ランサムウェア攻撃を阻止して戦うための最終チェックリスト

「2016 年はランサムウェアの年になる」。業界シンク タンクである Institute for Critical Infrastructure Technology はその最新の報告書でこう告げています。ランサムウェアとの戦いでは、防御を固めることこそが最善の攻撃になります。攻撃を回避するための準備はできていますか。防御戦略を考えているだけで時間を浪費しないでください。代わりにこのチェックリストを使用して、高度な攻撃からビジネスを保護してください。

□ 1. すべてのデータをバックアップする

ランサムウェアを阻止するための最も強力な武器は定期的なバックアップです。攻撃が発生した場合は、ネットワーク上の他のシステムにランサムウェアが広がるのを防ぐために、まずはエンドポイントの電源を切り、次にエンドポイントのイメージを再適用して最新のバックアップを再インストールしてください。

ランサムウェアを駆除するには、システムを完全に入れ替える必要があります。そのため、攻撃から迅速に回復するには、システム状態のバックアップまたはスナップショットが不可欠です。バックアップを頻繁に行うほど、失われるデータが少なくて済みます。バックアップの頻度は、データの戦略的重要性と組織が許容できるデータ損失量に基づいて決定する必要があります。接続デバイスはすべて暗号化されるため、ストレージはネットワークの外部に配置し、バックアップ完了後はデバイスとのマッピングまたは接続を解除する必要があります。

□ 2. パッチを繰り返し適用する

ランサムウェア攻撃者は、多くの場合、既知の脆弱性がある古いソフトウェアを使用しているユーザに狙いを定め、それらの脆弱性を悪用してネットワークにひっそりと侵入します。一貫性のないパッチ適用や古いソフトウェアを使用することで組織を危険にさらします。ソフトウェアを定期的に更新することを習慣にしてください。Java や Flash など頻繁に悪用されるサードパーティ ソフトウェアにパッチを適用すれば、間違いなく多くの攻撃を防ぐことができます。

□ 3. 攻撃元に関する情報をユーザに伝える

セキュリティ チェーンの一番の弱点は一般に人です。従業員は、フィッシング メールやその他のソーシャル エンジニアリング スキームに引っかかり組織を危険にさらすことがあります。ソーシャル エンジニアリングに関する脅威の手口をユーザに説明してください。犯罪者がこの手口を使用するのは、他人を信頼したいという人々の自然な性向につけこむほうが、ソフトウェアをハッキングする方法を見つけるよりも簡単だからです。

結局のところ、セキュリティは誰が、そして何が信頼できるかを知ることにかかっています。電子メールを読むときには、次の質問を自分自身に問いかけるようユーザを教育してください。

1. 送信者を知っているか。
2. そのファイルを開くか、リンク先に移動する必要が本当にあるか。
3. この会社から本当に何かを注文したのか。

☐ 4. ネットワークを保護する

階層型アプローチを導入してネットワークを継続的に保護してください。これには、次世代ファイアウォール（NGFW）や侵入防御システム（IPS）などのテクノロジーを使用します。階層化された防御では、ネットワーク内の複数の領域で複数のアプローチに基づくセキュリティ対策を適用できます。単一障害点を排除することで、ネットワークとデータを効果的に保護できます。

☐ 5. ネットワーク アクセスをセグメント化する

ネットワークをセグメント化することで、攻撃者がアクセスできるリソースの量を制限できます。ネットワーク アセット、リソース、アプリケーションを論理的にグループ化し、区画化された領域に配置します。常に動的にアクセスを制御することにより、ネットワーク全体が 1 回の攻撃で侵害されるのを回避できます。

企業ネットワークの大半は「フラット」であり、部門間、ユーザとデータ間、部門固有のデータ間ではほとんどまたはまったくセグメント化されていません。セグメント化は、マルウェアの水平展開を阻止または鈍化させるためにも、脅威の封じ込めにも活用できます。

☐ 6. ネットワーク アクティビティを注意深く監視する

見えないものを守ることはできません。ネットワークを詳細に可視化することは困難な作業に思えるかもしれませんが、絶対に必要なことです。ネットワークとデータセンターで起こっていることすべてを可視化できれば、境界をバイパスして内部環境に侵入する攻撃を検出できます。

