IBM Security

Five indisputable facts about IoT security

Some concepts have long been accepted as universal truths. Among the most familiar of those: Sir Isaac Newton's laws of motion, which date back to the 17th century. Today, however, there are new principles defining how technologies will behave in specific situations. For example, the proliferation of Internet of Things (IoT) devices has generated serious concerns for IT security. And that's led us to identify five indisputable facts you need to know about IoT security.

1 Devices will operate in hostile environments

Unlike the mobile phones, tablets and laptops we use and carry with us virtually every day, IoT devices often operate without human supervision. So it's important that IoT devices, such as remote office temperature controls, must be both rugged and resistant to physical tampering. At the same time, they need to be able to recover from an attack and fail safely by degrading to an acceptable processing level—all without requiring human involvement. While cognitive security solutions can handle many threats and attacks, administrators of IoT deployments also need the visibility and control to deal with exceptional situations.

2 Software security will degrade over time

All software in use must be kept updated. And when it comes to IoT sensors and devices, the patching process typically takes place in very distributed, highly uncontrolled environments—at an enormous scale. But even if all known vulnerabilities are addressed with the first release, new exposures and vectors for attack will almost certainly be discovered. The risk of attack increases with the length of time the equipment remains in service. That means system defenses will need to be updated repeatedly—for the life of these devices—impacting the supply chain for both software and equipment.

3 Shared secrets do not remain secret

A sizable number of IoT devices come preloaded with identical credentials across multiple devices. Although these default credentials should be changed by users before the devices are made operational, they're often left as is. Default secrets aren't secret. Attackers can use them to take over such devices for unintended purposes, making them vulnerable to sabotage or disruption. By delivering devices that prompt for a mandated password change upon first use, however, manufacturers can help ensure that default credentials can't persist—and that secrets will remain secret.

4 Weak configurations will persist

The default configuration of an IoT device will usually remain in place because it takes thought and effort by users to change it. If the default settings for a given device have access control turned off, for example, it's left up to the owner to take measures to improve that security. Instead, security options should be enabled either by default or as part of an initial setup process, so that users are required to make a conscious decision to remove the default protections.

5 As data accumulates, exposure issues will increase

One of the key business drivers for IoT is the data that's generated from devices and solutions. That puts the spotlight on data security—along with how it's created, used and deleted. Over time, connections between different, seemingly disparate datasets may emerge. IoT devices are accumulating massive amounts of personal and sensitive data, including everything from audio recordings and transcripts to GPS locations and heart rate readings. If the data isn't managed, secured and destroyed when it's determined to be worth less than the risk of holding on to it, the results may lead to loss of privacy and to issues of data ownership—all of which increase the importance of partnering with IoT vendors and solution providers who can be trusted with your data.

Get the facts about what you can do

To learn more about how IBM can help your organization create a more secure environment for taking advantage of IoT technology, visit: **ibm.com/**IoT/security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2017

SEF03018-USEN-01