MSP 業者はランサムウェア攻撃に対しもっと深刻に対処すべき
2021 年 12 月 1 日 Minerva のブログから

MSP(マネージドサービスプロバイダ)にとってランサムウェア攻撃の危機意識が対岸の火事レベルであったのかも知れません。なぜならランサムウェア攻撃に対しては、MSP は常に自分たちのインフラセキュリティに対して過剰な自負を持っているのと、まさかうちが攻撃に会うはずはないと甘い意識を持っていたからです。それにもかかわらず、MSP をターゲットに攻撃者は慈悲もなく襲い掛かりました。彼らのメインシステムへ侵入し、認証情報などを盗み取り最終的にクライアントサイドのネットワークへも脅威の手が伸びてしまったのです。そのケースがまさに今年の初めに起きた Kaseya インシデントでした。まず MSP 側のソフトウェアプラットフォームへ侵入、さらに支障なくクライアントの特権アクセス情報まで不正に取得されてしまったのです。

当然、攻撃者にとっては、まさに宝の山を探し当てたことに等しく、今後も MSP への攻撃はエスカレーションするでしょう。ランサムウェア攻撃に対して真摯にそして現実的な対策をする必要があるようです。

攻撃者は MSP をターゲットにシノギを削る
なぜ MSP が格好の標的に絞られるか想像してみてください。MSP はインフラにおいてサイバー攻撃対策を行い各企業組織(クライアントサイド)へ SaaS サービスを展開しています。つまりサービス開始後も保守サービスを提供しセキュリティーも担保しています。このシステム設

計に対し、攻撃者は侵入の努力を重ねてきました。MSP 側のネットワークへ侵入に成功すれば、さらにクライアントの情報も不正取得可能になるからです。個別単体の企業組織ネットワークを狙うよりMSPを狙った方が一石二鳥となります。

さらにグローバル規模のコロナ蔓延により、多くの企業組織がリモートワーク展開へ急激にシフトし、MSPのニーズに比例する傾向にあると思います。

MSP のランサムウェア攻撃防御

このような状況の中で MSP サービスのセキュリティレーンについて再対策の必然性が起こり、いくつものハードルを打破しないとならない状況になりました。つまり MSP システム側の脆弱性イコールクライアントへのリスクに晒しだされる縮図が浮上したのです。新たなセキュリティー構想で防御策を考える必要性が出てきました。

以下の項目を見直す課題になると思います。

MSP ツールを再度見直す

MSP はセキュリティーに脆弱性のあるツールについては注意を払う必要があります。
MSP 運営者にとって Kaseya 社のサプライチェーン攻撃のようなインシデントについて知らない人は少しセキュリティー意識が低いといえます。一方、特定の IT 技術者が特定のツール（リモートソフトウェア又は監視ツール）を使用することで、マルウェア感染になる可能性は低いですが、セキュリティーに脆弱性のある IT ツールを使用するケースでセキュリティーホールになる場合もあるので注意が必要です。

使用していないユーザーアカウントを無効

MSP が提供するサービスでは個人アカウントが作成された後、ユーザーが退社しているケースもあり、結果として使用されていない個人アカウントが多く存在するケースが絶えません。
この状態はセキュリティーを考慮する上で良好な状態ではなく、不使用なアカウントを削除又は無効にするなどして整理するようにしましょう。

ネットワークアクセスを制限

ゼロトラストネットワークと厳格なアクセス権限は管理する観点からは少し不便さを感じますが、これはセキュリティーリスクを抑える上でとても重要です。MSP 業者は、いくつもの企業組織をクライアントへサービスを提供しているので全ネットワークは特に一つにつながります。
MSP が各クライアントのネットワークへアクセスする場合などを想定すると特にアクセス制限においては注意を払うべきです。また新規エンドポイントが新規アカウントでアクセスするためには、確実に安全かどうかを実証し、いくつかのセキュリティプロトコールがクリアにならない

場合はアクセスを拒否すべきです。

エアーギャップバックアップ

バックアップ。それは MSP としては重要事項です。例えばランサムウェア攻撃があった場合はファイルが暗号化されてしまいますからバックアップは必須になってきます。しかしそのバックアップデータが他のシステム又はデバイス上に保管されていたとしたらどうでしょう？これらの管理方法はとてもリスクな状況です。なぜなら攻撃者はあなたのメインネットワーク上から侵入したマルウェアは必ず横展開し、バックアップデータの場所を突き止めるからです。

このリスクを抑える方法としてエアーギャップでバックアップすることです。エアーギャップとはオフライン上でデータを保管するということです。オフライン上ですとインターネット経由でアクセスできない状態であるためセキュリティーリスクが低くなります。もしエアーギャップでデータをバックアップすることが困難な場合、クライアントサイドのネットワークから切り離して保管することが賢明です。

検知回避型ランサムウェアを先制防御するために Minerva Armor を導入

MSP にとってランサムウェア攻撃を検知することは難しくはないでしょう。例えばブルートフォース攻撃でパスワードなどを盗み取る行動は未知のホーストによるポートスキャンニングを簡単に検知しアラートを出すことができます。

しかし最近のマルウェアは EPP や EDR 製品の検知を回避するランサムウェアが数多く登場しています。このような状況を打破するために MSP は Minerva Labs 社の Minerva Armor（製品名）を導入することを推奨します。このソリューションは検知を回避する行動ロジックをカウンター攻撃で先制防御を行います。よってマルウェアが攻撃を実行する前にシャットアウトしますので感染を完全に防ぐことが可能です。

まとめ

昨今、コロナ蔓延により多くの企業組織は在宅ワークにより MSP のサービスへ依存する機会が増えてきたことで、MSP を狙うランサムウェアが急増しております。MSP はランサムウェア対策で現在採用している IT ツールやセキュリティポリシーなどを改めて見つめ直しサプライチェーン攻撃を防がなくてはならないでしょう。

Minerva 製品（Minerva Armor）についてのお問い合わせは Pico Technologies（info@pico-t.co.jp）までお願い致します。