A Checklist for Securing IP Cameras
Visible and Thermal

Cybersecurity is a topical issue within the surveillance space. Multiple reports suggest that almost all IP-based cameras ship with default credentials, but many were left unchanged by customers.

While thermal cameras are rarely mentioned in the discussion, security precautions mentioned in this article are essentially the same for all IP-based cameras, both visible and thermal.

An IP camera is an endpoint for a network. As such, it represents a potentially vulnerable point of entry for attackers to execute code and launch exploits. For example, in 2016, a massive Distributed Denial of Service (DDoS) attack, using a Mirai botnet, slowed or knocked offline a group of major websites, causing significant outages across the Internet.

The security of all network devices is a shared responsibility, and one weak link can affect the entire network. The threat of inadequate security measures by some manufacturers has prompted the US Government to include Section 889, the Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, in the 2019 National Defense Authorization Act (NDAA). Section 889 prohibits the Federal Government from obtaining or extending a contract to acquire "any equipment, system, or service that uses covered telecommunication equipment or services as a substantial or essential component of any system, or as critical technology as part of any system." This rule was put into place to prevent cyber-attacks and efforts from exfiltrating information and intellectual property by foreign adversaries, which pose risks for the US government and industry.

An organization can make large investments in physical security technology. Still, technologies such as cameras can often be used as a backdoor into networks, negating network security and putting a business at risk. According to Mike Sanchez, CISO of United Data Technologies: "They start in the surveillance system and go from there to the data center, and...to the accounting department".

The alignment of security teams and integrators with IT/OT teams is more important than ever to ensure the highest cybersecurity protection level. The majority of cyberattacks stem from human error, and there can be severe consequences without adequate IT/OT security policies. All teams involved in working with endpoint devices should have relevant training to ensure they understand the potential risks. Cameras that are not updated, according to the manufacturer's recommendations, are more susceptible to cyberattacks.

Cyber vulnerabilities are a continuous threat, but effective policies should prevent risks to the network, such as password policies, encryption certificates, limiting network ports, and training.

The following is a checklist of best practices for proactively implementing cyber defenses in network cameras.

Secure Login

Most electronic devices require a password-based login, and entering passwords has become an intrinsic part of our daily lives. Often people will opt for simple or repeat the same passwords to ensure they are memorable, but this creates a security risk. Organizations must adopt a password policy that provides the highest security level for their devices and networks.

Most cameras have a default username and password, which are available in manuals and online. Often integrators and end-users will neglect to change these credentials, making the devices an easy target for malicious attacks.

“These devices come from the manufacturer with a common user ID and password, something like ‘admin’ for both. People don’t bother to change that, or they don’t have a complex password policy, so the password is not strong enough,” Mike Sanchez says.

The best practice to protect organizations is for the manufacturer to ship cameras without a pre-configured login, prompting the administrator to configure his unique login out of the box, preventing backdoors. The most critical step in protecting devices and networks is to use a password unique to each device.

Authentication and Encryption

One method of securing the camera’s data across the network is to create a Secure Sockets Layer (SSL) encryption certificate. A known Certification Authority (CA) should sign the certificate. The CA’s root certificate should be installed on the computers accessing the camera to validate the certificate on the cameras and set a reasonable expiration date of a year or two. Once you upload a certificate to the camera, you can ensure all communications go through the HTTPS port (encrypted).

The best practice is to create the Admin user for the first time through a direct connection or secure environment to the camera and upload the SSL certificate before using it in an operational environment. When connected to the network and creating additional users, it’s highly recommended not to send plain text passwords. The administrator should protect video access by requiring a username and password and tunneling communications over HTTPS when it’s enabled.

Network Configuration

Many hackers are using scanners to scan for connected devices. A simple way to impede these scanners is to change the ports of the networked cameras. Generally, cameras use well-known default ports. Changing these to alternative ports will ensure an extra step when entering the address into the web browser, hence protecting the camera from scanners or manual entries.

It is advisable to permit the changing of ports, specifically HTTPS and RTSP, ensuring an additional layer of protection against scanners and other attempts to compromise the camera’s security.

