Talking About Cybersecurity

A step-by-step guide to convincing an IT team that your AV gear is safe to live on their network

There's no question that AV is moving onto the network. But there are still a lot of unanswered questions about whether it's safe to put AV gear directly onto the main network, or if it needs to be segmented off onto a VLAN or an entirely separate network.

With all these questions, we need to have more conversations between AV and IT teams, and also with a new contingent of interested parties related to "smart buildings": Operational Technologies (OT). Networked technology is a part of nearly every element of an enterprise, school, museum, stadium, hospitality venue or healthcare facility. And it's in the best interest of everyone in AV/IT/OT to ensure that linked systems operate smoothly, efficiently and safely on a network.

We've created a high-level overview of the topics that matter most to IT decision-makers and their OT counterparts. AV designers and integrators who address these problems early and often in their conversations will build lasting relationships with clients – which is especially vital when it comes to cybersecurity and the ongoing monitoring and updates.

Conversation Starters

Policies

Before you begin anything – Ask for details on the client's network policies, security standards and compliance requirements.

Passwords / User Privileges

Guidance on password safety is constantly changing – make sure you're up to date on the latest password protocols before you promise how those will be implemented within your AV systems.

Set up account privileges to control access to the networked systems and client data.

AV Hardware Documentation

Be prepared to provide AV hardware specifications (including port access details – more on that below), capabilities and potential security risks.

Include any security certifications or assessments the hardware has undergone. Collaborate with the CISO or IT team on any third-party audits.

List built-in security features such as encryption, access control and authentication mechanisms.

Risk Assessment

Address potential security risks and vulnerabilities. Explain how these risks are mitigated by the hardware's security measures.

Data Protection and Privacy

Emphasize how the AV hardware respects data protection and privacy. Establish with IT and OT how audio and video data will be handled, stored and deleted as per privacy regulations.

Testing / Pilot Phase

Suggest running a limited pilot phase to demonstrate the hardware's safety before full deployment.

Highlight the need for testing and validation of Ethernet port configurations before full deployment. Explain that thorough testing will ensure that AV hardware functions seamlessly on the network.

Monitor and evaluate the hardware's performance and security during the pilot phase. Address any issues promptly. Contact design services support at manufacturers or ADI to help figure out the best strategy.

Don't forget the QoS - Test to find out if security settings increase latency or create other problems in delivery of AV content.

Continue the Conversation

Vulnerability Management

Set up a Network Monitoring plan to keep your systems protected throughout their lifecycle. Continually monitor systems and networks to check for unusual or unauthorized activity. Identify future problems before they impact business operations.

Create a strategy for conducting software updates and firmware patches to keep the AV hardware secure. Test these first for compatibility with your system before deploying across a network.

Keep an inventory of all devices and their configurations.

To VLAN or Not to VLAN

This is the eternal question, and will still vary from client to client. So make sure to ask it early, when you're looking at the client's network security protocols.

If needed, explain that dedicating specific VLANs for AV traffic can enhance security and network performance. This separation can prevent potential conflicts with other network traffic and limit the attack surface for the AV hardware.

Ethernet Port Allocation

Port requirements will vary by manufacturer. This gets back to the documentation phase. Provide a clear breakdown of which ports are needed for data, control and any other specific requirements.

Describe port security measures, such as MAC address filtering if the client prefers it and it's possible to provide instead of AV's preferred IP addresses. This is still a sticking point in conversations, so be prepared to compromise.

Don't forget to allocate enough capacity for Power over Ethernet.

Read our eBook on delivering the best AVoIP experience

Read the E-Book