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

практическое применение в деятельности руководства и персонала конкретного предприятия, на котором планируются и проводятся мероприятия по обеспечению ИБ объектов информационной инфраструктуры. Недостаточная подготовка персонала организации, слабое знание им нормативно-правовой базы по вопросам обеспечения безопасности может стать причиной уязвимостями эксплуатируемых информационных систем. Применение организационных методов обеспечения ИБ является обязательной составляющей обеспечения ИБ любой организации.

Организационно-правовая база обеспечения ИБ разрабатывается и описывается при проектировании и создании, а также последующей аттестации СЗИ информационной системы предприятия. Государственное предприятие «НИИ ТЗИ» является одной из ведущих организаций Республики Беларусь в области защиты информации. Вот уже более четверти века одним из направлений деятельности государственного предприятия «НИИ ТЗИ» является проектирование и создание СЗИ, предназначенных для решения задач защиты информации в самых разных информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено и не отнесенной к государственным секретам, а также аттестации таких систем в соответствии с действующим законодательством Республики Беларусь.

В докладе подробно представлены основные этапы разработки и формирования документации, регламентирующей организационные методы обеспечения ИБ и сопровождающей СЗИ информационной системы предприятия на всех этапах ее проектирования, создания и аттестации.

НАВЫКИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Т.Н. Беляцкая, В.С. Князькова

По оценкам специалистов, к 2019 г. в мире будет не заполнено от 1 до 2 миллионов вакансий в сфере информационной безопасности (ИБ). Например, в 2015 г. в США было свободно около 209000 вакансий в сфере ИБ. Такая нехватка специалистов может быть причиной сдерживания развития электронного общества, в частности, электронной экономики. Исследование, проведенное компанией Intel Security, показало, что 82% всех респондентов (страны: Австралия, Франция, Германия, Израиль, Япония, Мексика, Великобритания и США) указали на нехватку знаний в области ИБ. Это напрямую приводит к экономическим затратам у 71 % респондентов, главным образом из-за большей уязвимости организаций перед хакерскими атаками, а также в связи с необходимостью оплачивать труд специалистов в сфере ИБ более высоко. Так, в указанных выше странах заработная плата специалиста в области ИБ в 2,7 раза выше средней по отрасли.

Выделяют следующие основные навыки, которыми должен обладать специалист области ИБ. Во-первых, аналитические (способность к изучению компьютерных систем, оценке потенциального риска и способность предложить возможное решение). Во-вторых, коммуникационные (специалист в области ИБ должен обучать пользователей, объясняя им важность ИБ и способы защиты персональной и коммерческой информации). В-третьих, креативность (необходимо предугадывать действия компьютерных преступников, что требует нестандартного мышления). В-четвертых, внимательность к деталям (зачастую угрозы ИБ трудно распознать, поэтому специалист в области ИБ должен отслеживать даже незначительные изменения в информационной системе, предвидя любые, даже несущественные, потенциальные проблемы). В-пятых, знания в IT сфере (и угрозы, и методы их предотвращения постоянно меняются, поэтому необходимо постоянно совершенствовать свои знания по последним решениям, законодательству, практиками и методикам в области защиты информации). В качестве основных элементов образовательной системы в области ИБ рассматривается классическое академическое образование; при этом его интеграция с практической компонентой лучше подготовит будущего специалиста. Для оценки качества подготовки специалистов в сфере ИБ, Intel Security разработала интегрированный показатель, учитывающий расходы на образование; программы по науке, технологиям, инженерии и математике; наличие дисциплин по ИБ в вузах; использование передовых практик. Наилучшие результаты достигнуты такими странами, как США и Великобритания.