электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056.5

Проблемы управления инцидентами информационной безопасности на предприятии

***Бобров Н.В.**, магистр*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Системы обработки информации и управления»

Научный руководитель: Кесель С.А., к.т.н, доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Системы обработки информации и управления»
n.b.marco@gmail.com

Ни одна из существующих, даже самая совершенная, мера по снижению рисков информационной безопасности, будь то досконально проработанная политика или самый современный межсетевой экран, не может гарантировать полную защищенность информационной среды от событий, потенциально несущих угрозу бизнесу любого предприятия.

Разнообразие видов деятельности современного бизнеса и их сложность предопределяют наличие остаточных рисков вне зависимости от качества подготовки и внедрения мер противодействия угрозам информационной безопасности. Также всегда существует вероятность появления новых, ранее неизвестных угроз. Неготовность предприятия к подобного рода ситуациям, а именно отсутствие четко формализованной процедуры реагирования на возможные угрозы информационной безопасности, может существенно затруднить восстановление бизнес-процессов и потенциально усилить нанесенный ущерб.

Таким образом, любому предприятию, серьезно относящемуся к вопросам обеспечения информационной безопасности, необходимо реализовать комплексный подход к решению следующих задач:

- обнаружение и учет инцидентов информационной безопасности;

- реагирование на инциденты информационной безопасности, включая применение необходимых средств для их предотвращения, уменьшения нанесенного ущерба и восстановления нормальной деятельности предприятия;

- анализ произошедших инцидентов с целью планирования предупредительных мер защиты и улучшения процесса обеспечения информационной безопасности в целом.

Также следует отметить, что при эксплуатации различного рода систем менеджмента информационной безопасности процесс управления инцидентами является одним из важнейших источников информации для анализа функционирования подобных систем, оценки эффективности используемых мер снижения рисков и планирования улучшений в работе системы.

Таким образом, одним из важнейших моментов управления информационной безопасностью на предприятии является управление инцидентами.

К настоящему времени в международной практике разработано достаточное количество нормативных документов, регламентирующих вопросы управления инцидентами информационной безопасности. Необходимо отметить, что вопрос управления инцидентами возникает не только в рамках обеспечения информационной безопасности конкретного предприятия, но и при управлении ИТ-сервисами в целом. Семейство международных стандартов ISO 20000:2005 в разделе Service Delivery and Support описывает ряд требований к организации процесса управления инцидентами в ИТ-инфраструктуре. Согласно данным стандартам под инцидентом понимается «любое событие, не являющееся элементом нормального функционирования службы и при этом оказывающее или способное оказать влияние на предоставление службы путем ее прерывания или снижения качества».

А в стандарте ISO/IEC TR 18044:2004 дано следующее определение инцидента: «Инцидентом информационной безопасности является нежелательное событие информационной безопасности (или совокупность событий), которое может скомпрометировать бизнес-процессы компании или непосредственно угрожает ее информационной безопасности».

Одним из основных показателей того, правильно ли функционирует система управления безопасностью компании, служит частота появления и количество инцидентов, связанных с информационной безопасностью.

Из-за отсутствия процедур управления инцидентами на предприятиях в большинстве случаев не представляется возможным проследить все изменения характера и количества инцидентов информационной безопасности. Нельзя сделать однозначного вывода о правильности работы системы управления безопасностью из-за отсутствия инцидентов. Это чаще всего является показателем того, что инциденты просто не определяются или не фиксируются.

Можно выделить следующие основные проблемы, возникающие при управлении инцидентами:

- определение инцидента;

- оповещение о возникновении инцидента;

- регистрация инцидента

- устранение последствий и причин инцидента

- расследование инцидента

- реализация действий, предупреждающих повторное возникновение инцидента.

