How to Secure Your Devices in a Machine-to-Machine World

Peter Holmelin, VP of Development, Netop

What the 'Internet of Things' means for your company.

If you mention connectivity, most people think of smartphones, PCs, web TVs, web cams, and the Internet. But soon, these devices will make up only a small proportion of the machine-to-machine (M2M) connected world. With the number of M2M devices set to balloon over the next few years, there are some serious security ramifications for businesses.

Big Data Collection Starts Here

Around the world there are countless smart devices that have sensors, are connected to the Internet and are sending information somewhere. If you haven't heard it before, the term the "Internet of Things" will soon become commonplace and the "things" it describes are those very devices.

These M2M smart devices will be the "front line" for data capture, with the Internet becoming more a transport mechanism than the core of connectivity. The data could be anything from a coffee machine reordering coffee beans to a, a smart utility meter sending data to the accounting department to a sensor feeding temperature data into a building safety system. This is the first stage in the capture of Big Data, in which M2M devices will be key.

Millions of Devices Means Millions of Access Points

While all this connectivity will speed information gathering and response times, and increase efficiency, a potential downside is the impact on security. Each connected M2M device represents a security risk through the millions of new "attack surfaces" now available.

Perimeter security will no longer be enough, because the perimeter won't be nearly as easy to define. Before, online attacks were directed at a limited number of computer ports. In the near future, billions of M2M devices will be connected to each other as well as the corporate network. Each one can be hacked and used as an entry into the rest of the corporate network.

To make an analogy, Bring Your Own Device currently presents a similar but lesser threat. In BYOD's case most of the devices are known (smartphones, tablets, PDAs and smart TVs) and there are much smaller numbers involved than the predicted numbers of M2M smart devices. But even with these lesser numbers, BYOD is a significant security concern. Imagine the threat posed by billions of unknown M2M connected devices. After all, a person may have a few smart devices but eventually many organizations will have millions of smart devices.

Securing Remote Devices

To make a smart device smart, "intelligence" is bestowed via an embedded module. Embedded modules use powerful processors to do increasingly complex tasks that require more code. The more code there is, the more opportunity a hacker has to access that code and take control. As a result, there will be a growing need for sophisticated encrypted communications links in addition to the already existing individual device and central systems' protection.

Regulations around M2M devices are non-existent or still being developed and the predicted proliferation of smart devices has yet to become reality. And with some analysts predicting 2.1 billion M2M devices in use by 2020, regulating them will become a greater necessity. Still, there are some mart steps to take to start securing M2M smart devices:

- Prepare systems to support unique and emerging technologies and devices.
- Implement security measures that enable the organization to centralize controls, integrate with existing corporate policies and adhere to compliance requirements;
- Ensure that M2M devices are equipped with remote control technology and properly monitored and maintained; and
- Require robust logging and reporting capabilities, so that the organization can perform session audits.

Securing the Organization without Compromising the Business

To sum up, over the next few years M2M smart devices will grow significantly in number and will form a critical component in many organizations' networks as companies try to become more efficient reduce costs.

While adding to an organization's performance, these devices will also present a threat that will need to be addressed. And as M2M data becomes an integral part of an organization's management information system, solution providers will need to be ready to adopt security solutions to address the issues. Despite the risk, there are also significant benefits to be had. The millions of bytes of information these devices will collect will form the beginnings of the building blocks of Big Data, the next step in the future of corporate information analysis.

For more information visit www.netop.com [1].

Source URL (retrieved on *05/18/2013 - 3:44am*):
http://www.wirelessdesignmag.com/blogs/2013/02/how-secure-your-devices-machine-machine-world?qt-blogs=0

Links:
[1] http://www.netop.com