中規模ビジネスのための6つのセキュリティ・ヒント

中規模ビジネスにとって、ネットワークのセキュリティ侵害リスクを減らすことは重要です。以下の実証済みヒントで、会社とネットワークの安全を確保しましょう。

ヒント#1：ユーザーに適切なアクセス権を与える

ユーザーは常に移動しており、IoTデバイスはあらゆる場所で使用されているため、最適なロールベースのアクセス制御を行えるWi-Fiソフトウェアを使用する必要があります。使用するSSIDの数を最小限に抑えながら、ゲスト、プリンター、さらに職場に持ち込まれたApple TVでさえも、ユーザーやデバイスの種類ごとにアクセスを分けることができます。

ヒント#2：アプリケーション・フレンドリーなポリシーを構築する

場所、使用中のアプリケーション、トラフィックの種類に基づいて追加のセキュリティを適用します。自動化されたポリシー適用なら、それを簡単に行えます。場所や時間にかかわらず、ゲストのトラフィックが従業員のビジネスに不可欠なアプリケーションに悪影響を与えることを心配しなくて済みます。

ヒント#3：最新のWI-FIセキュリティ規格を使用する

WPA2 Wi-Fiセキュリティはもはや役に立ちません。ネットワークおよびクライアントをパスワード・フィッシング攻撃にさらす可能性のあるセキュリティ脆弱性がWPA2で最近発見されました。選択した無線機器がWPA3とOpportunistic Wireless Encryption（OWE）に基づくEnhanced Open対応認定済みであることを確認し、不必要なリスクから保護しましょう。

ヒント#4：侵入防御機能がビルトインされているWI-FIアクセス・ポイントを選択する

ネットワーク上に不明なアクセス・ポイントが見つかった場合、ITは夜通しの対応を迫られます。Wi-Fiアクセス・ポイントには、不正なAPや悪影響を及ぼすAP、あるいは脅威となり得る他のデバイスを見つけてシャットダウンするのに役立つ無線侵入保護の機能が搭載されている必要があります。最良なのは、望ましくない脅威についてネットワークがIT管理者にアラートを通知できる機能です。

ヒント#5：ビルトインのコンテンツ・フィルタリングでWEBアクセスを管理する

ユーザーが悪意のあるコンテンツにアクセスするのを防ぐことは難しく、安全性の低いインターネット・サイトの増加に対応し続けることはほぼ不可能です。ネットワークを安全に保つための適切な方法は、URL、場所、またはIPアドレスで簡単にフィルタリングして安全な閲覧を行えるようにできるWi-Fiソリューションを選択することです。

ヒント#6：セキュリティを最優先事項に据えるベンダーを選択する

強力なネットワーク・セキュリティは賢明な選択ですが、複数の場所から複数のデバイスに接続するユーザーの増加に対応するため、ユーザーとデバイスのレベルでの一元管理を追加することを検討する必要があります。外部のポリシー・サーバーは非常に役に立ちます。ビルトインのセキュリティ機能が、フルセットのAPIが基本的な要件を満たす高度なセキュリティ・ソリューションとシームレスに統合されていることを確認してください。

賢明なセキュリティ、賢明なネットワーク・アクセス

aruba
a Hewlett Packard Enterprise company

© Copyright 2019 Hewlett Packard Enterprise Development LP.本書の内容は、将来予告なしに変更されることがあります。Hewlett Packard Enterprise製品およびサービスに対する保証は、当該製品またはサービスに付帯する明示的保証条項でのみ規定されます。本規定のいかなる部分も、他の保証を構成すると解釈されるものではありません。Hewlett Packard Enterpriseは本書の技術上または編集上の誤謬、欠落についての責任は負わないものとします。

SixSecurityTipsMidsizeBusiness_080519