05/05/2025

Modern Security Challenges and Practices for Media Facilities

Michael Bany, Fox

Security used to be simpler

- Air chains and Media facilities had large numbers of distinct components.
- A lot of these components were more difficult to compromise due to obscurity.
- Everything was connected by SDI and patch panels.
- The risk of being compromised via SDI or GPIO was low.
- You could add extra redundancy fairly easily.
- If everything else failed, you could patch around an issue.

Security became more important

- Security has always been a concern.
- It became more of a concern after a major studio was hacked about ten years ago
- Dedicated Security Budgets Appeared
- Companies have added CISOs
- As more and more major security events have occurred security has become the top priority everywhere.

Facilities are more flexible and efficient

- That also makes them harder to secure.
- COTS equipment is more flexible and economical.
  - Standard Servers
  - IP Networking
- This includes their security risks.
- Consolidation of functions puts more eggs in a single basket.

Security for a Media Facility

- When you look security for a media facility and all the workflows that go on in that facility it becomes very complex.
- The on air or production components of the media network are considered the highest security segments of your network.
- As a rule, you do not allow access to the internet from these segments.
- You do not allow lower security network segments to have access to higher security segments.
- Never allow a device to span security zones.

Walled Garden not good enough

- A lot of people still think that creating a walled garden and preventing access from the outside is enough.
- Software updates can compromise your network.
- An endpoint can be easily compromised and establish a command-and-control channel.
- Even DNS can be a concern as threat actors have used it for control
- Vendor equipment that phones home can setup a reverse ssh or ssl tunnel that allows unrestricted remote access to your network.

Exceptions

- Very shortly after building this walled garden you will get requests.
  - Remote access for employees.
  - Remote access for vendors
  - Local access for vendors.
  - Moving files in and out
  - Transferring Files between security zones.
  - Installing and Updating applications and operating systems
  - Licensing
  - Live Research
  - Outside services
  - Vendor control
  - Data services
  - Closed Captioning
  - Artificial Intelligence
- You either say no and loose functionality or say yes while trying to secure it as much as possible.

Security Concepts

- Penetration testing
- North south
- East West
- Zero Trust
- NDR Network Detection and Response
- EDR Endpoint Detection and Response
- NAC Network Access Control

North South

- Classic firewall security with multiple security zones.
- If a zone is compromised everything in it can be compromised.
- To many rules can be unwieldly and require dedicated staff to maintain.
- You can end up with hundreds of rules that nobody knows are in use or why they are there.
- Firewalls can become costly choke points on your network.
- Media flows can utilize significant bandwidth on firewalls.
- UDP can cause issues with firewalls that are not configured correctly.
- There are options for securely bypassing a firewall for media flows.

Penetration testing

- It is better to be do before going into production.
- A lot of equipment doesn't handle this well.
- Devices can crash or go offline.
- Every time you update a system new issues can appear.

East West

- Securing all traffic within a security zone
- Helps prevent the spread of a compromised endpoint
- Requires the network itself to support access control
- Greatly increases the number of security rules over North South alone

EDR Endpoint Detection and Response

- Run software on each endpoint to monitor for threats and respond to them.
- Can flag many issues before they become serious.
- Gives very good insight into what is going on.
- Getting support from vendors to run security software is a huge challenge.
- Make sure your endpoints have additional processing power to run EDR.

NDR Network Detection and Response

- Monitor all traffic on the network for threats
- Tap aggregation network
- Built-in detection within switches
- Allows EDR like functionality without require software on endpoints.

NAC Network Access Control

- Authenticates the device
- Verify it meets minimum security policies
- Disconnect suspicious endpoints

Zero Trust

- One of the most secure concepts
- Combines most of the other concepts together
- Opposite of a Walled Garden
- Continuous verification
- Can require a re-architecture of your facility
- Fairly complex. A failure can cause loss of control

Challenges

WIFI

- WIFI requests for portability in studios etc.
- WIFI can be hacked.
- How to secure access?
- Disable WIFI in secure devices as it allows a device to span security zones

Foreign Computers

- Rental Equipment
- Foreign Trucks
- Vendor Laptops
- Even company owned laptops can be concerning

Vendor and Remote Access

- How do you allow vendors access to your network to resolve issues.
- Only connect to the network when someone has permission and notifies engineering.
- VPNs are risky
- VDI helps

Cloud based services.

- Private cloud is easier to secure as you own it.
- Public cloud requires significant due diligence.
- Are the service provider security policies sufficient?
- How safe is your data?
- How do you get your data back when you no longer need the service?
- How do you make sure they delete it?

Patching

- We usually test vendor software for security when installed. How often do you reverify?
- It is very important to have the latest patches. However, there are new patches weekly in some cases and patches can break things.
- How frequently do you test and patch broadcast systems?
- How do you recover from an unsuccessful patch?

Backup and Recovery

- Backing up bare metal
- Virtualization helps but adds additional cost and support overhead
- Store immutable backups
- Practice restorals

Identity and Authentication

- SAML or OIDC authentication to prevent stagnant local credentials.
- What happens if your authentication provider is not accessible?
- How to efficiently maintain break glass passwords.

Documentation and Education

- Most important

Thank you

vsf.tv