ホワイトペーパー

在宅ワーカーのセキュリティ保護に向けた7つの戦略

macOS

ウイルスの感染拡大によって多数の従業員が在宅ワークを余儀なくされる今、在宅ワーカーのセキュリティ基盤作りは、業務の存続を左右します。

この世界的なパンデミックの中、大量の在宅ワーカーを安全にサポートする準備は整っているでしょうか？先行きが不透明な現状において、CDCなどの感染症の専門家は、企業に対して、事業継続/災害復旧計画の一貫としてソーシャルディスタンスの実践と隔離期間の延長に備えることを推奨しています。
その対策の1つがゼロトラストアーキテクチャなどのツールの活用です。これにより、従業員は社内のシステム、データ、生産性スイートに安全にアクセスし、ワークフローの中断を最小限に抑えることが可能になります。ゼロトラストとは、効果的なセキュリティ制御により、IT環境とインタラクションを行うすべてのユーザー、デバイス、アプリケーション、システムを統制する戦略を指します。

パンデミックなどの大規模災害の影響で従業員が在宅勤務へと移行する場合、在宅ワーカーがシームレスなワークフローを維持できるようにしなければなりません。その対応として、IT部門やサイバーセキュリティ部門はゼロトラスト戦略を採用し、重要度の高い業務を継続するコラボレーション/生産性ツールを安全な方法でサポートする必要があります。

ウイルスの感染拡大によって多数の従業員が在宅ワークを余儀なくされる今、在宅ワーカーのセキュリティ基盤作りは、業務の存続を左右します。本書では、自宅のみで仕事をする従業員のセキュリティ保護に最適なソリューションを検討する企業に向けて、重視すべきポイントの説明と提案を行います。

VPN の制限 ：

- ライセンスコストが高い
- 導入コストが高い
- ネットワーク要件が増大
- 設定が複雑
- 速度と機能に制限がある
- 接続がダウンした場合のオフライン機能がない

VPNの速度制限を解消

現在提供されている従来型の在宅ワーク向けセキュリティソリューションは、VPN（仮想プライベートネットワーク）テクノロジーを採用しています。そのため、貧弱なパフォーマンスによって生産性が損なわれるだけでなく、組織のネットワークやワークフローを高度な脅威から効果的に保護できないばかりか、セキュリティ脆弱性の原因になるケースもあります。

パフォーマンスについて言えば、VPNを使用している企業や、在宅ワーカーのサポートにVPNを使用しようと考えている企業は、速度と機能性に制限がある点を理解する必要があります。VPNのパフォーマンスと速度は、インターネット接続を上回ることはありません。コンシューマーグレードのISPの場合、その速度は、企業ネットワーク環境よりも格段に低速になります。

また、セッション中のパケット暗号化/復号化機能もありません。したがって、VPNの設計仕様によっては、パフォーマンスがさらに低下する可能性があります。特に、サイズの大きなファイル、画像、ビデオコンテンツ、演算処理プロセスなどを含むワークフローでは、速度が大幅に低下してしまいます。

大企業の在宅ワーカーが業務に必要なファイルと生産性ソフトウェアにアクセスするには、ゼロトラストセキュリティ原則に沿った、より高速でセキュアな接続チャネルが必要です。ウイルス感染の拡大によってオフィスで勤務していた従業員が在宅ワークへと移行し、しかもこの状況が長期化すると考えれば、これは重要な鍵となります。

こういったニーズに応えるには、企業ネットワーク上に存在するあらゆるアプリケーション、デスクトップツール、ファイルに場所を問わずアクセスできるソリューションが必要です。また、従来のオフィス環境に匹敵するパフォーマンスを維持でき、従業員、契約社員、パートナーが私物デバイスからファイアウォールの背後にあるコンテンツにアクセスできる機能も必要です。