A Checklist for Securing IP Cameras
Visible and Thermal

Disabling Unused Ports, Services, or Protocols

Many cameras are considered edge computing devices with the processing power and operating systems of a computer. This helps bring computation and data storage closer to the endpoint device, i.e., the camera, saving on network bandwidth. It is therefore essential to ensure that unused services and protocols are disabled or removed. Several attacks have occurred through services, such as telnet, which are not always necessary for a camera's functioning.

Unused services, such as DDNS, QoS, and Bonjour, should be removed from the operating system to prevent unnecessary risks. Another suggestion is to block the SSH network protocol by default. The camera's administrator can then open SSH manually if remote support is required. The SSH session should open only for the computer from which the request originated and have a specific timeout. It's advisable to ensure there's a timeout for all web-based Graphical User Interface (GUI) sessions.

Device Logs

It's essential to regularly check the logs of the cameras to review changes made and by whom.

These logs should be encrypted to ensure that data is not easily accessible if there is a need to share them with the manufacturer.

During a reset, the camera should retain the logs. The logs should contain all login attempts across all protocols. If there is something suspicious in the log file, a reset to factory defaults may be required. After the camera has returned to default, the administrator should change the password in case of a network breach. It should be possible to retain network settings and users during a reset.

Device Logs

It's essential to regularly check the logs of the cameras to review changes made and by whom.

These logs should be encrypted to ensure that data is not easily accessible if there is a need to share them with the manufacturer.

During a reset, the camera should retain the logs. The logs should contain all login attempts across all protocols. If there is something suspicious in the log file, a reset to factory defaults may be required. After the camera has returned to default, the administrator should change the password in case of a network breach. It should be possible to retain network settings and users during a reset.

Configuration Backup

A regular backup is vital to ensure continuity in the case of an attack. This backup ensures that the administrator can quickly restore affected cameras to their configurations without causing lengthy interruptions to security.

Ensure it's possible to export site defaults of every camera for continuity of service.

References

[i] Hacked Cameras Were Behind Friday's Massive Web Outage - https://www.forbes.com/sites/briansolomon/2016/10/21/hacked-cameras-cyber-attack-hacking-ddos-dyn-twitter-netflix/

[ii] National Defense Industrial Association – Section 889 - https://www.ndia.org/policy/section-889

[iii]Cyber-Securing Video Cameras - https://www.securitymagazine.com/articles/89377-cyber-securing-video-cameras

[iv] Report: Majority of surveillance cameras running out of date firmware - https://www.securityinfowatch.com/video-surveillance/cameras/ip-network-surveillance-cameras/news/21117133/report-majority-of-surveillance-cameras-running-out-of-date-firmware

OPGAL
Beyond the Visible

CONTACT US

Firmware Updates

Hackers prey on software vulnerabilities, particularly outdated software that doesn't conform to current security standards. A hacker will promptly broadcast any security vulnerabilities online, effectively exposing the network to other individuals. It is vital to ensure that you always have the latest firmware on your camera.

"Our primary research data points to the fact that more than half of the cameras with out-of-date firmware (53.9%) contain known cybersecurity vulnerabilities. By extrapolating this to an average security network, nearly four out of every ten cameras are vulnerable to a cyber-attack," Mathieu Chevalier, Lead Security Architect at Genetec, said in a statement.

Ask your camera manufacturer how often they release firmware updates and whether they are tested against an application security verification standard.

Summary

We are living in an increasingly connected world in which hackers will continue to exploit network security vulnerabilities. Year on year, requirements for network cameras will increase, hence increasing the likelihood of an attack. Check cameras are appropriately secured to prevent them from becoming an open door to a network. Ensuring that best practices are adhered to can help prevent attacks, provide network integrity, and the continuous operation of a critical function

Opgal, a world leader in thermal technology and camera manufacture, has heavily invested in ensuring its cameras comply with cybersecurity requirements now…and in the future. For more information on our cybersecurity measures or thermal camera technology, please contact Howard Glick at:

glick@opgal.com