Для описания процедуры управления инцидентами безопасности используется классическая модель непрерывного улучшения процессов, получившая название от цикла Шухарта-Деминга – модель PDCA (Планируй, Plan – Выполняй, Do – Проверяй, Check – Действуй, Act). Стандарт ISO 27001 описывает модель PDCA как основу функционирования всех процессов системы управления информационной безопасностью. Естественно, что и процедура управления инцидентами подчиняется модели PDCA.

На рисунке представлена обобщенная процедура управления инцидентами согласно модели PDCA.

Рассмотрим более подробно эти проблемы.

Зачастую на предприятиях не применяются способы и методы определения и учета инцидентов, поэтому сотрудники не знают, какие события необходимо отнести к инцидентам.

В связи с этим сотрудники компании должным образом не информированы о порядке действий и форме отчетности при возникновении инцидента.

В большинстве случаев на предприятиях не установлены порядок и правила регистрации инцидентов – отсутствуют журналы их регистрации, не соблюдаются правила и сроки их заполнения.

Также предприятия не имеют четко формализованной, зафиксированной документально процедуры, описывающей порядок устранения последствий и причин возникновения каждого инцидента. В свою очередь эта процедура не должна препятствовать проведению мероприятий по расследованию инцидентов, т.к. при устранении последствий инцидентов не должно быть утеряна возможность установить виновных в произошедшем.

Ведение журналов регистрации инцидентов, четкое разделение прав пользователей, ответственность за выполненные ими действия являются определяющими при расследовании каждого инцидента. Это важно для определения участников инцидента и выявления их действий. Но в большинстве случаев процедуре расследования инцидентов на предприятиях не придают должного значения. Сразу же после ликвидации последствий инцидентов необходимых действий по выявлению виновных в произошедшем не предпринимается.

В тех случаях, когда предприятию был нанесен какой-либо ущерб, существует стандартная практика применения разного рода взысканий к виновным в возникновении инцидента. Но обычно виновники определяются без предусмотренных в таких случаях процедур, и внесение дисциплинарных взысканий не подчиняется утвержденным процедурам. Аналогично и другие действия по предотвращению повторного возникновения инцидента выполняются не всегда.

В первую очередь необходимо своевременно и должным образом устранить последствия инцидента, а также проконтролировать, что для этого было сделано. На

следующем этапе надо расследовать инцидент: определить причины его возникновения, виновных лиц и далее применить конкретные дисциплинарные взыскания. Далее выполняется оценка необходимости принятия мер по устранению причин инцидента. Если эта необходимость выявлена, то происходит их реализация, и выполняется ряд действий по предупреждению повторения возникшего инцидента.

Немаловажным является сохранение всей информации об инцидентах информационной безопасности предприятия, т.к. ведение статистики инцидентов информационной безопасности помогает осознавать их количество, характер и изменения во времени. Т.о. с помощью такого рода данных о статистике инцидентов определяются наиболее актуальные угрозы для предприятия и, следовательно, можно с максимальной точностью провести планирование мероприятий, направленных на повышение уровня защищенности информационной инфраструктуры предприятия.

Итак, выше были рассмотрены только основные причины необходимости создания строго формализованной процедуры управления инцидентами информационной безопасности, но и они являются достаточными для осознания всей важности данной процедуры. Об этом также говорят и стандарты по управлению безопасностью ISO 27001:2005 и ISO 17799:2005.

Итак, выше были рассмотрены все этапы модели PDCA применительно к процессу управления инцидентами информационной безопасности. В дальнейшем для эффективного и правильного функционирования этой процедуры, все эти этапы должны непрерывно и последовательно повторяться. Через определенное время (как правило, через полгода или год) необходимо заново пересмотреть перечень событий, называемых инцидентами, форму отчета и пр., внедрить обновленную процедуру в информационную систему, проверить ее функционирование и эффективности и реализовать превентивные действия. Таким образом, цикл модели PDCA будет непрерывно повторяться и гарантировать четкое функционирование процедуры управления инцидентами и, главное, ее постоянное совершенствование.

