Myth №5 Programmers are strange people

Is that because of their clothes, which don`t include a tie and a T-shirt. I may agree that those who are engaged in development – are often introverts, so they quietly do their work and can seem to someone strange.

Display, if I may say so, some special technological or behavioral type – "programmer", it is impossible, but probably not need is those stories that are probably of films about hackers.

Scientific supervisor: Denisenko N.G.,
Senior Lecturer

UDC 004.056.5 (043.2)

Voznyuk O.V.
National Aviation University, Kyiv

THE INTERNET OF THINGS SECURITY CHALLENGES

Nowadays The Internet of Things (IoT) is rapidly covering entire societies enabling to advance each individual and business and creating significant opportunities for enterprises in order to invent new services and products and offer increased convenience to their customers. The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. In addition, according to researchers the Internet of Things is becoming a growing enterprise threat taking into account a tremendous number of electronic devices which will be connected to the Internet in the nearest future. The most meaningful six IoT security risks as well as recommendations to organizations how to prepare for the security challenges and implement an IoT policy are listed and described in this paper.

1. Disruption and denial-of-service attack. It will be important to provide constant availability of IoT-based devices to avoid disruptive attacks, such as distributed denial-of-service attacks, interruptions to enterprise services and possible performance failures. This will demand the enterprise to enforce physical security measures preventing unauthorized access to devices outside of security area.

2. Understanding the vulnerability complexity. To decrease the risk, any project associated with IoT devices must be created with security approach, and should include security controls, offering a pre-designed security model. It's necessary to keep in mind the growing danger which many IoT devices can cause as these devices may have hardware and software platforms that enterprises have never used before and, consequently, the types of vulnerabilities may differ from those they have dealt with earlier.

3. IoT vulnerability management. An efficient way of patching IoT device vulnerabilities is considered to be another serious challenge for businesses in an IoT field. This requires enterprises to create a compliance team for testing and scanning configuration settings to identify any types of vulnerabilities they have, control the elimination of operational vulnerabilities found and certify that the device can be produced.

4. Detecting and implementing security controls. The factors of identifying the need of security controls for emerging IoT devices and further implementing high-profile controls are supposed as significant ones in the IT world taking into account the abilities of enterprises to manage IoT risk. In any case, organizations dealing with IoT have to detect their information security controls ensuring proper and obligatory protection of the IoT trends and involving experienced experts.

5. Fulfilling the need for security analytics capabilities. It is critical for authorized and malicious traffic patterns on IoT devices to be identified by various enterprises. Moreover, the perfect analytical tools will both detect and improve the services offered to the consumers. To get ready for these problems, enterprises must be able to develop the corresponding set of tools and processes to provide corresponding security analytics capabilities.

6. Rapid demand in bandwidth requirement. However, business continuity risks will potentially proliferate due to increased demand for the Internet. In order to provide high service availability, organizations must analyze enhancing traffic management adding bandwidth.

In particular, we can conclude that enterprise security experts must deal with updating existing security policies to ensure communication between machines, enormous data collection and multiple other uses. It will be necessary to support threat modeling for providing and maintaining primary security principal of availability, integrity and confidentiality in an increasingly developing digital world.

Scientific supervisor: Hurska O.O.,
Senior Lecture

UDC 336.764.2 (477) (043.2)

Yackubovich S.R.
National Aviation University, Kyiv

COMPOUND HELICOPTER AS A PERSPECTIVE BRANCH IN THE GLOBAL DEVELOPMENT OF AVIATION

An idea of compound helicopter is not new. Increasing the speed of ordinary helicopter became one of main problems in 60s of XIX century. In America and Soviet Russia machines that can fly faster than helicopter were autogiros. But they didn't have an engine-driven main airscrew and could not take-off vertically. So combination of maneuverability of helicopter and speed and range of airplane was only a question of time.