INFORMATION SYSTEMS

Risks of default password in IoT devices(CCTV) and how to make them more secure.

Risks of Default Passwords in IoT Devices

Password hacking- hackers are concentrating on the construction of malware which comes preloaded with huge list of default passwords, so that breaking through defenses becomes a little bit easier and quicker. The default password can then be leaked and shared online, this can be used maliciously to carry out attacks. It is importance to change default passwords as soon as possible as cyber criminals could use it as a tool to gain access into systems and take control of IoT devices.

Command injection- is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

DDoS attack. Is a malicious attempt to disrupt the normal traffic of a targeted server, services or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic. It utilizes multiple compromised computer systems as a source of attack traffic. It is carried out with networks of interconnected machines. These networks consist of computers and other devices such as IoT which have been infected with malware allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots and a group of bots is called botnet. Once a botnet has been established the attacker is able to direct an attack by sending remote instructions to each bot to the targets IP address, causing the server t or the network to become overwhelmed, resulting in a denial-of-service to normal traffic.

Scanning attack- is a method used by threat actors to identify vulnerabilities in a network **or** system. Scanning attacks typically involve using automated tools to scan for open ports, vulnerabilities, and other weaknesses that can be exploited to gain unauthorized access and/or launch a cyber-attack. These IoT devices are mostly manufactured in bulk by a company, and then another company design the software. This tends to result in very poor life-lance management and written code. Some IoT devices such as a CCTV IP-camera, are shipped with a built-in backdoor. This poses a threat since it is prone to malicious attack. A malicious actor who installs this backdoor either as a Man-in-the-Middle (MitM) or a supply chain attack has the element of Security personnel access to CCTV IP camera, which means a malicious actor could gain security personnel credentials to other services when these credentials are compromised.

IoT botnet attack- is a large-scale cyber-attack carried out by malware-infected devices which are controlled remotely. It turns compromised devices into ‘zombie bots’ for a botnet controller. Botnets pose a greater threat because they let a threat actor perform a large number of actions at the same time. Malware delivered via botnet often includes network communication features that allow attackers to use the botnet to route communications with other threat actors through the vast network of compromised machines. Attackers use botnets to compromise systems, distribute malware and recruit new devices to the brood. A botnet attack may be mostly for disruption or a means of blazing a path to launch a secondary attack.

IoT ransomware, is a malware designed to deny a user or organization access to files on their computer Threat actors control or lock a device to extort payment. Hackers infect devices with malware to turn them into botnets that probe access points or search for valid credentials in device firmware that they can use to enter the network. With network access through IoT device, attackers can exfiltrate data to the cloud and threaten to keep, delete or make the data public unless paid ransom

Malicious node injection. Hackers can also attack an IoT ecosystem by inserting or injecting fake nodes into the web of legitimate connecting nodes, thereby enabling hackers to alter and/or control the data flowing between the fake and legitimate nodes and, ultimately, all the nodes in the web.

Protecting Against Default Password in IoT Devices(CCTV)

Ensure the CCTV system does not respond to ping requests. Ping is a method used to detect whether an IP device is connected to the online. If the router is connected to respond to ping requests, it may alert potential attacker that a device is vulnerable to attack. Turn off ping request in the router and video serve to prevent this from happening.

Change the password on the CCTV system. Always change the manufactures default password. Also use a mix of uppercase letters, lowercase letters and digits to strengthen the password.

Configure your routers firewall. The firewall within your route will allow you to limit access to your CCTV to certain IP address ranges or MAC addresses.

Ensure the firewall on the CCTV system is up to date. Regularly check that your devices have the latest firmware Manufactures often address ant security or vulnerability issues with firmware updates.

Avoid using Admin as a username. Admin is probably the most common username used in IT departments and hackers are well aware of this. Even if you've changed your default password to something highly cryptic, a simple username such as 'admin' instantly halves the amount of work a hacker has to do.

Run regular audits on all IoT devices. Detecting and monitoring new devices on your network should become a priority. Any new and unknown devices to your network should instantly be blocked and an authentication process put in place. With this information you can then track down the devices owned and ensure that any default passwords are changed before further access to the network is granted.

Create a risk-driven security strategy. Involves identifying which assets in your IoT networks are critical then whichever ones have been assigned the most outstanding value are protected accordingly.

Manage and track IoT devices. Each new device that connects to your network represents a new security hole. That's why it is essential to understand any new devices that are connecting. The best way of doing this is to invest in software since tracking, monitoring and managing manually is next to impossible. The software can automate this process which gives you a better understanding.

Utilize the latest security protocols. Data that isn't encrypted is vulnerable to cyber-attack. That's why you need to use encryption protocols to encrypt any information coming or going from IoT devices.

Evaluate patching and remediation. Occurs when connected devices have their code changed to improve security. Some devices are too complex for a complete patch. In that case, you will think twice about incorporating them into your network.