Далее рассмотрим правила управления инцидентами информационной безопасности и конкретные действия, необходимые для разработки процедуры управления инцидентами информационной безопасности на предприятии.

Процедура управления инцидентами является составной частью общей системы управления информационной безопасностью предприятия, поэтому важна позиция руководства по вопросу ее создания и функционирования и процесс разработки подобной процедуры должен быть инициирован самим руководством. При этом большое значение

имеет тот факт, что все сотрудники предприятия должны осознавать – обеспечение информационной безопасности в целом и управление инцидентами в частности являются основными бизнес-целями предприятия.

Затем службе информационной безопасности предприятия необходимо разработать нормативные документы по управлению инцидентами, которые должны содержать:

– определение инцидента информационной безопасности, а также список событий, которые необходимо относить к инцидентам (что на предприятии является инцидентом);

– порядок информирования, в том числе и документальный, специалистов службы информационной безопасности о возникновении инцидента;

– порядок мер по устранению последствий и причин инцидента;

– возможные действия по расследованию инцидента: определение причин, виновных в возникновении инцидента, порядок сбора и сохранения информации об инциденте и т.п.;

– перечень и порядок вынесения дисциплинарных взысканий;

– принятие мер по предотвращению повторного возникновения инцидента.

Выявление тех событий, которые необходимо отнести к инцидентам, – один из основных этапов разработки процедуры управления инцидентами. При этом необходимо принять во внимание, что события, не отнесенные службой безопасности к инцидентам, будут рассматриваться как штатные, даже если они несут угрозу информационной безопасности предприятия. В частности, в список инцидентов информационной безопасности могут быть внесены:

–отказ в обслуживании оборудования, средств обработки информации, сервисов;

–нарушение конфиденциальности, целостности, достоверности ценной информации;

–нарушение правил обработки информации и несоблюдение других требований к информационной безопасности, принятых на предприятии;

–несанкционированный мониторинг информационной системы;

–появление вредоносных программ в информационной системе предприятия;

–оставление компьютера незаблокированным без присмотра;

–пересылка конфиденциальной информации с помощью корпоративной или личной почты;

–разглашение паролей пользователей и др.

Итак, в зависимости от задач и структуры предприятия не все требования и рекомендации по защите информации могут быть реализованы на практике, следовательно, каждая компания должна тщательно подойти к построению своей

собственной системы управления процессами информационной безопасности. И в этой системе одним из важнейших аспектов является грамотно сформированный процесс управления инцидентами.

Результаты, получаемые в этом процессе, являются необходимыми для работы других процессов управления информационной безопасностью, в том числе проведения оценки рисков информационной безопасности, аудита, управления изменениями, доступом и непрерывностью бизнеса, оценки эффективности существующих защитных мер.

Список литературы

1. Медведев Н.В., Квасов П.М., Цирлов В. Л. Стандарты и политика информационной безопасности автоматизированных систем // Вестник МГТУ им. Н.Э.Баумана. Серия «Приборостроение». 2010. № 1(78). С. 103-102.
2. Барабанов А.В., Марков А. С., Найханова И. В. Методика оценки соответствия средств защиты информации общим критериям // Вестник МГТУ им. Н.Э.Баумана. Серия «Приборостроение». 2013. № 2(91). С. 48-58.
3. ISO/IEC 27001:2005. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования. 2005. 54 с.
4. ISO/IEC 27035:2011. Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности. 2011. 78 с.
5. ГОСТ Р ИСО/МЭК 18044:2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М.: Стандартинформ, 2009. 50 с.
6. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». М.: Стандартинформ, 2005. 26 с.
7. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Методы и средства обеспечения безопасности. Практические правила управления информационной безопасностью». М.: Стандартинформ, 2006. 56 с.
8. ISO 13335-1:2004 «Информационные технологии. Руководство по управлению ИТ безопасностью. Концепции и модели для управления безопасностью информационных и телекоммуникационных технологий». М.: Стандартинформ, 2007. 22 с.