包括的な防御戦略が用意されていない事例が一貫して見られます」

ランサムウェアの手の届かない安全な場所に最新のデータコピーが保存されていれば、ランサムウェアの要求に対して簡単にノーを突き付けることができます。同様に、データを簡単に復元して生産性への影響や業務の中断を最小限に抑えられることも重要なポイントになります。そのためには、以下のような効果的なソリューションが必要です。

- 重要なビジネスデータをポリシーベースでバックアップでき、適切な RPO と RTO を実現できる
- 必要とするリカバリのパフォーマンスを実現できるよう、プライマリストレージと緊密に統合できる

1 **CISCO 年次サイバーセキュリティレポート**
2 **記事：アジア太平洋地域の企業における 2018 年のマルウェア検出件数は 270% 上昇：エンタープライズ**
3 **2017 年のインターネット犯罪レポート**

- 1 時間単位でスナップショット作成を実行するスナップショットのスケジュール管理により、ランサムウェア攻撃が発生した場合のデータ損失を最小限に抑えることができる
- 高度な重複排除機能により、ネットワークの帯域幅およびストレージ領域を効率的に利用できる
- データの送信時および保管時の両方でセキュリティを確保できる
- 異機種のハードウェアにも復元可能で、システム情報とデータの両方を復元できるベアメタルリカバリ機能を備えている

30 年以上の実績を誇るデータ保護ソリューション、OpenText™ Data Protector を無料で安全にお試しいただけます。こちらからご登録ください。

2. 真の意味でのバックアップソリューション

IT チームは、企業の資産を保護するという非常に大切な責任を担っています。そもそもユーザーが感染しないよう防御することが、ランサムウェアやその他のサイバー攻撃に対する唯一かつ真の解決策となります。しかし、防御しなければならない範囲は非常に広く、対策も複雑なため、適切なツールと自動化の仕組みを取り入れることが欠かせません。

そのためには、IT チームが現在のランサムウェア攻撃に対抗できるのみならず、今後登場する IT ビジネスを狙ったさまざまなサイバー攻撃に対しても防御できる機能を備えた効果的なソリューションが必要です。侵入、感染、被害拡大などのあらゆる段階において、重要な企業資産を保護できる総合的な機能を備えている必要があります。このようなソリューションでは、以下のような機能が求められます。

3-2-1 バックアップルール

よく知られているバックアップ戦略として、3-2-1 ルールがあります。「3」とは、データのコピーを 3 つ以上保持することを意味します (オリジナルのデータと 2 つ以上のバックアップ)。「2」とは、バックアップデータをディスク、テープ、クラウドなど、2 種類以上のストレージに保管することを意味します。最後の「1」とは、データ保護や障害復旧の効果を最大限に高めるため、少なくとも 1 つのバックアップコピーをオフサイトで保管することを意味します。オフサイトでのバックアップは多くの場合、長期的な保管目的で使用されます。コンプライアンス上の理由から、さまざまなテクノロジーを使用してデータを保管することが求められる場合もありますが、このルールを使えばそのような要件にも対応することができます。

Data Protector は、拡張性の非常に優れたエンタープライズグレードのバックアップおよびリカバリソフトウェアソリューションで、オンサイトまたはオフサイトのディスク、テープ、クラウドなど、複数のバックアップ先にデータをバックアップすることができます。Data Protector を使用すると、特別なバックアップの仕組みを別途構築する必要はなく、既存のファイルシステムやイメージのバックアップの追加コピーを作成できます。企業のニーズに応じて、さまざまな場所のさまざまなメディアに、さまざまなデータセットを対象とした追加のコピーを作成できます。

一元管理が可能なため、レポートやステータスダッシュボードを通してデータのバックアップステータスを瞬時に把握できます。

各データの RPO および RTO ポリシー

Data Protector は、Oracle、SQL、Microsoft Exchange、SharePoint、SAP、SAP HANA などのミッションクリティカルなアプリケーションに対して最高レベルの包括的な保護機能を提供します。企業全体のバックアップに対応しており、データ損失やシステムの中断が発生した場合でも迅速なリカバリでビジネス継続性を確保します。

ミッションクリティカルなアプリケーションごとに、ダウンタイムを短縮するためのリカバリポイント目標 (RPO) とリカバリ時間目標 (RTO) を個別に設けなければならないことがあります。重要性の低いアプリケーションを低めのサービスレベル期待値に応じて階層化できるため、戦略的な障害復旧を実現することが可能です。

アプリケーションとの統合により、個別のファイル、ディレクトリ、またはファイルシステムレベルのきめ細かなリカバリが可能なため、迅速にリカバリを進めてビジネスの中断を最小限に抑えることができます。クラッシュ整合性リカバリに頼ることなく、Data Protector のアプリケーション整合性リカバリを活用することによって、データの破損やリカバリ後の不整合を回避できます。

また、このソリューションではアプリケーションに対応した形でスナップショット作成を行うため、Windows、Linux、HPE-UX を含む OS でスナップショット管理を自動化できます。

George Crump 氏 が『**How to Ensure Your Backups Protect You From Ransomware**』の記事で述べているように、ランサムウェア攻撃からのリカバリにおいて最も重要な点はバックアップです。そのため、IT チームはバックアップシステムの保護に特に注意を払う必要があります。ランサムウェア攻撃によって悪用されうる脆弱性がバックアップソフトウェアに存在するということだけでも、新しいバックアップベンダーに乗り換える十分な理由となりえます。バックアップソフトウェア自体に十分な保護機能が備わっており、確実にマルウェアに感染しないことが重要です。

ランサムウェア攻撃は目まぐるしくその形を変え続け、そして重大な被害をもたらします。そのため、マルウェアに対する包括的な保護を行うアプローチが不可欠です。継続的なデータ保護と高度なリカバリオプションを手にできれば、この戦いを確実に勝利へと導くことができます。

実績のあるデータ保護ソリューション、Data Protector を無料で安全にお試しいただけます。こちらからご登録ください。

お問い合わせ

詳細

Data Protector を無料でお試しになれます。こちらをご覧ください。

www.opentext.com

opentext™