さらに、企業資産を1つの仮想デスクトップ環境へとセキュアかつ監査可能な方法で集約し、インターネットに接続できない状況でも、すべてのエンタープライズアプリ、ツール、ファイルにアクセス可能な機能も必要になります。そして、ユーザーのオンボーディング/オフボーディングを迅速に行い、エンドポイントプロビジョニングを容易に実行できるターンキーアクセスも求められます。

デバイスに依存しない機能は必須要件

ユーザーが業務ソリューションに求める機能はますます高度になっています。また、在宅ワーク向けのソリューションでは、セキュリティ機能はもちろんのこと、Microsoft® Word、Excel®、PowerPoint®などのワークプレースアプリケーションのほとんどをサポートし、時間や場所を問わないドキュメント共有機能も求められます。IT部門がソリューションを選定する場合には、Windows®、macOS®、Linux®をはじめとする一般的なオペレーティングシステムを搭載したデバイスから、場所や時間を問わずに仕事ができるソリューションを検討すべきです。

一般的なWebアプリケーションやレガシーアプリケーションを実行できるセキュアなブラウザ機能と、オフィスで使い慣れたイントラネットリソースにアクセスできる機能を実装していることが理想的です。また、ブラウザベースのソリューションであれば、電子メール、カレンダー、連絡先などにシームレスに接続できるだけでなく、IT部門が個々のデバイスや低パフォーマンスのVPNシステムを管理する必要もありません。

セキュアなブラウザベースのプラットフォームは、ゼロトラストアーキテクチャの一部であり、大量のデバイスを管理する手間を省くことができます。必要なのはセキュアなブラウザの管理のみなので、デバイスやオペレーティングシステム単位の管理は不要です。

生産性アプリには、次のようなコンポーネントへのアクセス機能が必要:

- 電子メール、カレンダー、連絡先
- ドキュメント
- Microsoft® Office 365® アプリ
- イントラネットサイト
- クラウドベースのビジネスアプリ(Salesforce、Workday®など)

大規模なモビリティの課題を予測

SaaSの時代、ドキュメント、スプレッドシート、スライドを作成するソフトウェアプラットフォームはいくつかありますが、エンタープライズ環境で求められる要件を満たしているものはありません。ほとんどの従業員がWord、Excel、PowerPointを使用しますから、在宅ワークでも同じ生産性を維持できるように、Microsoft® Officeへのシームレスなアクセスは必須です。

従業員の大部分が在宅ワークを余儀なくされる企業では、コラボレーション、ISV、カスタマイズツールなど、すべての中核的ビジネスアプリケーションをモバイルでも使用可能にするソリューションが求められます。ところが、IT部門、開発者、ビジネスオーナーには相反するモビリティニーズが存在し、「モバイルのみ」のイニシアティブを阻む大きな要因となっています。したがって、共通のアプリケーションプラットフォームを提供するソリューションを選定することで、個々のユーザーがほぼまたはまったく中断のない環境で業務を遂行できるようにし、モバイル対応プロセスを加速する必要があります。

緊急時の一斉通知とコラボレーション

- SMS、モバイルアプリ、セキュアな電子メールでアラートを迅速に受信
- 場所やグループごとに通知を送信
- 従業員の行動を把握 – 従業員のステータスの通知、感染拡大の防止措置、生産性低下の回避

オフィスでの業務に慣れている従業員が完全な在宅ワークへと移行する場合、企業は、モバイル対応とITアジリティを加速し、重要な業務機能の中断を回避しなければなりません。企業の中には、ワークフローをサポートするカスタムアプリケーションを短期間で開発するために、社内開発者が慣れ親しんだ開発ツールと手法を使用し、コードの効率的な再利用と社内セキュリティポリシーへの準拠に対応するケースもあります。優れた企業モビリティソリューションとは、多大なIT投資や長い調達サイクルを必要とせず、事業部のリーダーが幅広いアプリケーションを柔軟に採用または開発できるソリューションです。

