新型コロナウイルス蔓延時代のサイバーセキュリティ：リモートワークへの移行と保護に向けた重要事項

11 March 2020 | Michael Sentonas（CrowdStrike）

新型コロナウイルス（COVID-19）が世界的なパンデミックであることを世界保健機関（WHO）が宣言したことから、このウイルスがもたらす病が、前例のないレベルの社会的･経済的混乱を引き起こすことになるということを私たち皆が理解し始めています。私たちのお客様からは、従業員の就業の場をオフィスから在宅ワーク、テレワークに切り替えるという会社の命令を速やかに実行に移す方法を模索するなかで、想定外かつ深刻な問題に直面しているという話を伺っています。全世界的なオフィスからの大移動に際して、セキュリティの維持が求められるなかで、ほとんどの組織が重大なリスクを背負うことになるでしょう。

リモートワークモデルの早急な採用にあたっての課題

最新の International Workplace Group のレポートによると、世界的には従業員の 50%が少なくとも週に 2.5 日は本拠とするオフィスを離れて働いています。しかしながら、新型コロナの影響で、もっと多くの（おそらくはすべての）組織がすぐにリモートワークを受け入れなければならなくなる可能性が出てきました。このオフィスからの脱出劇が IT チームやネットワークアーキテクチャー、機器のサプライヤーに与える影響のほかにも、組織が検討しなければならない決定的なサイバーセキュリティ上の問題が生じています。

リモートワーカーのサイバーセキュリティを確保するために役立つ 6 つの重要な要素：

- **現在のサイバーセキュリティポリシーにリモートワークに関するポリシーが盛り込まれていること。**強力なセキュリティポリシーが既に存在しているかもしれません。しかし、そのポリシーがオフィスだけではなく自宅で作業する従業員が増えた場合にも適切であるかを再確認することが重要です。セキュリティポリシーには、リモートワーカーのアクセス管理、個人用デバイスの使用、およびドキュメントやその他の情報への従業員からのアクセスに対するデータのプライバシー保護についての注意事項を含める必要があります。また、シャドー IT やクラウドテクノロジーの利用が増加することについても考慮する必要があります。

- **企業に接続する BYOD デバイスに対する計画を策定すること。**在宅勤務、テレワークの従業員が個人用デバイスを使用して業務を行う可能性もあります。特にサプライチェーンの停滞により、企業がデバイスを提供できなくなると、BYOD デバイスの割合も高まるでしょう。個人用デバイスにも、企業所有のデバイスと同レベルのセキュリティが必要です。また、ビジネスネットワークに接続する従業員所有のデバイスのプライバシーについても考慮しなければなりません。

- **安全でない Wi-Fi ネットワークを介した機密データへのアクセスに備えること。**在宅勤務、テレワークの従業員が、オフィスのファイアウォールのようなセキュリティ制御がない自宅の Wi-Fi ネットワークを介して企業の機密データにアクセスする可能性があります。リモートからの接続が増えるとともに、データ保護により一層注力する必要が出てくる、そして増大するエントリーポイントからの侵入にも対応しなければなりません。

- **サイバーウイルスに対する予防策と可視性。**個人用デバイスのサイバーセキュリティレベルが劣っていることは珍しくありません。従業員が在宅勤務、テレワークになると、企業はリモートのデバイスに対する可視性を失い、それらの設定がどうなっているか、パッチは適用されているか、あるいは、セキュリティ保護が行われているかすら把握できなくなるでしょう。

- **コロナウイルスに便乗した詐欺の増加に備える継続的な従業員教育。**WHO および米国連邦取引委員会（FTC）は、**コロナウイルスに便乗したフィッシング攻撃や詐欺が発生**していることをすでに警告しています。エンドユーザーの継続的な教育およびコミュニケーションを行い、リモートワーカーが迅速に IT 部門に連絡してアドバイスを受けることができる環境を確保する必要があります。また、より厳格な E メールセキュリティ対策についても検討しなければなりません

- **危機管理およびインシデント対応計画をリモート環境の従業員も実行できること。**異常な状況下において発生したサイバーインシデントは、制御不能となる可能性が大いにあります。会議専用ツールやメッセージングプラットフォーム、生産性向上のためのアプリケーションといった効果的なリモートコラボレーションツールを使用すれば、分散されたチームを「バーチャルの作戦指令室」としてまとめ上げ、そこから対応措置を講じることができます。侵害されたマシンの復旧または交換などの特定のタスクを、物理的なアクセスや遠方から出張してくる技術者に依存して行っている場合には、代わりとなる方法や、ローカルのリソースを探しておくべきでしょう。

リモートワーカー全員のセキュリティを確保

CrowdStrike は、在宅勤務、テレワークへの突然の移行に取り組む企業に対し、独自の支援を提供できる立場にあります。その理由のひとつは、当社のクラウドベースのプラットフォームと軽量のエージェントアーキテクチャーが、リモートワーカーのサポートと保護に最適であること。もうひとつは、当社が「自分の犬の餌を自分で食べている」―つまり、我々自身が自社製品を使用して、その有用性を証明している企業であるということです。CrowdStrike には、広く分散している当社の従業員を安全かつ効果的にサポートするための深い知識があるのです。

