Five IoT security risks and ways to secure yourself

By Yana Vardomatskaya

21 Apr 2017

It is expected that there will be 3.9 IoT (internet of things) based devices per person by 2020.

© My Make OU via 123RF

By putting together the operational technology (OT) and information technology (IT), unstructured digital information that is generated by the connected objects (gadgets, tools, devices) can be examined for improvements without immediate human interaction. However, along with all the potential improvements, the potential rise of smart nodes and transferring of data is causing new concerns about online privacy, anonymity, and security.

Reasons why security protection is an issue

Being put into the internet environment means that any device's system unavoidably comes up against multiple online threats. Any connectable device is supplied with an embedded operation system, which is not primarily designed with stringent protective built-in technologies. In view of this, having decided to use IoT, any customer should think about the security issues:

1. DDoS attacks

After being attacked, IoT-based devices can be controlled from one server, which allows an adversary to use them to overwhelm a website with traffic coming from multiple 'zombified' gadgets. Any confidential business content or database can be leaked from the compromised website and misused in the wrong hands. The DDoS attack that targeted Brian Kreb's website in 2016 is one of the most vivid examples of how the IoT can work against you.

Ransomware: more than just file encryption [part I]

Doros Hadjizenonos 6 Apr 2017

2. Deadly vulnerabilities

We already know that the IoT system has achieved wide acceptance in the industrial sector, notably related to energy and nuclear facilities. It needs little imagination to think of the consequences if an adversary finds breaches in the devices' OSes and starts changing internal settings in these facilities.

In the medical sector, devices such as insulin pumps, x-ray systems, CT-scanners, and implantable defibrillators were found to contain deadly vulnerabilities in 2016 by the Symantec Global Intelligence Network.

3. A flood of data

Having armed a business with the IoT, the enterprise could well encounter problems with the heavy load of traffic, which needs to be collected, processed, stored, and analysed. As a result of the increased data flow, the needs for increased or limitless bandwidth will grow.

Besides additional expenses for network maintenance, a company needs to monitor the traffic. Moreover, the enterprise needs to be aware that there are malicious and legitimate data patterns passed to IoT devices. The companies should secure their network by identifying malicious activity and eliminating the problem.

4. Lack of hardware and software protection

Protection should be present for each component of the IoT system, as in most cases hardware is not initially stuffed with military-grade defensive technologies and often the built-in tools are out of date. To gain better control over any internet-connected device an attacker will look to compromise a chain of IoT-based gadgets by trying to implant a malicious code or infect one of the OSes for further distribution.

5. Smart home devices' vulnerabilities

Millions of homes now suffer from cyberattacks. More than 50 commercial devices (smart light bulbs, locks, energy management devices, etc.) have been found to include dozens of vulnerabilities. Thus, a 'smart' door lock can be opened remotely without a password – an ideal opportunity for some robbing.

How to secure your IoT

The main issue is that IoT should be created with security in mind and any customer should follow a holistic approach for IT security. Regardless of the fields of the IoT usage, the protective measures are the same:

- Any connected device needs to be supplied with effective security layers that include code signing, authentication, and on-device security measures. For identification and traffic protection you should opt for SSL/TLS encryption technologies.

- Advanced companies offering customised IoT development should protect their software with a built-in VPN. The

private network establishes a secure tunnelling run with the help of up-to-date protocols, such as OpenVPN, L2TP/IPSec, etc, and long-term bit-keys, which make all the traffic routed from a connected device to a VPN server encrypted and therefore sheltered from interception, misusage, and surveillance.

- When used for a corporate network, a VPN gives much broader possibilities for web threats prevention including protection of all sensitive data, bypassing geo-restrictions and shifting authentic addresses.

- Security-concerned customers can isolate the IoT-based devices to their own vLAN, which practically excludes a chance of virtual unauthorised accessing.

- As strange as it might sound, many companies fail to undertake regular and well-timed updating of their anti-virus software, which inevitably leads to system infections.

- You can also subscribe for additional services that provide security for IoT. Such services as Bitdefender BOX, for instance, offer a piece of hardware that protects every connected device in your network. Due to a regular scanning for weaknesses and backdoors, as well as having bad websites and network access control undertaken by the hardware, you won't need to install any other protective software.

- All communication of IoT-based devices on a network should use SSL certificates, which protect the master of the chain devices from attacks.

The numerous spheres of successful implication for IoT, such as environmental monitoring, infrastructure, energy and medical systems management, offer strong grounds for assessing that the technology has already brought plentiful positive results and has become a part of our daily life. However, this rapidly evolving area requires some protective efforts to be taken. So, don't wait until you are caught off guard, take steps to ensure that your IoT devices are secured.

ABOUT YANA VARDOMATSKAYA

Yana Vardomatskaya is a VP of Business Development for HQSoftware, a custom software development company with offices in New York City, Tallinn and a development centre in Minsk, Belarus. Having started with a wide variety of custom software development projects, the company is now working in IoT and AR/VR.
- Five IoT security risks and ways to secure yourself - 21 Apr 2017

View my profile and articles...