CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

eMAGAZINE

INSIDE THIS EDITION

And much more...

JANUARY 2019

MORE INSIDE!

Technology Takeover: How to Secure IoT Environments

By Julian Weinberger, NCP engineering

Internet of Things (IoT) devices continue to transform office environments around the world. From intelligent air conditioning units and smart lighting, to digital assistants and even app-based access control, IoT is having a tremendous impact on business efficiency and productivity. Smart thermostats, for example, can learn worker preferences and automatically maintain an optimum room temperature. As a result, energy savings of up to 60% are possible.

Smart equipment is commonly used to manage everyday tasks such as lighting, booking meeting rooms and hot desking – often via an app on smartphones. Building access is also changing. Conventional keys and code locks will soon be replaced by electronic access control units that allow managers to set their own access parameters. Many of these systems can track usage over time and integrate with other systems to give an overall picture of energy usage or security.

Security Challenges

Most businesses recognize the value of their data and do whatever they can to protect it. Security technology such as a firewall, anti-virus software and network monitoring is commonly deployed to detect threats and keep out attackers. However, these security investments are easily undermined by the introduction of IoT systems. Security measures built into most IoT devices still fall short of the required business standards for protecting proprietary data.

The risk of confidential company data or personally identifiable information (PII) being intercepted by unauthorized parties is extremely high. Symantec found that the number of attacks on IoT equipment rose by 600% last year. Concerned that businesses may be opening themselves up to targeted cyberattacks, the FBI released new advice to help recognize when IoT equipment is compromised and how to mitigate the effects. According to a recent public service announcement from the FBI, “Cyber actors actively search for and compromise vulnerable Internet of Things (IoT) devices for use as proxies or intermediaries for Internet requests to route malicious traffic for cyber-attacks and computer network exploitation.”

Unfortunately, there is no obvious way of knowing when IoT equipment has been compromised. The only option is to regard any

sudden changes in network activity as suspicious. Suspicious activity can include an unusually high uptick in monthly broadband usage, rising Internet bills, a drop off in network performance, anomalous Domain Name Service (DNS) queries or data syphoning off to unfamiliar destinations. As cyberattacks remotely probe devices for weak points, it's important to know if all IoT devices in the office – from CCTV and thermostats to routers and smart building access devices – have the latest firmware updates, robust authentication measures, and strong passwords in place. Network separation of IoT devices is one of the best ways to keep IoT devices away from any of your regular IT infrastructure.

Defense-in-Depth Strategies

To reduce the risk of IoT security compromises, there are many elements to consider. Companies should keep IoT equipment as self-contained as possible so that it is isolated from the main business network. Firewalls should also be set to block traffic from unrecognized IP sources and to disable port forwarding. Another precautionary measure is to switch devices off and on again at regular intervals in order to remove any malware stored in the device memory.

Perhaps the most effective way to mitigate cybersecurity risks is to secure IoT devices with a virtual private network (VPN). A VPN encrypts all traffic entering and leaving IoT devices, rendering the data unintelligible to anyone trying to intercept it. A professional, enterprise grade VPN typically uses military-grade encryption and can manage deployments comprising many thousands of IoT devices remotely.

An example of a common assault against IoT equipment is a distributed denial-of-service (DDoS) attack. A DDoS attack is a malicious attempt to disrupt the normal operation of a digital device by bombarding it with an overwhelming amount of Internet traffic or hacking the IoT device to make it a part of a DDoS attack. VPNs help protect against this kind of attack by shielding the IP address by replacing it with a proxy address. Many other endpoints with the same VPN service will share the same proxy address. This makes it much harder for cyber criminals to pinpoint any individual target device. An IP address shielded in this way also stops intruders being able to track user activity. It also reduces the number of available attack vectors, helping IT support teams to focus defense efforts and increase the chances of malicious activity being quickly detected and stopped before any harm is done.

In summary, government authorities remain concerned about the vulnerability of IoT devices in the workplace. After all, as soon as an IoT device goes live on the Internet it becomes susceptible to viruses, malicious programs, or hackers. Although the FBI issued advice on what to look for and how to mitigate IoT attacks, ensuring that IoT devices are completely protected requires a multi-layered security strategy. A virtual private network is an essential part of a company's defense-in-depth strategy to protect data in IoT environments. As VPNs encrypt and protect the IoT data as it travels from device to platform, attacks are either repelled or the data is completely indecipherable to any outside party that intercepts it.

About the Author

Julian Weinberger, CISSP, is Director of Systems Engineering for NCP engineering. He has over 10 years of experience in the networking and security industry, as well as expertise in SSL - VPN, IPsec, PKI, and firewalls. Based in Mountain View, CA, Julian is responsible for developing IT network security solutions and business strategies for NCP.