従業員をオフィスから各自宅へとシフトするにあたり、迅速な移行とセキュリティの確保に役立てていただけるクラウドネイティブの CrowdStrike Falcon® の利点をいくつか紹介いたします。

クラウドならではの拡張性と費用対効果を享受できる。顧客の要求に柔軟に対応すべく、クラウド向けに一から構築されたアーキテクチャーは、従業員がどこから接続していてもリアルタイムの保護を実現するための膨大なストレージと処理能力を提供します。クラウ追加のリソースを必要に応じてプロビジョニングすることができます。もちろんリモートの従業員のサポートを展開する際には、ハードウェアやソフトウェアの計画、準備、クラウドリソースの追加プロビジョニングが不要です。

従業員がどこにいても最高レベルのセキュリティを確保する。100%クラウドベースで提供されるセキュリティアーキテクチャーにより、組織のファイアウォール外を含むあらゆる場所のワークロードを保護し、最高レベルのリアルタイムセキュリティ機能と、コンプライアンス対応情報を提供します。たとえオフラインであっても、ローカルを保護します。またすべてのデバイスにおいて**脅威ハンティング**を行うことが重要です。特に組織のネットワーク外のデバイスには注意が必要ですが、どこからでも即座にログ情報にアクセスできる環境であれば、それは簡単に行えます。ただし、それを実現できるのは、ネイティブのクラウドベースのソリューションだけです。

包括的な可視性を提供するシンプルなセキュリティアーキテクチャーを活用。ネットワーク上に誰のどのようなデバイスが存在しているかを把握することが、プロアクティブなセキュリティ管理の基本です。デバイスがどこからアクセスしようとも、ネットワークに接続しているすべてのデバイスの完全な可視性を得ることが不可欠です。CrowdStrike® Falcon の単一の軽量エージェントは、インストール時の再起動が不要です。エンドポイントのパフォーマンスへの影響を最小限に抑え、エンドユーザーのエクスペリエンスに影響を及ぼす「スキャンストーム」や大量のシグネチャーアップデートを生じさせることなく、ユーザーを瞬時に保護します。Falcon プラットフォームの継続的かつ包括的なワークロード監視および脅威検知機能により、セキュリティチームはすべてのデバイスを完全に可視化して把握できます。その対象には、オンプレミスのデバイス、リモートオフィスや自宅内のデバイスおよびクラウド上のワークロードが含まれます。コンテナ環境やモバイルデバイスの保護状態も可視化できます。

サービスとして提供されるエンドポイント保護を利用して、不安のないセキュリティを確保できる。CrowdStrike Falcon Complete™ を利用すれば、エンドポイントセキュリティの実装、管理、**インシデント対応**を CrowdStrike の実績のあるセキュリティ・エキスパート・チームに任せることができます。その結果、包括的なエンドポイントセキュリティを管理するための手間、オーバーヘッド、コストを費やすことなく、セキュリティ体制を即時に最適化できるようになるため、社内のリソースをほかのプロジェクトに集中させることができます。100%手を煩わす事なく安心できるエンドポイント保護ソリューションである **Falcon Complete** は、利用開始時から構成から保守、監視、インシデント対応、修復に至るまで、エンドポイントセキュリティのあらゆる側面に必要な人材、プロセス、テクノロジーを独自の方法で提供し、オンプレミスのワークロードもリモートの従業員も一様に保護できます。

まとめ

新型コロナがもたらす危機は、しばらく続くと思われます。企業とその従業員は、難しい決断を迅速に下すことを強いられるでしょう。リモートワークへの移行もそのような決断のひとつです。これを迅速に実行するにはリスクが伴います。しかし、御社のネットワークやデバイス、データをリスクに晒すわけにはいきません。

既存のお客様には、リモートワーカー急増への対応への特別プログラムを用意しておりますので、CrowdStrike の担当者にお問い合わせください。

そして全ての皆様に対して CrowdStrike は、果断な対応の妨げとなるものを排除し、あらゆる場所のすべてのユーザーが、安全なオペレーションに必要なテクノロジーと専門知識を活用できるように尽力しています。

追加のリソース

- CrowdStrike Falcon プラットフォームの詳細についてご紹介しています。
- Web キャスト『新型コロナウイルス蔓延時代のサイバーセキュリティ：リモートワークへの移行と保護に向けた重要事項 (英語)』はこちらからご覧いただけます。
- マネージド・エンドポイント保護の詳細については、Falcon Complete の Web ページをご覧ください。
- CrowdStrike Falcon Prevent™ の無料トライアルで、真の次世代型アンチウイルスが、今日の非常に高度な脅威にどのように対抗できるかを体験ください。