INTERNET OF THINGS: WHAT ABOUT THE SECURITY OF THINGS?

Ревуцький Микола Вячеславович,
Київський національний університет технологій та дизайну
Науковий керівник – к. пед.н. Гальченко О. Ю.

It is easy to get excited about all the new gadgets that the era of the IoT has delivered, but it is important to take a step back from all the excitement to address the issue of security. In recent years, the IoT has experienced exponential growth, fuelled by decreasing costs in computing, a proliferation of mobile devices, ubiquitous connectivity and the rise of cloud computing. Last year saw a rapid increase in the number of commercial rollouts of IoT-enabled projects, and the unveiling of business models and services that didn’t exist previously.

Today, IoT is already branching out into commercial networks as well as enterprise applications. Smart devices are becoming more commonplace in our households with everyday appliances now able to communicate with the internet to help our lives to run more smoothly and interconnected devices are now essential tools in our working lives as well. This is all fantastic news…right?

Infosecurity experts have long warned that IoT devices are set to be a security nightmare as they are often deployed with little or no consideration for security. The question is: are enough people aware of this and are the right security measures being taken, particularly by organizations that need to protect business critical and sensitive data? In its early days, the World Wide Web brought with it little protection from misuse. This, of course, generated consumer distrust, consequently slowing down initial e commerce efforts. This is in no doubt due to the fact that today data encryption and other security measures are simply assumed. People no longer fear sending their credit card information over the wire. As a result, security issues for the most part are kept in the background.

It almost seems as though we are in a cycle in which consumers and organizations blindly trust companies with their valuable data and it is only when a case of known and reported intrusions arises that action is taken and data security is examined.

This, in some respects, also echoes the initial response to the cloud, which saw low user adoption for the first few years due to security worries around the security of the data being stored offsite. It has been found that most of the IoT devices that have been hacked to date have had default usernames and passwords, and at no point had the manufacturers prompted users to change these.

The overwhelming majority of modern security solutions — encryption, firewalls, two-factor authentication, tokens — target data confidentiality, erecting barriers against unauthorized access. But machines, their communications protocols, software, rules and exposed APIs will always have vulnerabilities.

Recent distributed denial of service (DDoS) attacks such as that experienced by the DNS provider, Dyn – which made it impossible to access the likes of Twitter, Amazon and Netflix – should be a serious wakeup call.

Increasingly, hackers are able to use malware software to scour the web for devices that have basic security and detect vulnerabilities. This enables the hackers to upload malicious code so that the devices can be used to attack a targeted website. What is really worrying is that the owners of the IoT devices are usually unaware of the attack. This is because once a device has been hijacked it can be impossible to tell as they often continue to work exactly as normal.

Issues will then begin to occur behind the scenes when the compromised system is subsequently put on the same network as personal computers, corporate servers and even confidential government data. The main issue is, without knowing which devices exchange data within a specific network or the internet as a whole, there is no way to develop an adequate security strategy.

In theory, every single device that is being added to a network needs to be evaluated, but this is just as painstaking as it sounds. Whether it is the IoT or the cloud, companies need to begin using security technologies and procedures that have already been proven to be reliable.

This means applying on premise levels of IT security to cloud workloads. For example, two factor authentication, role based access control, encryption, and vulnerability scanning can enable a protective shield for the cloud to scan all incoming and outgoing data for malicious code, regardless of the device being used.

The right level of security technologies embedded into the cloud platform allows companies to gain control of all web based traffic in order to actively manage which communications should be permitted and which should be blocked.

Recent high profile cyber attacks and, increasingly, ransomware threats have spurred a long overdue discussion about the gaps in IoT security. Unless the security side of IoT is sorted out, it could hold back wider adoption of the technology.

Early adopters beware; the best advice is to follow the data. Know how the company behind your latest gadgets and interconnected devices handles security and ensure that any cloud provider is able to provide you with the reports and ongoing visibility that will enable security settings to be managed and maintained.

СПИСОК ЛІТЕРАТУРИ

1. Teri Robinson, SC Magazine US (04 Nov 2016) IoT Security Let's do this thing;

2. Jim Martin, PC Advisor (Mar 2016) Tech in 2016: Why we’re excited about the year ahead;

3. Mike Gault, TechCrunch (May 6, 2016) Rethinking Security for the Internet of Things;

4. Tara Seals, Infosecurity Magazine (16 Mar 2017) Hyperconnectivity and IoT Set to Radically Disrupt Cyber by 2019;