УДК 004.4'242

ОСОБЕННОСТИ КОНТРОЛЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНОЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ

FEATURES CONTROL OF THE INFORMATION SECURITY INCIDENTS IN THE CORPORATE INFORMATION - TELECOMMUNICATION NETWORK

М.М. МОНАХОВА
M.M. MONAKHOVA

(Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых)
(Vladimir State University named after Alexander and Nikolay Stoletovs)
E-mail: mariya.monakhova@gmail.com

В статье представлен подход к решению задачи контроля инцидентов информационной безопасности в корпоративной информационно-телекоммуникационной сети. В основе предлагаемого подхода лежит выявление факторов нарушения технической политики информационной безопасности.

In this paper is presented an approach to the problem of control of information security incidents in the corporate information - telecommunication network. The proposed approach is the identification of factors of technical violations of information security policy.

Ключевые слова: корпоративная информационно-телекоммуникационная сеть, инцидент информационной безопасности, техническая политика информационной безопасности, система защиты информации.

Keywords: corporate information-telecommunication network, information security incident, technical information security policy, information security system.

Политики информационной безопасности (ИБ) и создаваемые на их основе системы защиты информации (СЗИ) не могут полностью гарантировать защиту корпоративной информационно-телекоммуникационной системы (КИТС). После внедрения защитных мер и средств всегда остаются уязвимые места в КИТС, которые могут сделать обеспечение ИБ неэффективным. Кроме того, могут быть сбои и отказы самой СЗИ, выявляться новые, ранее не идентифицированные угрозы. Ситуации, связанные с "замеченными" нарушениями политики ИБ и отказы СЗИ в выполнении своих функций, определяют понятие "инцидента ИБ" [1]. В международной практике разработаны нормативные документы, регламентирующие вопросы управления инцидентами ИБ. В [2] выдвигаются общие требования к построению системы управления ИБ, в частности, относящиеся и к процессам управления инцидентами. Документ [3] описывает инфраструктуру управления инцидентами в рамках циклической модели процессов Шухарта-Деминга – модель PDCA. Стандарт [6] описывает аналогичную PDCA модель как основу функционирования всех процессов системы управления ИБ. Даются подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса. Стандарт [4] основной упор делает на организацию работы CISRT – подразделения, обеспечивающего поддержку предотвращения, обработки и реагирования на инциденты. Вводится ряд критериев, на основании которых можно оценивать эффективность данных сервисов, приводятся процессные карты. Сборник "лучших практик" по построению процессов управления инцидентами приведен в [5]. Подробно разбираются вопросы реагирования на разные типы угроз, такие как распространение вредоносного ПО, НСД и другие. Документ [3] определяет формальную модель процесса реагирования на инциденты ИБ.

Для настоящей работы принципиально то, что подходы, приведенные в [2…6], описывают процедуры управления – менеджмента инцидентов, не затрагивая технических вопросов. Из данных публикаций непонятно, каким образом практически обнаружить инцидент, какие события могут быть причинами инцидента, не конкретизированы понятия "нарушение политики безопасности" и "неизвестная ситуация". Далее будем рассматривать ряд функций менеджмента инцидентов, связанный только с техническими вопросами контроля инцидентов в КИТС.

Политика ИБ КИТС [7] представляет собой систематизированное изложение целей и задач защиты, как набор правил, процедур и практических приемов обеспечения ИБ, которыми руководствуется организация в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения ИБ в КИТС. Для конкретной КИТС политика ИБ зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д. Анализ руководящих документов в области технической защиты информации, стандартов и "лучших практик" [8…15] построения Политики ИБ корпоративных сетей позволяет выделить ряд структурных и функциональных особенностей, принципиальных для предлагаемого подхода:

А. Стратегия и тактика построения СЗИ (Политики ИБ) определяется через защитные функции (ЗФ): предотвращения причин возникновения угроз, их (угроз) сдерживания, обнаружения, предупреждения

воздействия на элементы КИТС проявившихся угроз, обнаружения воздействия необнаруженных угроз и устранения обнаруженного воздействия угроз. Причем в конкретных политиках могут присутствовать не все функции из перечисленных. Главное, чтобы в определенном сочетании они обеспечивали требуемый уровень обеспечения ИБ (конечно, в пределах принимаемых рисков [16]). Следовательно, нарушение политики ИБ и соответственно типы инцидентов ИБ следует связать с невыполнением данных функций. Выполним такую классификацию. Выделим типы инцидентов нарушения ПИБ: "Не устранены условия возникновения угроз", "Не обнаружена реализация угрозы", "Нет защиты от реализованной угрозы", "Реализация неизвестной угрозы", "Не устраняется воздействие реализации угрозы".

