SHRINKING THE CYBERATTACK SURFACE BY HARDENING IOT SYSTEMS

VIAKOO

(650) 263-8225 | sales@viakoo.com | viakoo.com

Introduction

If the data isn't already at hand, ask your IT manager how often someone tries to compromise your website or information network. Chances are, it's in the range of several hundred times each and every day. For the largest companies and most active websites, the number can reach 100,000. That is, on average, more than once every second.

If these numbers are not sobering, also consider that datacenters and IT equipment is not where hackers are typically starting their attacks. All too often, it's ancillary systems like HVAC, physical security, and others that provide welcoming points of entry to a corporate network. These IoT (Internet of Things) devices interconnect with others in such a way that there may be additional vulnerabilities that are not obvious to your IT teams. Attackers are aware of these vulnerabilities, and working quickly to exploit them and gain access to information networks through the relatively unprotected IoT devices.

This paper reviews some of the potential vulnerabilities in your IoT systems' security and discusses hardening methods that can be employed to bolster your defenses. Understanding these issues, and ensuring that countermeasures are in place, is a matter of some urgency – you might have had a dozen cyber-breach attempts, or more, in the time it took to read this introduction.

Part I: IoT Vulnerabilities

DIGITAL SYSTEMS PROVIDE BENEFITS AND RISKS

In recent years, many systems and devices have moved towards digital formats and IP connections. Digital systems provide key advantages for users – for example, many can now provide basic analytics functions at the edge, and can generate metadata to support enhanced performance, service assurance, and other advanced functions. Once deployed, IoT devices are often left unmanaged, as they typically are not supported by IT and the specific organization using them (e.g. physical security, facilities, and other Operational Technology teams) are not staffed or trained in maintaining digital devices.

Importantly, a large part of the value derived from IoT devices from the user point of view is the ability to interconnect them with IT, manufacturing, identity, and other systems, and to connect them to the internet-based services. Interconnection between systems provides for additional management and information functionality. For example, access to sensitive IT resources can be made dependent on successful multifactor verification in the access control IoT system, within the expected working hours in accord with HR databases. That is, someone could be granted access to sensitive information only within their normal working hours, and after they were confirmed to arrive at the office that day. In theory, for example, this would prevent a coworker from using someone else's password after normal working hours to access unauthorized documents – a level of control that was not possible without these interconnected digital IoT systems.

And, connecting these systems over the internet infrastructure enables managers to access information and take actions remotely – an enormous benefit that is almost taken for granted in today's mobile environment.

The trouble with these developments is that by making it possible for managers to access their IoT systems from anywhere, and interconnecting them to allow for enhanced management and information functionality, if not architected and managed securely, companies can simultaneously expose themselves to hackers and intruders.

Today, many IoT system elements are networked, making them reachable through a network, and also, if not architected securely, can make each of them a possible entry point for attackers. These vulnerable IoT points include networked video cameras and video recorders, printers, VOIP, switches and transmission devices, access controllers, card readers, and keypads, badge printers, among many others.

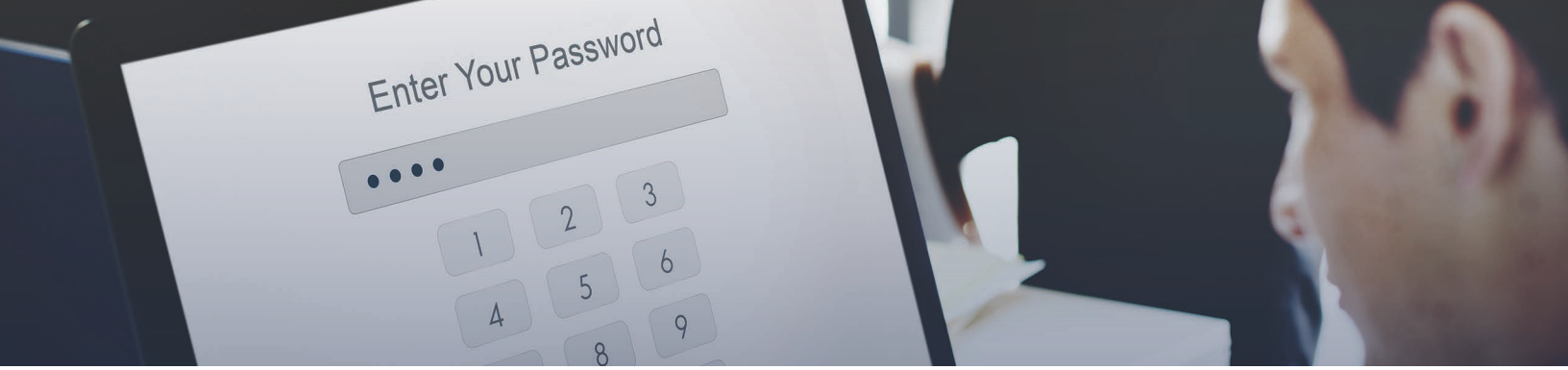
VULNERABILITY IS 'BAKED IN'

Moreover, the nature and the reality of the situation often makes addressing these vulnerabilities more difficult. For example, many installed IoT systems are made up of devices from multiple suppliers. And, few companies installed all their systems at the same time; instead, systems were installed, upgraded, expanded, and replaced over time, as needed. As a result of both of these factors, essentially many installed IoT systems are both "multi-vendor" and "multi-generational" – a situation that cannot be changed under any reasonable circumstances. Any solution that would strive to improve cyber-resilience for such systems would have to span across all networked devices and account for wide ranges of functionality, scale, and complexity.

