物理層のデータセキュリティを用いた社内外の脅威の防止

高度な接続性を誇る、今日のスマートビルにおいては、あらゆるネットワーク接続が企業ネットワークやミッションクリティカルなネットワークへ侵入するための入口となり得ます。同時に、内部の脅威については、保護するデータにアクセスできる人々の数が、攻撃ポイントの規模を直接左右します。

特に、アジア太平洋ではデジタル接続の割合が高く、その一方でサイバーセキュリティの認知度が低く、国境を越えたデータ転送が増加しており、規制が弱いため、サイバー犯罪者にとっては理想的な環境です。例えば、東南アジアではデジタル変革がすべての経済分野へ進出しており、インターネットは人口の大半で利用されるまでに至っています。

内部の脅威がデータ侵害で軽視されがちな要素であるのと同様に、ネットワークアクセスのセキュリティもまた、保護対策であまり重視されない領域です。CommScope Ruckus Cloudpath導入システムのように、セキュアなオンボーディングと認証用のシステムを使用すれば、役割に基づいたネットワークアクセスのポリシーを簡単に定義して管理できます。許可されない活動が検出された場合、IT部門はネットワークへのアクセスを遮断できます。

ネットワークアクセスに関するヘルプデスクへの問い合わせを劇的に減らせるセキュアなオンボーディング以外にも、あらゆる進入の経路や層にて、企業は未承認のアクセスを防止しなければなりません。この対策には、アプリケーションレベルでの暗号化、仮想プライベートネットワーク、ファイアウォール、物理層のセキュリティが挙げられます。

物理層のセキュリティ

企業ネットワークでのデータ侵害のコストは、金銭的な損失の範囲をはるかに超えます。企業が信頼を取り戻し、評判を回復するまでに数年はかかります。データセキュリティ侵害の60%は、社内の人物による悪意のある攻撃や不注意によって起こると推定されています。社内外の脅威に対するデータセキュリティのプランでは、物理層のインフラが明らかに重要な役割を果たします。

ヘルスケアや金融などの業界では、ネットワークセキュリティの問題は、データストレージに関する規制と準拠要求を生み出しました。ネットワークセキュリティ上の課題は主に2つのカテゴリーに分類されます。

- 権限を持たない人による不認可のアクセスは、IP接続されたカメラ、占有率センサー、アクセス制御、その他の物理的セキュリティを賄う接続された要素の実装によって、防止または軽減できます。キー付きコネクタ、セキュアなパッチコード、ポートブロッカーなどの物理的な配線セキュリティを導入し、不認可アクセスの脅威を減らせます。同様に、自動インフラ管理（AIM）ソリューションは物理層におけるすべての未承認活動を記録し、報告できます。

- 権限を持つ人物による未許可のアクセスは、検出と排除がより難しくなります。エンタープライズネットワークの複雑さと深遠さに対処するAIMシステムを使用して、ネットワーク管理者は内部からネットワークの接続を監視して管理できます。インテリジェントなケーブル配線、コネクター、パッチパネルを使用し、同システムはリアルタイムでポートとデバイスレベルの物理層での活動すべてを自動的に検出してマッピングします。権限を持たない人物がデバイスへ接続したり、接続を解除すれば、CommScopeのimVisionが自動的にIT担当者へ警告を発します。

ビル内ワイヤレス

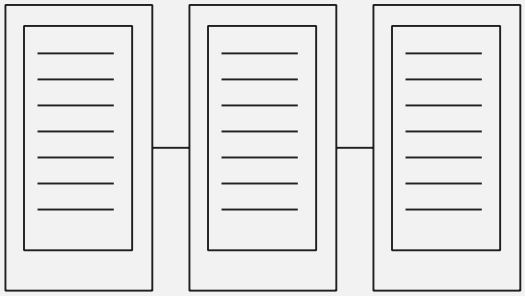
モバイルトラフィックの大部分はビル内から発信されるかビル内へ送信される事実を踏まえ、ビル内ワイヤレスネットワークは企業にとって、水道や電気と同程度に必須のインフラと化しています。悩ましいことに、ハッカーがほとんどの企業Wi-Fiシステムで使用されるWPA2セキュリティプロトコルの脆弱性を悪用する方法を発見しています。

同プロトコルの最新バージョンであるWPA3（企業向け）は、192ビットの暗号化と同等の強度を誇ります。代わりに、サービスプロバイダーが一括してセキュリティを管理して制御する、専用の分散アンテナシステム（DAS）で駆動されるセルラーやモバイルネットワークのほうが、旧来のWi-Fiよりも強固で高い応答性を示します。