Б. Политика ИБ в качестве обязательного структурного элемента содержит "Модель угроз" – документ, в котором перечисляется полное множество угроз, противодействие которым реализовано в СЗИ, точки воздействия угроз в КИТС, причины и источники их возникновения, а также механизмы (меры) защиты. Следовательно, нарушения политики ИБ (по ряду функций, обозначенных в п.А) следует искать в фактах недостаточной защиты конкретно против угроз, выделенных в Модели.

В. В качестве защитных мер реализации ЗФ, как правило, приводятся процедуры и механизмы: идентификации и аутентификации, контроля и разграничения доступа к локальным и разделенным информационным ресурсам (ИР), защиты от вредоносных программ, обеспечения целостности ИР, защиты внутренних и внешних каналов связи, защиты от удаленных атак.

Г. Как правило, техническая политика ИБ [8…15] содержит требования к средствам защиты. Среди таких средств наиболее распространены: штатные средства ОС, средства антивирусной защиты, средства защиты от НСД, средства шифрования, средства аутентификации, средства резервного копирования, межсетевое экранирование, системы обнаружения вторжений, VLAN, VPN. Следовательно, обнаружение инцидентов – нарушения политики – есть выявление факторов (причин) некорректной работы средств ЗИ. Множество таких факторов составить несложно – они представляют по сути "отрицания" требований к "настройке" средств ЗИ пполитики. Приведем пример перечня некоторых таких факторов, соответствующих типовой технической политике ИБ КИТС.

1. Антивирусная защита (АВЗ) не установлена и активирована на – шлюзе доступа (HTTP, FTP трафик), на почтовых системах (SMTP/POP3 трафик), на файловых серверах и рабочих станциях.

2. АВЗ не обновляются централизованно и регулярно.

3. Не все компоненты КИТС идентифицированы и учтены.

4. Имеется доступ к активному сетевому оборудованию (АСО) не только у системного администратора.

5. На портах АСО не установлен режим управления доступом к среде.

6. Не на всех используемых портах АСО установлен режим STP.

7. Не все неиспользуемые порты АСО отключены.

8. Не установлен контроль доступа на границе КИТС для входящих и исходящих данных на сетевом и транспортном уровне.

9. Нет межсетевого экрана на сетевом взаимодействии между КИТС и сторонней организацией.

10. Нет аудита контроля доступа по сетевому соединению.

11. Имеется "множественный" доступ к журналам аудита.

12. Не весь входящий и исходящий трафик анализируется на наличие вредоносных программ и сигнатур известных атак.

13. На рабочей станции сетевые конфигурационные параметры не соответствуют шаблону.

14. Учетные записи пользователей не актуальны.

15. Учетная запись не соответствует роли ее владельца.

16. Учетные записи уволенных сотрудников не блокируются и не удаляются.

17. Использование некорректных паролей.

18. Не все используемое программное обеспечение (ПО) идентифицировано в реестре разрешенного ПО.

19. В рабочих станциях и/или серверах имеется ПО, сведения о котором не внесены в реестр разрешенного ПО.

20. Реестр ПО содержит сведения о ПО с "просроченной" лицензией.

21. В личных папках пользователей присутствует информация "неслужебного" характера.

22. Пользователям не запрещено самостоятельно организовывать файловые серверы.

23. На рабочих станциях пользователей открыт общий доступ к папкам.

24. Изменена аппаратная конфигурация рабочей станции.

Таким образом, имеются предпосылки: выявить взаимосвязь функций защиты, мер защиты, средств защиты и факторов нарушения Политики, определить параметры КИТС, позволяющие измерить (оценить) факторы, и далее по значениям этих параметров идентифицировать тип инцидента и локализовать место нарушения для оперативной ликвидации последствий инцидента.

Л И Т Е Р А Т У Р А

1. ГОСТ Р ИСО/МЭК 18044:2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М.: Стандартинформ, 2009.

2. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. – 2005.

3. ISO/IEC TR 18044. Information security incident management.

4. CMU/SEI-2004-TR-015. Defining incident management processes for CISRT.

5. NIST SP 800-61. Computer security incident handling guide.

6. ISO/IEC 27035:2011. Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности. – 2011.

7. *Домарев В.В.* Безопасность информационных технологий. Методология создания систем защиты . – К.:ООО "ТИД "ДС", 2001.

8. Политика информационной безопасности ОАО "Газпромбанк" [Электронный ресурс]. – Режим доступа: www.gazprombank.ru/upload/iblock/ee7/infibez.pdf.

