СЕКЦИЯ 1
ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

DEVOLOPMENT OF THE VULNERABILITY MANAGEMENT PROGRAM IN BANKING

S. Joe-Madu, A.M. Prudnik

A vulnerability is defined in the standard as “A weakness of an asset or group of assets that can be exploited by one or more threats” [1]. Vulnerability management is the process in which vulnerabilities in are identified and the risks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an organization (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the organization) [2].

The increasing growth of cyber-crime and the associated risks are forcing most organizations to focus more attention on information security. A vulnerability management process should be part of an organization’s effort to control information security risks. This process will allow an organization to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them. Only by identifying and mitigating vulnerabilities in the IT environment can an organization prevent attackers from penetrating their networks and stealing information [3].

Banks that do not maintain vulnerability management program could not comply with Payment Card Industry Data Security Standards but also place their customers and their data at risk. There are a number of techniques available to find and to eliminate vulnerabilities and offer increased level of protection of the private data. A successful and robust vulnerability management requires incorporation of various security components, the most critical of which are the risk, patch, asset, change and configuration management. Scanning a system will identify vulnerabilities and weaknesses that must then be addressed. The paper discusses the content of each component and integration of the vulnerability management program into the information security program.

NIST recommends that organizations create a group of individuals, called the patch and vulnerability group (PVG), who are specially tasked to implement the patch and vulnerability management program [4]. The paper also discusses paper the responsibilities of the PVG members.

References

1. ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls.

2. Tom Palmaers. Implementing a vulnerability management process SANS Institute. 2013.

3. Williams, A and Nicollet, M: Improve IT Security With Vulnerability Management, Gartner ID Number: G00127481, May 2005.

4. Special Publication 800-40 Rev. 3, Guide to Enterprise Patch Management Technologies (July 2013). http://dx.doi.org/10.6028/NIST.SP.800-40r3.

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗРАБОТКИ, ФОРМИРОВАНИЯ И ПРИМЕНЕНИЯ ОРГАНИЗАЦИОННЫХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.В. Безмен, О.А. Дугушкина

Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности (ИБ) с каждым годом становятся все более и более актуальными, и одновременно более сложными. Технологии обработки информации непрерывно совершенствуются, а вместе с ними меняются и методы обеспечения ИБ. Организационно-правовое обеспечение ИБ представляет собой совокупность решений, законов, нормативов, регламентирующих как общую организацию работ по обеспечению ИБ, так и создание, и функционирование систем защиты информации (СЗИ) на конкретных объектах. Организационные методы обеспечения ИБ находят