モビリティへの急速なシフトが起こると、毎日新たに登場するビジネスニーズに対応するために、エンドポイントアプリケーションがネットワークへと次々に追加されます。その結果、IT部門は、絶えず変化する要件に対応できるサービスの提供に迫られるため、新たなアプリケーションとデバイスの統合にも迅速に対応できる拡張性を備えたソリューションが必要になります。それには、単一のプラットフォームで管理を簡素化するソリューションが理想的です。これにより、IT部門がデバイスを管理しない状況にあっても、企業と従業員間、企業とパートナー間、企業と顧客間、企業とサプライヤ間のニーズすべてにまとめて対応することができます。

インターネット接続状態に依存しない生産性

ウイルスの感染拡大に伴い、安全確保のために大勢の従業員がソーシャルディスタンスを実践するとなると、一時的にネットワーク接続できなくなる従業員も出てくるでしょう。したがって、堅牢性に優れたオフラインモードを備え、インターネット接続がない状態でも幅広い企業資産にアクセスできる在宅ワークプラットフォームを選定しなければなりません。

ドキュメント、スプレッドシート、PDF、プレゼンテーションをモバイルデバイスから安全な方法で作成でき、ワークフローの混乱を最小限に抑える機能を備えたソリューションが理想的です。ほとんどのオフィス生産性ツールは、インターネット接続を前提に最適化されています。したがって、オフライン時も在宅ワーカーが生産性ツールにアクセスできるようなオプション機能を導入しておく必要があります。

緊急時には、信頼性の高い方法で全社員に一斉通知

企業は、全社的なコミュニケーションを維持し、従業員の健康状態を確認する必要があります。したがって、一時的にインターネットに接続できなくなる可能性のあるモバイルワーカーも、大きな課題の1つです。このニーズを満たすには、緊急時のコラボレーションに特化したコミュニケーションツールを検討すべきです。緊急時通知システムは、緊急時に通常業務が中断された場合に必須の減災ツールです。従業員の安全をリアルタイムで確認することで、災害への効果的な対応や事業継続が可能になります。

対応チームや責任者による災害発生時の状況確認に役立ち、重要な事業部のステータスの可視化はもちろん、社内リソースや社外/サードパーティサービスを使った安全かつ効果的なコラボレーションを可能にします。あらゆる通信手段に対応し、全員にワンクリックでアラート通知できる機能を備えたソリューションが理想的です。これにより、緊急時対応の責任者は、信頼性の高い方法で全社員に速やかな一斉通知を行うことができます。

サイバーセキュリティのベストプラクティスを強化

在宅ワークを必須とする企業は、公衆インターネットを介してカフェや図書館で仕事をする場合のリスクなど、基本的なセキュリティベストプラクティスを従業員に再確認する必要があります。

業務で使用するすべてのデバイスのファームウェア、オペレーティングシステム、ソフトウェアを最新バージョンに更新するべきです。また、ディスク全体の暗号化ソフトウェアは、モバイルデバイスの紛失または盗難時に機密データへの不正アクセスを阻止できる点で、セキュリティ上のメリットがあります。

モバイルデバイス向けの最先端エンドポイントセキュリティオプションには、人工知能(AI)が搭載されています。
また、ファイルレス攻撃、ゼロデイ攻撃、外部デバイスを悪用した攻撃など、高度な脅威を回避する予測機能を備えています。

会社が支給するデバイスと私物デバイスのいずれにも、エンドポイント保護ソフトウェアをインストールする必要があります。モバイルデバイス向けの最先端エンドポイントセキュリティオプションには、人工知能(AI)が搭載されています。また、ファイルレス攻撃、ゼロデイ攻撃、外部デバイスを悪用した攻撃など、高度な脅威を回避する予測機能を備えています。さらに、スクリプト制御とメモリ保護のような機能、攻撃を自動で検知およびブロックする機能を備え、クラウドルックアップ、シグネチャ、ヒューリスティック、サンドボックスに頼らず、オフラインでもデバイスを保護できるソリューションが理想的です。