9. Политика информационной безопасности АО "Фонд развития предпринимательства "Даму" – www.damu.kz/content/files/PolitikaInformatsionnoy Bezopasnosti.pdf.

10. Политика информационной безопасности АО НК „КазМунайГаз“ [Электронный ресурс]. – Режим доступа: www.kmg.kz/upload/company/Politika_informacionnoi_bezopasnosti.pdf.

11. Политика информационной безопасности ОАО "Радиотехнический институт имени академика А. Л. Минца" [Электронный ресурс]. – Режим доступа: www.rti-mints.ru/uploads/files/static/8/politika_informacionnoy_bezopasnosti_rti.pdf.

12. Политика информационной безопасности ЗАО "СМАРТБАНК" [Электронный ресурс]. – Режим доступа: http://smartbank.ru/sites/default/files/documents/politika_informacionnoj_bezopasnosti.pdf.

13. *Бондаренко А.* Политика информационной безопасности [Электронный ресурс]. – Режим доступа: http://www.leta.ru/press-center/publications/article_295.html.

14. *Петренко С., Курбатов В.* Разработка политики информационной безопасности предприятия http://www.nestor.minsk.by/sr/2005/08/sr50803.html.

15. *Грибунин В.Г.* Разработка и реализация политики безопасности предприятия [Электронный ресурс]. – Режим доступа: http://bre.ru/security/22754.html.

16. *Милославская Н.Г., Сенаторов М.Ю., Толстой А.И.* Управление рисками информационной безопасности. – М.: Изд-во "Горячая линия – Телеком", 2014.

R E F E R E N C E S

1. GOST R ISO/MJeK 18044:2007. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Menedzhment incidentov informacionnoj bezopasnosti. – M.: Standartinform, 2009.

2. ISO/IEC 27001:2005. Informacionnye tehnologii. Metody obespechenija bezopasnosti. Sistemy upravlenija informacionnoj bezopasnost'ju. Trebovanija. – 2005.

3. ISO/IEC TR 18044. Information security incident management.

4. CMU/SEI-2004-TR-015. Defining incident management processes for CISRT.

5. NIST SP 800-61. Computer security incident handling guide.

6. ISO/IEC 27035:2011. Informacionnye tehnologii. Metod obespechenija bezopasnosti. Upravlenie sluchajnostjami v sisteme informacionnoj bezopasnosti. – 2011.

7. Domarev V.V. Bezopasnost' informacionnyh tehnologij. Metodologija sozdanija sistem zashhity . – K.:OOO "TID "DS", 2001.

8. Politika informacionnoj bezopasnosti OAO "Gazprombank" [Jelektronnyj resurs]. – Rezhim dostupa: www.gazprombank.ru/upload/iblock/ee7/infibez.pdf.

9. Politika informacionnoj bezopasnosti AO "Fond razvitija predprinimatel'stva "Damu" — www.damu.kz/content/files/PolitikaInformatsionnoy Bezopasnosti.pdf.

10. Politika informacionnoj bezopasnosti AO NK „KazMunajGaz“ [Jelektronnyj resurs]. – Rezhim dostupa: www.kmg.kz/upload/company/Politika_informacionnoi_bezopasnosti.pdf.

11. Politika informacionnoj bezopasnosti OAO "Radiotehnicheskij institut imeni akademika A. L. Minca" [Jelektronnyj resurs]. – Rezhim dostupa: www.rti-mints.ru/uploads/files/ static/8/politika_informacionnoy_bezopasnosti_rti.pdf.

12. Politika informacionnoj bezopasnosti ZAO "SMARTBANK" [Jelektronnyj resurs]. – Rezhim dostupa: http://smartbank.ru/sites/default/ files/ documents/politika_informacionnoj_bezopasnosti.pdf.

13. Bondarenko A. Politika informacionnoj bezopasnosti [Jelektronnyj resurs]. – Rezhim dostupa: http://www.leta.ru/press-center/publications/ article_295.html.

14. Petrenko S., Kurbatov V. Razrabotka politiki informacionnoj bezopasnosti predprijatija http://www.nestor.minsk.by/sr/2005/08/sr50803.html.

15. Gribunin V.G. Razrabotka i realizacija politiki bezopasnosti predprijatija [Jelektronnyj resurs]. – Rezhim dostupa: http://bre.ru/security/22754.html.

16. Miloslavskaja N.G., Senatorov M.Ju., Tolstoj A.I. Upravlenie riskami informacionnoj bezopasnosti. – M.: Izd-vo "Gorjachaja linija – Telekom", 2014.

Рекомендована кафедрой менеджмента и маркетинга. Поступила 09.07.15.