Securing Your Physical Security Network

The 12 point checklist of critical security flaws typically found in surveillance systems, and what to do about them

Updated: **November 2022**

Introduction

- **Surveillance systems are mission-critical for many organizations, yet the combination of camera devices, encoders, switches, storage, and other network elements leave you open to security vulnerabilities. Compliance to many standards (PCI, NERC, NIST, etc) also requires ensuring your surveillance system can't be compromised.**
- **Most of the potential security breaches come down to a few key parts of the network that you need to pay attention to. Based on supporting over 1.2 billion hours of video from surveillance video networks, Viakoo has found that the "80/20" rule is alive and healthy.**
- **This checklist is meant as a starting point for reducing potential security issues. Once security issues are found and resolved, Viakoo encourages you to refer back to this checklist to ensure that changes across your network still maintain the security of your security video network**

1. Default Camera Passwords

- Have all default camera passwords been changed? This is one of the most-overlooked and also most basic security flaws. The risk of this is great because default passwords often can be found online, as many recent cases have shown. As part of initial deployment all camera devices should have unique passwords set.

2. Failed Login Attempts

- Is your network able to provide alerts on multiple failed login attempts? Multiple failed login attempts are a sign that hackers are attempting to breach security. Security video networks typically have multiple points of entry, all of which should be observed for this behavior.

3. No VPN Access

- Have you set a policy to never allow VPN access to your security video network? Allowing VPN access is risky because there is no control over who is on other end, and no audit trail. Diagnostic information should not require VPN or other form of remote login.

4. Outsiders on Production Network

- Can the production network be accessed by third parties onsite? Unmanaged access can lead to video content being removed or deleted by third party service providers. Safeguard against laptops or other devices connecting to the production network, and provide a sandbox or non-production network to verify fixes.

5. Eliminate USB Device Access

- Are there open USB ports in your security network? Eliminating physical or logical access through USB devices prevents malicious agents or malware from being injected into the video security network. There are both physical and logical ways to restrict USB access.

6. Foreign Device Connections

- Is it another authenticated device you're connecting to? Your network should have an automated alert process if foreign devices (e.g. non-authorized devices like laptops, rogue APs, etc) are attached to the network. In general, using wired connections avoids "honeypot" threats.

7. Video File Deletions

- Can you tell if video files have been tampered with? Any unauthorized file deletions/modifications should trigger an alert. Unauthorized file deletions may cause you to violate retention policies or otherwise fail compliance requirements.

8. Software Drivers & Firmware

- Do you know if you are using the most current (and secure) software? Automated checking of drivers and firmware detects if an up-to-date driver is replaced with earlier versions. Tracking software drivers & firmware prevents older versions that are susceptible to security breaches from remaining on your network.

9. Camera Device Tampering

- Has there been physical tampering? Automated alerts should be in place in the event that the camera device has been tampered with (the lens is covered, the power removed, scene changes, etc). Tampering will reduce or eliminate both situational awareness and evidentiary records.

10. Workspace for Collaboration

- Do you have a method for collaborative problem resolution that does not violate security policies? Having a sandbox, staging, or other test environment separate from production is a best practice; never use production for fixing security.

11. Keep Diagnostic Data Elsewhere

- Is there a separate repository for diagnostic data? The diagnostic data for the video security network should be stored in a different location from the production network and video stream data in case there is any malicious tampering.

12. Keep Content Restricted

- Does accessing video data directly require a higher level of authentication? Whether at the camera device, in the network, or in the storage environment, user access to video streams or files should require specific and more stringent authentication. Weakly-managed viewing access may lead to privacy, compliance and brand risk.

Viakoo helps automates many of the best practices described here, as well as other aspects of keeping your video security network up and running.

We encourage you to visit www.viakoo.com for more information, and to sign up for a free demo account.