鍵はセキュリティと簡素化

危機的状況下で在宅ワーカーが簡単にアクセスできるパスが提供されていたとしても、認証とユーザーアクセスを保護する高レベルのセキュリティを備えたモビリティソリューションが必要です。ゼロトラスト原則に沿い、継続的な認証によって正当なユーザーのみに業務上のドキュメントやシステムへのアクセスを許可するプラットフォームの検討をお勧めします。

機械学習と予測的AIを搭載したゼロトラストソリューションは、ユーザーの場所、デバイスの操作、行動上の要素といった条件に応じて、セキュリティポリシーを動的に適応させることができます。これにより、効果的なセキュリティ制御だけでなく、人為的なミスやセキュリティ機能の意図的な迂回を阻止できます。また、継続認証により、中断が最小限に抑えられ、複数のデバイス/アプリケーションを不必要に再認証することもなくなるため、ユーザーエクスペリエンスが改善されます。

継続認証ソリューションでは、パッシブなバイオメトリクスなど、使用ベースのパターンが利用されます。ユーザー IDを継続的に検証できるだけでなく、不正アクセスを迅速かつ自動的にブロックすることが可能です。その結果、組織のセキュリティ態勢の強化とより良いエンドユーザーエクスペリエンスを両立できます。継続認証ソリューションは、学習を通じて、ユーザーやユーザーの行動に基づいたきめ細かなセキュリティ保護を行います。信頼できる場所にいるユーザーのセキュリティポリシーを緩め、リスクの高い場所にいるユーザーのポリシーを動的に調整します。

さらに、以上のプロセスをIT管理者が包括的に管理できる機能も必要です。ウイルスの感染拡大といった非常事態に伴って在宅ユーザーが急増する今、ユーザー、デバイス、アプリケーションのオンボーディング/オフボーディングを簡単に実行できるプラットフォームが求められています。

結論

在宅ワークはもはや、限られた状況で限られた従業員に提示される「オプション」ではありません。在宅ワークが「必須」要件であることを、ほとんどの企業のITリーダーが認識しています。

ゼロトラスト戦略は、効果的なセキュリティ制御により、組織のIT環境にアクセスするすべてのユーザー、デバイス、アプリケーション、システムを統制する上で不可欠です。在宅ワーカーがシームレスなワークフローを維持できる環境を整えるには、IT部門やサイバーセキュリティ部門はゼロトラスト戦略を採用し、重要度の高い業務を継続するコラボレーション/生産性ツールを安全な方法でサポートする必要があります。

新型コロナウイルス(COVID-19)の感染拡大を契機にモバイルユーザーが急増する今、モバイルユーザーをセキュリティ保護し、危機的状況でも事業を継続する方法として、ゼロトラスト戦略に基づいたリモートインフラストラクチャの必要性が注目されています。

詳細については
www.blackberry.comをご覧ください

BlackBerryについて

BlackBerry(NYSE:BB、TSX:BB)は、世界中の企業と政府機関にインテリジェントなセキュリティソフトウェアとサービスを提供しています。そのソリューションは、1億5,000台の車両を含め、5億を超えるエンドポイントをセキュリティ保護しています。カナダ・オンタリオ州ウォータールーに本拠を置くBlackBerryは、サイバーセキュリティ、安全、データプライバシーをはじめとする分野において、AIと機械学習を搭載した先進的ソリューションを提供しています。また、エンドポイントセキュリティ管理、暗号化、内蔵システムの分野をリードする企業でもあります。BlackBerryは、明確なビジョンに基づいて、信頼できる相互接続された未来を創造します。

BlackBerry. Intelligent Security. Everywhere.

詳しくは、BlackBerry.comを参照、または@BlackBerryをフォローしてください。