いわゆる緩衝地帯（DMZ）を導入して強化することで、境界を保護してください。DMZ とは、組織の外部向けサービスを格納し、インターネットなど一般には大規模で信頼できないネットワークに公開する物理的または論理的サブネットワークのことです。DMZ により、ローカル エリア ネットワーク（LAN）のセキュリティ レイヤが 1 つ追加されます。外部のネットワーク ノードが直接アクセスできるのは DMZ 内のサーバだけで、内部ネットワークのその他の部分にはアクセスできません。

☐ 7. 最初の侵入を防止する

ユーザは何も考えずに感染サイトにアクセスしたり、マルバタイジングを含む電子メールを開いたりして、組織のネットワークをマルウェアにさらしてしまうことがあります。一般に、ランサムウェアの最初の感染は、電子メールの添付ファイルを開くか、悪意のあるソフトウェアをダウンロードすることによって発生します。ランサムウェア対策の一環として、悪意のある Web サイトや攻撃者が送信した電子メールと添付ファイルを念入りにブロックすることで、ネットワークを継続的に保護できます。

組織内のユーザやパートナー企業がファイルを交換するための会社公認ファイル共有プログラムへの投資を検討します。ファイル共有ソリューションを導入し、電子メールを介したファイルの共有や受け取りを一切行わないようにユーザに指導することで、添付ファイルを使用したフィッシング攻撃のリスクはほぼ完全に解消できます。

□ 8. エンドポイントを武装する

エンドポイントにウイルス対策ソリューションを導入するだけでは、ランサムウェアに対する十分な防御にはなりません。個人所有デバイスの持ち込み（BYOD）を許可する職場がますます増えているため、ネットワークに接続するラップトップ、モバイル デバイス、およびタブレットを管理するソリューションを見つける必要があります。このソリューションでは次の 2 つのことを行う必要があります。1 つはネットワークに接続しているものを可視化すること、もう 1 つはユーザが感染した Web サイトにアクセスしたり、疑わしいファイルをダウンロードしたりするのを防止するポリシーを適用できるようにすることです。

「最小権限」の概念を実践することを検討してください。つまり、どのアカウントにも該当するタスクを実行するのに必要な権限のみを付与する必要があります。この概念は一般に、エンドポイントのユーザ権限とネットワーク共有のユーザ権限に適用できます（適用できない場合もしばしばあります）。この概念の鍵となるのは、悪意のあるソフトウェアは、ほとんどの場合、現在ログインしているユーザの権限レベルを使用するということです。そのユーザが管理者である場合は、攻撃者も管理者になります。常に 2 要素認証を使用してください。ハッカーはパスワードを盗むことがありますが、パスワードとスマートフォンまたはトークンを同時に盗むことはほぼ不可能です。

□ 9. リアルタイムの脅威インテリジェンスを得る

脅威にプロアクティブに対抗するには、攻撃者を知ることが重要です。脅威インテリジェンスは、組織が属する地域や業種、さらには特定の企業を標的にしたサイバー犯罪に関する警告を事前にセキュリティ担当者に提供します。これにより、必要な対策を講じるための時間が得られます。では、リアルタイムの脅威インテリジェンスを得るにはどうすればよいのでしょうか。世の中の動向に耳を傾け、Talos などの脅威インテリジェンス組織から学ぶことです。

Talos チームは、既知の、または新しいサイバーセキュリティ脅威からの保護に取り組んでいる 250 人以上のフルタイムの脅威研究者で構成されています。Talos チームはブログの投稿やニュースレター、ソーシャル メディア、コミュニティ フォーラム、セキュリティ情報、教育ビデオなどを通じて、すべての人がインターネットをより安全に利用できるように、情報を発信しています。身近で脅威が発生したときには、これらの情報に忠実に従って組織を変更することで、Talos チームの情報を有効に活用できます。

□ 10. 身代金要求に応じない

多くの企業はシステムの制御を取り戻すために身代金を支払おうとしますが、これは最後の手段と考えるべきです。代わりにしかるべき機関に連絡してください。身代金の支払いは、このようなサイバー犯罪に資金を提供することになるので、できる限り控えてください。

関連情報

ネットワークの可視性とシスコのランサムウェア対策の詳細については、http://www.cisco.com/jp/go/ransomware を参照してください。