ユースケース

ゲスト Wi-Fi を保護する

エグゼクティブサマリー

デジタル技術による業界の変化に伴い、企業は進化を続けています。従業員のモビリティ（機動力）が高まることで、スピードと効率化が不可欠となり、動的なクラウドベースのインフラや接続が必要とされるだけでなく、場所や時間、デバイスに関係なく、安全かつ制限なくアプリケーションを利用できることが必要です。リーダーには進歩を続けるために障害を取り除くことが求められますが、新しい取り組みやプロセスをビジネスに取り入れることで、攻撃対象領域が広がり、企業が危険にさらされることにつながりかねません。

多くの企業では、このような課題に正面から応えるために、ゼロ・トラスト・セキュリティ・モデルを採用しています。ゼロ・トラスト・アーキテクチャは、ネットワーク上のすべてが敵対的であると仮定します。「内部対外部」という考え方や境界セキュリティの時代は過去のものとなり、「信ぜよ、されど確認せよ（信頼が前提だが確認は怠るな）」という合言葉も時代遅れとなりました。それらに代わって、組織では「決して信頼せず必ず確認せよ」という態度で臨み、アプリケーションやデータを配信する前にすべてのデバイスとユーザーの認証と承認を行い、ロギングや行動分析によってアプリケーションアクセスとネットワークアクティビティを監視することが必要です。

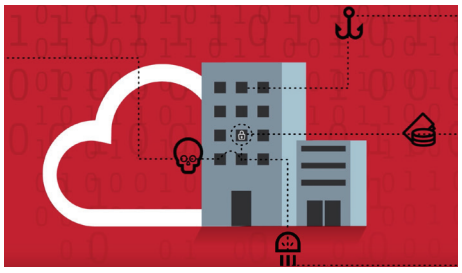
ゼロ・トラスト・セキュリティ戦略に関連する多くのユースケースの 1 つとしてあげられるのが、ゲスト Wi-Fi ネットワークを保護することです。

ゲスト Wi-Fi を保護する

ここ 10 年間で、「Wi-Fi は使えますか？」という質問は、Wi-Fi が使えるということを想定したうえでの「Wi-Fi のパスワードは何ですか？」という質問に取って代わられました。ただ単にインターネットに接続できるというだけでなく、高性能の Wi-Fi にさまざまなデバイスから（多くの場合は同時に）無料で接続できることは、ロケールに関係なく、ほぼ世界に共通して期待されることです。私たちは自宅、職場、電車内、空港、カフェ、お店、競技場、上空 1 万メートルの旅客機内でさえもネットワークに接続されています。

企業や組織にとって、このようなネットワーク接続をゲスト Wi-Fi ネットワーク経由で提供することには、ブランド認知の向上、客足の増加、優れた顧客体験など、多くの利点があります。ただし、このような差別化に課題は付きものです。自由にアクセスできて監視もされていない Wi-Fi ネットワークは、それを利用するお客様、訪問者、ボランティア、従業員にとって重大なリスクとなるからです。保護されていないままのゲスト Wi-Fi ネットワークは、サイバー脅威やデータ盗難だけでなく、大規模なブランドダメージの潜在的な温床となります。

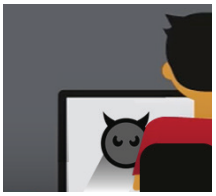
ユーザーが自分のデバイスを Wi-Fi ネットワークに接続するということにおいて、接続されたマシンの健全性やユーザーの意思の善意を、ネットワーク提供者は期待してはいけないということです。以前にウィルス感染したことのある、ノート PC、スマートフォン、ネットワーク接続されたウェラブルデバイス、タブレットによって、大量のマルウェアや高度な標的型脅威がネットワークに持ち込まれる可能性があります。ネットワークがノーチェックの場合、他のゲストユーザーとそのデバイスに感染が急速に広まってしまいます。そして、ゲスト Wi-Fi ネットワーク上のアクティビティのボリュームと種類を考えると、偶然であろうと意図的であろうと、悪意のあるドメインへのリクエストになる可能性があります。



したがって、再帰ドメイン・ネーム・システム（DNS）インフラストラクチャ上で検証されずに遍在的に返されるインターネットリクエストによって、サイバー脅威が感染したエンドポイントを経由して、その脅威がネットワークに戻される可能性が高くなります。脅威がネットワークに到達すると、CnC（コマンド＆コントロール）フレームワークに接続しようとします。この通信が確立すると、DNS ベースのデータ窃盗によって機密データや個人情報がネットワークから抜き取られる可能性があります。これによって、企業の専有データ、個人情報、ゲストユーザーの ID などが抜き取られる可能性があります。

ゲスト Wi-Fi を保護する

さらに、保護も監査もされていないゲスト Wi-Fi ネットワークは、企業ネットワークのセキュリティ対策を迂回しようとする従業員による誤用も多く見られます。従業員がそのエンタープライズ組織の利用規定（AUP）で禁止されているコンテンツにアクセスしようとしているのか、生産性の妨げとなるセキュリティメカニズムの使いにくさやイライラを回避しようとしているのかに関係なく、このようなネットワーク間のバウンスによって社内セキュリティ対策は損なわれ、多層防御戦略に亀裂が生じます。



保護も監視もされていないゲスト Wi-Fi は、お客様、訪問者、ボランティア、従業員を危険にさらすサイバー脅威の手段であるだけでなく、企業が苦労して手に入れたブランドの評判に危険をもたらすものです。企業の価値観や行動に個人的に共感できることが消費者のロイヤルティを左右するという今日の情勢において、そのことがかつてないほど重要であることは間違いありません。そのように、サービスを悪用して不適切あるいはいかがわしいコンテンツ、さらには違法なコンテンツまでも得ようとするゲスト Wi-Fi ユーザーは、企業ブランドの評判に多大な弊害をもたらし、最終的には従業員の収入にも悪影響を及ぼす可能性があります。

ゲスト Wi-Fi に接続するユーザーは、このような利用規定の違反を克服した上でのセキュリティに期待しています。そのため上記のように、ネットワークへの接続中にデバイスや個人情報に悪影響が生じたりデータ漏えいが発生したりすると、企業のブランドイメージは間違いなく損なわれます。Wi-Fi によって壊滅的なランサムウェアがコンピューターに侵入したり、クレジットカード情報が公開されたりした場合、その Wi-Fi を所有する企業を信頼して将来のビジネスを託す人がいるでしょうか。

対策の実施：ゼロ・トラストの実装

お客様、訪問者、ボランティア、従業員に対して、責任を持って安全な Wi-Fi 接続を提供するには、ネットワークのセキュリティを確保し、ユーザー、デバイス、情報を保護する必要があります。そして、当然のことながら、収益とのバランスを図る必要があります。ゲスト Wi-Fi のセキュリティ強化のためのコストは、取り組みを制限する要因になることが多いからです。ゼロ・トラスト・セキュリティ・モデルを採用して、アプリケーションやデータを配信する前にすべてのデバイスとユーザーの認証と承認を行う一方で、ロギングや行動分析によってアプリのアクセスとネットワークアクティビティを監視することで、ゲスト Wi-Fi を簡単に保護できます。

ゼロ・トラスト・セキュリティ・モデルについて詳しくは、**「Moving Beyond Perimeter Security（境界セキュリティを超える対策）」**をご覧ください。また、ゲスト Wi-Fi のセキュリティを確保するクラウドベースの集中管理型で拡張が簡単な Akamai のソリューションについて詳しくは、akamai.com/etp をご覧ください。

Akamai