Highlights from webcast on IoT Security

UEM AND IOT: THE SUM IS GREATER THAN ITS PARTS

Based on a webcast featuring Tim Warner, an Author Evangelist with Pluralsight and Ken Galvin, Senior Product Manager, KACE

chombosan / Shutterstock.com

Although PCs were once the computing device of choice in the workplace, today's organizations leverage a seemingly endless array of traditional computing, mobile, and IoT devices. The proliferation of non-traditional devices has broken long used inventory and asset management systems, which are ill equipped to deal with devices other than PCs. This is especially problematic given that these non-traditional devices introduce new security risks, while also complicating an organization's compliance initiatives.

In a recent webcast, Tim Warner, an Author Evangelist with Pluralsight, explained that Internet of Things (IoT) is a broad term referring to a huge variety of network enabled devices that take readings through an analog sensor, and transmit those readings over the network. IoT devices have become widely used as a way of monitoring HVAC equipment, medical devices, and security cameras. Warner also explained that IoT devices are used in factories and in agriculture.

In spite of the tremendous benefits that these devices provide, there are also disadvantages associated with their use. According to Warner, "every rose has its thorn, as the great 80s hair band Poison used to sing." One such "thorn" is that connecting an IoT device to a network can introduce security risks. Warner illustrated this point by showing a Website called Shodan.io. "It's a fascinating site, and it's also a frightening site, because this is essentially a search engine that lists publicly accessible IoT devices such as security cameras, network printers, HVAC systems and home security systems." Warner went on to explain that you can use Shodan.io to search for your own devices and find out if they are being accidentally exposed to the Internet.

The vulnerabilities introduced by IoT devices vary by device type. Devices such as tablets, VoIP phones, and wireless printers have the potential to cause data leakage. Not all avenues for data leakage are directly tied to network exploits. In the case of a network printer for example, "Somebody comes by and there is a payroll statement that somebody printed and forgot to pick up."

IoT devices can present other types of vulnerabilities as well. Audio assistants could conceivably be used to record conversations. "Smart TVs can be taken over" and "enlisted in a botnet army to perform DDoS attacks on others." Of course these are just a few examples. Any device with an IP address could potentially be compromised. Some of the other reasons why IoT devices are potentially dangerous include:

- Lack of industry standards
- Weak default settings
- Inconsistent updates

- Invisible vulnerability (you may not know that the device is online)

The bottom line is that the security risks posed by IoT devices drive the need for a User Environment Management (UEM) solution. “If you don’t have a UEM solution in place you may not know all of the devices that are online in your environment, and how many if any may have already been compromised.”

> “If you don’t have a UEM solution you may not know all of the devices that are online in your environment, and how many may have been compromised.”
>
> *—Tim Warner, Pluralsight*

There are several things that organizations should look for in a UEM solution:

- A robust discovery engine
- Asset management capabilities
- Centralized administration for command and control of devices
- Threat intelligence
- File protection and encryption
- Patch management capabilities
- No dependence on agents

At the conclusion of Warner’s presentation, Ken Galvin, Senior Product Manager for KACE gave a presentation on unified endpoint management. Galvin explained that the KACE unified endpoint management solution has united mobile and client management into one pane of glass, and now you can review all of your assets under one console.

One of the pain points that organizations are dealing with today is that they have to perform comprehensive management of various types of systems. In the case of Windows desktops for example, “you’ve spent a lot of time putting together group policy, you have to worry about patching, you [also] do scripting and software distribution” as well as software license compliance and asset management. Of course, these are just a few of the many different management tasks associated with PCs. At the same time, organizations also have to perform management on Windows and Linux servers. There are also non-computer devices to manage, such as “printers, projectors, network devices, universal power sources, embedded point of sale machines, point of service machines, electronic signage, Raspberry Pi [small single-board] based IoT devices, medical devices, and so on.”

Galvin went on to explain that the more endpoints an organization accumulates, the larger the risk to the organization’s security. In fact, there are 80,000 new malware variants created every day, and 323,000 new malicious mobile programs have been recently activated. Of course, a higher security risk also means a greater potential impact to the business. This impact can be catastrophic, the average cost of one data breach is currently $3.8 million, and the average cost of compromised data is $222 per record.

KACE seeks to mitigate these risks by taking a truly unified approach to endpoint management. The company’s goal with SMA 9.0 is to eliminate artificial barriers between mobile and fixed asset management, and to transition from device focused to user focused management. The KACE solution is designed to be easy to use, and can be fully operational in weeks (not months) with no need for extensive professional services to get started.

KACE’s UEM solution is based around a series of applications and appliances, which include:

- **KACE Systems Management Appliance** – KACE’s most comprehensive systems management solution, which streamlines asset management, while also improving security.
- **KACE Systems Deployment Appliance** – Provides initial provisioning and ongoing administration of master system images and driver updates
- **KACE Asset Management Appliance** – Provides comprehensive hardware and software inventory and asset management across a variety of operating systems
- **KACE GO Mobile App** – Provides a streamlined workflow for trouble tickets, which can be submitted from a mobile device.
- **KACE Cloud Mobile Device Manager** – A cloud based solution that when used with the KACE Systems Management Appliance, provides a comprehensive, single pane of glass view of traditional and mobile devices.

In addition, KACE offers KACE as a Service, which is a cloud based solution for the comprehensive management of all network connected devices.

SPONSORED BY:

Quest™

For more information:
www.quest.com/kace