セキュリティ監視とパワードファイバー／PoEケーブル配線

インテリジェントビルで一般的に設置されるIPセキュリティカメラと占有率センサーのネットワークが、権限を持たない侵入者の検出に役立っています。適切なケーブル配線インフラが設置されていれば、こうしたパワー・オーバー・イーサネット（PoE）社内セキュリティモニターをビルやキャンパス全体に配置できます。

AIMシステムはハッカーの疑いがある人物を特定することしかできませんが、カメラであれば視覚的な証拠を得られます。低電圧のパワードファイバーやPoEネットワークは、こうした接続センサー、カメラ、コントローラーをサポートします。主電源が切断されても、AIMシステムやすべての接続セキュリティデバイスはスイッチから電源を得て稼働し続けます。スイッチは通常、UPSバッテリーや発電機でバックアップされます。この電源体系の方が、本質的に復元力があり、セキュアです。



成功事例：ハノイ証券取引所、ベトナムと南オーストラリア州医療研究所、オーストラリア

継続的な監視と警告を通じて真のセキュアネットワークを実現

ハノイ証券取引所と南オーストラリア州医療研究所（SAHMRI）の両方において、接続性のパフォーマンスが最重要となるセキュアなネットワークインフラを確立することが主要な課題でした。

システム管理者がネットワークの物理層をリアルタイムで把握できるようにし、トラブルシューティングを速め、セキュリティを改善しつつ、同時にネットワークの休止時間を低減して、メンテナンスを低コストに抑えるため、インテリジェントなインフラ管理が必要とされました。

ソリューション

両組織は構内配線の大手サプライヤーであるCommScopeへ打診し、インフラの要件をすべて満たすSystem Managerソフトウェア、iPatch Manager、iPatchインテリジェント銅線／ファイバーパネルで構成されるSYSTIMAX iPatchシステムを導入しました。

CommScopeが行う設置は、グローバルなサポート体制と、業界最長の20年保証に裏付けられています。ハノイ証券取引所では、完成したインフラがCCTVとアクセス制御システムを接続します。データセンター内で、SYSTIMAXのケーブル配線がサーバーとストレージエリアのネットワークを接続します。

同時に、SYSTIMAX 360ソリューションをベースとするネットワークインフラがSAHMRIのデータシステムへ接続し、ビル管理、セキュリティ、ボイスオーバーIP、照明制御などの超低電圧システムをサポートします。こうした重要なアプリケーションは銅線とファイバーのケーブル配線に依存し、高性能と高信頼性を特徴とします。

メリット

両組織のIT管理者は物理層をリアルタイムに可視化し、制御できるようになりました。設置場所の銅線とファイバーの接続は、ネットワーク接続と取付られたデバイスの監視が可能なiPatchパネルを使用して管理されました。

成功事例：ハノイ証券取引所、ベトナムと南オーストラリア州医療研究所、オーストラリア

iPatchソフトウェアはまた、未承認のアクセスポイントを検出して位置を特定し、管理者へあらゆる変更を直ちに通報します。System Managerソフトウェアは、標準のウェブブラウザーを通じたインフラの文書化と監視を支援します。

imVision AIMプラットフォーム

iPatch Systemをベースに、CommScopeはimVision AIMソリューションを提供します。ネットワークの物理層とそこへ接続されるデバイスへ影響を与える事象を一段上のレベルで可視化し、リアルタイムのインテリジェンスを提供し、実行可能なインサイトを加えます。

AIMソリューションは、接続環境をリアルタイムで監視するために、インテリジェントケーブル配線、コネクター、パッチパネルを使用します。未認証または認証済みのデバイスが許可されない情報へアクセスを試みていることを検出すると、システムは直ちに警告を発します。

System Managerは、ワイヤレスで動作するものも含め全てのデバイスについて、ネットワーク内の移動を追跡します。同ソフトウェアはPoEデバイスとも統合し、接続場所へ電力が供給されていることを確かめます。さらに、iPatchインテリジェントパネルは、ネットワークで不慮の変更が検出された場合にリアルタイムで警告を発信します。

カテゴリ6Aのケーブル配線を使用したPoEとパワードファイバー技術を導入することで、IPセキュリティカメラやAIMベースのインテリジェンスといったセキュリティシステムの復元力を強化できます。