Part II: Hardening IoT Systems

As challenging as the situation seems, companies have little choice other than to put up a fight when it comes to blocking potential cyber attackers. Fortunately, there are straightforward steps that can be taken to harden interconnected and networked IoT systems, reducing vulnerabilities and the likelihood of a successful attack. These recommendations are based on an extensive set of cybersecurity best practices, as well as the recommendations of applicable standards bodies.

For convenience and clarity, the recommendations are organized by type, not necessarily by priority or importance. Evaluate the specifics of your circumstances to determine which steps are needed and in what order to prioritize them to support your business needs.



1. Staff

a. Provide ongoing security awareness and education as most vulnerabilities are actually from within an organization, whether accidental or intentional.

2. Software

a. Ensure that all software throughout the system is updated at all times, including device firmware.

b. Consider automating the checking and updating process with automated authenticity verification safeguards.

3. Passwords

a. Establish and enforce a password management policy.

b. No networked IoT devices should continue to use default passwords provided by the manufacturer.

c. Current best practices on passwords emphasizes length as a major security determinant. Longer is better.

d. Implementing periodic password changes will also greatly enhance security throughout the systems.

e. Failed login attempts, either by user names or passwords, should be limited, logged, investigated and locked out.

4. Privileges

a. Clearly define and determine the appropriate groups; differentiating between administrators, operators and users, and casual users and visitors.

b. Each group should be assigned the system rights and privileges necessary for their assigned functions, and no more.

c. VPN access should not be allowed for admin functions, diagnostics, or similar sensitive information or access.
d. Rights and privileges should be reviewed and adjusted periodically.

5. Securely Architected Systems

a. IoT systems can be securely architected so that they can have a low risk connection to the internet. Careful attention needs to be given to limit susceptibility to hacking attempts. Of course end points (IoT devices) and other access points, and links to information networks need to be programmatically managed to automatically determine all system elements and exactly what is connected to what.
b. Carefully curate all connections that support remote access.
c. Wireless devices have vulnerabilities that must be managed as they could provide an easy gateway to corporate servers. Secure all wireless devices connected to corporate networks, including cameras, locks, printers, and modems so they cannot be accessed by unauthorized traffic.
d. Implement logical separations for virtual local-area networks (VLANS) and access controls lists (ACLs) that instruct system elements to only allow access to specific authorized devices, and to deny all other requests.

6. Endpoint connections (including cameras, badge readers, control panels, security-related servers and video recorders).

a. Hackers can gain access to the IoT network by plugging into a network cable that was installed to reach an external device, or plugging into open USB ports on endpoints.
b. Port security can be used to protect against such connections by providing an additional layer of protection to restrict unauthorized devices from connecting to router or switch ports.

c. Port security makes use of the hard-coded MAC address of the authorized device, which unlike an IP address, is difficult to change. If a device is connected to a switch or router that doesn't match the registered MAC address, then the system can block access to that device and raise an alarm for follow up.

7. Improving cyber-event detectionwith automation

a. Many firms are short-handed when it comes to security. Many studies have reported on a global shortage of cybersecurity talent that is expected to continue.

b. Automated system verification tools such as those provided by Viakoo provide a powerful alternative that can provide a more consistent and better detection/alerting function to detect all types of security-related issues.

c. Automation can also check and verify that the installed firmware and software is current throughout physical security systems.

d. The most powerful solution is to programmatically check the integrity of the data streams and stored video files themselves to be sure that the system is operating as intended and that the video records are being stored as designed.

e. Automated methods of firmware, password, and certificate management should be used due to both the scale of IoT devices and the need to maintain logs for compliance and audit purposes.

Conclusion

Cybersecurity threats are a current real and present danger to any organization with networked security operations. Hardening the organization's IoT systems are a good way to reduce the risks from cyber criminals because determined attackers know that IoT devices generally have fewer cyber protections in place. The most powerful solution is an automated service assurance solution to verify that IoT systems are performing as they, so that immediate action can be taken in the case of gaps or anomalies. In addition, automated cyber hygiene solutions must be used to manage firmware, passwords, and certificates due to the large scale of such updates.

Hackers are almost certainly trying to penetrate your corporate network right now. Don't wait for them to find a weakness, take action to harden your IoT devices now.