INTERNET OF THINGS SECURITY FOR SMALL AND MEDIUM ORGANIZATIONS

OCTOBER 2019 ITSAP.00.012

WHAT IS THE INTERNET OF THINGS?

The Internet of Things (IoT) refers to the network of everyday web-enabled objects that can connect and exchange information. These "smart" objects include more than your computer, smartphone, or tablet. They include items like personal fitness trackers, TVs, thermostats, or cars. This list of IoT devices is continuing to grow. IoT Analytics[1] projects that there will be a 39% increase by 2025 in the global market of IoT devices. Understanding how to securely use IoT devices in your organization is increasingly important.

HOW DOES THE IOT WORK?

IoT devices require little to no input from you after their initial set-up is complete. They have embedded sensors, electrical components, and software that collect data and information from their surroundings. The data is sent over the Internet to the cloud for processing, where it is shared with other network-connected devices through Bluetooth or Radio-Frequency Identification (RFID) technologies.

HOW WILL THE IoT CHANGE AN ORGANIZATION'S WORKFLOW?

IoT devices make routine tasks and processes more efficient and convenient, saving time so that employees can focus on other priorities. For example, you might use a mobile payment device attached to a smartphone for a simple, portable payment method.

By using IoT devices, your organization can save money. For example, the use of automated heating and cooling management systems saves energy and reduces the cost of utilities.

WHAT ARE SOME EXAMPLES OF ORGANIZATION-RELATED IOT DEVICES?

When you look around your workplace, IoT devices might not always be obvious at first glance. Examples of IoT devices include:

- Teleconferencing equipment
- Smart boards
- Smart speakers and other voice-activated devices
- Building fobs or access cards
- Equipment sensors
- Smart meters (e.g. electrical and water meters)
- Motion sensors and air sensors
- Security cameras
- Corporate vehicle fleets
- Multifunction devices (MFD) (e.g. printers, fax machines)
- Smart appliances (e.g. kettles and fridges)
- Point of sale (POS) systems
- RFID tags on products to track inventory
- Building control systems (e.g. HVAC, electrical, water)
- Corporate mobile phones and portable IT equipment
- Smart watches or fitness trackers

Note: Allowing employees to bring their own smart devices to work can introduce more security risks.

WHAT ARE SOME OF THE RISKS TO AN ORGANIZATION?

Current IoT devices have a low degree of IT security control and weak encryption capabilities, leaving devices vulnerable to potential threats. Threat actors can take advantage of device vulnerabilities, such as in the following examples:

- Compromising environmental control systems and smart appliances (e.g. coffee maker, building heating and electrical) in physical workspaces could lead to profit losses (e.g. tampering with temperature controls in a server room, causing equipment malfunction)
- Gaining unauthorized access to company building security controls (e.g. unlocking doors, viewing surveillance cameras)
- Taking control of MFDs to maliciously disrupt Internet access (e.g. Mirai botnet attack)
- Accessing microphones remotely on IoT devices to listen in on sensitive conversations
- Taking control of a car's features (e.g. tampering with a vehicle's brakes)
- Controlling a hospital's medical equipment (e.g. interfering with magnetic resonance imaging [MRI] systems)
- Accessing sensitive data or personal information (e.g. customer names and credit cards) through unsecured IoT devices that are connected to company networks

HOW CAN I KEEP IOT DEVICES SECURE?

Before introducing IoT devices into your organization, you should research security protocols and understand the types of data that the devices send and receive. As more IoT products are brought into the workplace, your organization needs plans and policies to minimize the possibility of cyber security incidents on your network. Your plans and policies should address the following considerations:

- Restricting personal IoT devices to connect to a separate network (e.g. guest Wi-Fi)
- Changing the default passwords on IoT devices. If password rules allow, use passphrases, rather than passwords, on all IoT devices in the workplace
- Using two-factor authentication for devices or apps to add an extra layer of security
- Ensuring data generated by IoT items is encrypted
- Turning off any automatic connection functionality (e.g. plug and play)
- Applying security patches and updates to IoT devices (if the product allows)
- Monitoring, detecting, and correcting any IoT security issues
- Researching reviews and security ratings on manufacturers and products

WHAT SHOULD I REMEMBER?

IoT devices can help your organization find efficiencies in workflows and processes, but there are cyber security issues that come with using these devices. If used in the workplace, employees may have privacy concerns if their movements and work activities are monitored by smart technology.

Your organization should implement policies to ensure IoT devices are introduced, used, and managed securely.

REFERENCES:

[1] IOT ANALYTICS. *State of the IoT 2018: Number of IoT devices now at 7B—Market accelerating.* August 2018.

Need help or have questions? Want to stay up to date and find out more on all things cyber security? Come visit us at Canadian Centre for Cyber Security (CCCS) at **cyber.gc.ca**