PHYSICAL-LAYER DATA SECURITY STOPS INTERNAL, EXTERNAL THREATS

In today's hyper-connected smart buildings, every network connection is a path into a corporate or mission-critical network. At the same time, the size of the attack surface when it comes to insider threats varies directly with the number of people who have ac-cess to the data being protected.

Asia-Pacific, in particular, is an ideal environment for cyber criminals to thrive in due to high digital connectivity, contrasted with low cybersecurity awareness, growing cross-border data transfers and weak regulations. In Southeast Asia, for example, digital transformation is pervading across all economic sectors and internet access has become affordable for large segments of the population.

In the same way that insider threats are an underestimated cause of data compromise, network access security is an underestimated layer of defence. A system for secure onboarding and authentication like the CommScope Ruckus Cloudpath Enrollment System makes it easy to define and manage role-based policies for network access. It gives IT teams the power to cut off network access if any inappropriate activity is detected.

Apart from secure on-boarding, which dramatically reduces helpdesk tickets related to network access, enterprises have to avoid unauthorised access at every layer and secure every point of entry – from encryption at the application level, to authentication, virtual private networks, firewalls and physical-layer security.

PHYSICAL-LAYER SECURITY

The cost of a data breach in the enterprise network goes beyond financial damage; it can take years for a business to regain trust and rebuild its reputation. It is estimated that 60% of data security breaches were carried out by insiders with either malicious or inadvertent intent. The physical layer infrastructure is clearly a critical a part of any data security plan against internal and external threats.

In industries such as healthcare and finance, the issue of network security has spawned regulations and compliance requirements regarding data storage. Network infrastructure security concerns generally fall into two categories:

- Unauthorised access by an unauthorised person can be reduced or prevented through the deployment of IP-connected came ras, occupancy sensors, access controls and other connected elements of physical security. Physical cabling security such as keyed connectors, secure patch cords and port blockers can be deployed to reduce the threat of unauthorised access. Similarly, automated infrastructure management (AIM) solutions can record and report any unauthorised activity on the physical layer.

- Unauthorised access by an authorised person can be more difficult to detect and repel. Given the depth and complexity of the enterprise network, an AIM system enables network managers to monitor and manage network connections from the inside. Using intelligent cabling, connectors and patch panels, it automatically detects and maps all physical layer activity at the port and device level, in real time. If an authorised user connects or disconnects a device, an AIM solution like CommScope's imVision automatically alerts IT personnel.

IN-BUILDING WIRELESS

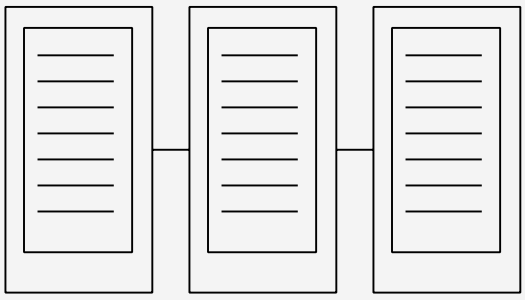
Given that the bulk of mobile traffic originates or terminates within a building, in-building wireless networks have become as vital to an enterprise as water or electricity. A worrying trend is that hackers have found ways to exploit weakness in the WPA2 security protocol used by most corporate Wi-Fi systems.

The latest iteration of the protocol – WPA3 for Enterprise – offers the equivalent of 192-bit cryptographic strength. Alternatively, a cellular or mobile network powered by a dedicated distributed antenna system (DAS) with security administered and managed centrally by service providers may be more robust and responsive than legacy Wi-Fi.

SECURITY MONITORING AND POWERED FIBRE/ POE CABLING

Networks of IP security cameras and occupancy sensors commonly installed in intelligent buildings are helping to spot unauthorised intruders. With the right cabling infrastructure, these Power over Ethernet (PoE) internal security monitors can be distributed throughout the building or campus.

While an AIM system can only locate a would-be hacker, cameras provide corroborating visual proof. Low-voltage powered-fibre or PoE network supports these connected sensors, cameras and controllers. If the main power fails, the AIM system and all connected security devices continue to function because they draw their power from the switches, which are typically backed up by UPS batteries and generators. This power structure is inherently more resilient and secure.



SUCCESS STORIES: HANOI STOCK EXCHANGE, VIETNAM AND SOUTH AUSTRALIAN HEALTH MEDICAL RESEARCH INSTITUTE, AUSTRALIA

CONSTANT MONITORING AND ALERTS MAKE A TRULY SECURE NETWORK

Establishing a secure network infrastructure where connectivity performance is critical had been a key concern for both Hanoi Stock Exchange and the South Australian Health Medical Research Institute (SAHMRI).

Intelligent infrastructure management was needed to provide system managers a real-time view of the network physical layer, speed up troubleshooting, and improve security while reducing network downtime and making maintenance more cost effective.

SOLUTION

Both organisations turned to CommScope, a leading supplier of structured cabling, and deployed the SYSTIMAX iPatch system consisting of the System Manager soft-ware, iPatch Manager, and iPatch intelligent copper and fibre panels that met all their infrastructure requirements.

CommScope's installations are backed by a global support network and industry-leading 20-year guarantees. At the Hanoi Stock Exchange, the finished infrastructure connects CCTV and access control systems. Within its data centre, SYSTIMAX cabling connects servers with a storage area network.

Meanwhile, SYSTIMAX 360 solutions-based network infrastructure connects SAHMRI's data systems and supports extra-low-voltage systems, including building management, security, voice-over-IP and lighting control. These critical applications depend on copper and fibre cabling with high performance and reliability.

BENEFITS

IT administrators at both organisations gain real-time visibility and control of the physical layer. Copper and fibre connections in the installations are managed using iPatch panels that allow monitoring of network connections and attached devices.

SUCCESS STORIES: HANOI STOCK EXCHANGE, VIETNAM AND SOUTH AUSTRALIAN HEALTH MEDICAL RESEARCH INSTITUTE, AUSTRALIA

The iPatch software also alerts administrators immediately of any changes by detecting and locating unauthorised access points. The System Manager software helps to document and monitor the infrastructure through a standard web browser.

IMVISION AIM PLATFORM

Building on the iPatch System, CommScope offers its imVision AIM solution, which drives actionable insights as well as a new level of real-time intelligence and visibility into events that impact the network's physical layer and the devices connected to it.

An AIM solution uses intelligent cabling, connectors and patch panels to monitor the connected environment in real time. Should it detect an unauthorised or authorised device attempting to access unauthorised information, the system issues an immediate alert.

The System Manager tracks all devices, even those operating wirelessly, as they move about a network. The software also integrates with PoE devices, verifying that power is available to a connection. Further, the iPatch intelligent panels initiate real-time alerts whenever they detect unexpected changes to the network.

Deploying PoE and powered-fibre technology using Category 6A cabling also increases the resilience in security systems such as IP security cameras and AIM-based intelligence.