**Управление инцидентами информационной безопасности**

Частота появления и количество инцидентов, связанных с информационной безопасностью, — один из наглядных показателей того, правильно ли функционирует система управления безопасностью. Как международные стандарты управления информационной безопасностью могут способствовать снижению количества инцидентов, а их соблюдение помогает предприятию перейти на новый уровень управления информационной безопасностью?

Международный стандарт ISO 27001:2005 обращает особое внимание на необходимость создания процедуры управления инцидентами информационной безопасности — очевидно, что без своевременной реакции на инциденты безопасности и устранения их последствий невозможно эффективное функционирование системы управления информационной безопасностью. К сожалению, в процессе аудита различных информационных систем приходится сталкиваться с множеством проблем регистрации и расследования инцидентов, свидетельствующих о том, что стандартам на предприятиях уделяется очень мало внимания. Например, в корпоративной сети одной из компаний появилась новая учетная запись пользователя с привилегированными полномочиями. В процессе расследования выяснилось, что пароль от единственной административной учетной записи знают несколько администраторов, а на контроллере домена не ведутся журналы регистрации событий, поэтому узнать, кто создал учетную запись, и расследовать данный инцидент оказалось невозможно. При этом пользователь, который будет заходить под новой привилегированной учетной записью, может выполнять в системе любые действия, просматривать, изменять или удалять информацию, останавливать или модифицировать работу сервисов.

*Сложности управления инцидентами информационной безопасности.* Во многих компаниях не всегда возможно проследить за изменением количества и характера инцидентов информационной безопасности — отсутствует процедура управления инцидентами. Часто отсутствие инцидентов не указывает на то, что система управления безопасностью работает правильно, а означает только, что инциденты не фиксируются или не определяются. Как правило, основные сложности при управлении инцидентами вызывают следующие моменты.

Определение инцидента. В компании отсутствует методика определения инцидентов, а сотрудники не знают, какие события являются инцидентами. Это особенно важно в случае инцидентов информационной безопасности — они не всегда мешают нормальной работе. Например, инцидентом безопасности будет оставление без присмотра на столе конфиденциальных документов, на что никто может и не обратить внимания, а злоумышленник (который может быть сотрудником компании) такие документы заметит.

Оповещение о возникновении инцидента. Сотрудники компании зачастую не осведомлены о том, кого и в какой форме следует ставить в известность при возникновении инцидента, — например, не определены ни формы отчетов, ни перечень лиц, которым необходимо отправлять отчеты об инцидентах. Даже если сотрудник заметит, что его коллега уносит для работы домой конфиденциальные документы компании, он не всегда знает, какие действия следует предпринимать в данной ситуации.

*Регистрация инцидента*. Ответственным лицам (даже если таковые назначены) часто не предоставляется методика регистрации инцидентов — не существует специальных журналов их регистрации, а также правил и сроков заполнения.

*Устранение последствий и причин инцидента*. В компаниях, как правило, отсутствует документально зафиксированная процедура, описывающая действия, которые необходимо выполнить с целью устранения последствий и причин инцидента. В первую очередь такая процедура должна предусматривать, чтобы мероприятия по устранению последствий и причин инцидента не нарушали процедуры их расследования: устранение последствий инцидента не должно «заметать следы», чтобы невозможно было установить виновных в инциденте.

*Расследование инцидента*. На этапе расследования инцидентов основную роль играют: ведение журналов регистрации событий, четкое разделение полномочий пользователей, ответственность за выполненные действия — важны доказательства того, кто участвовал в инциденте и какие действия он выполнял. К сожалению, про расследование инцидентов в компаниях часто просто забывают. Как только последствия инцидента устранены и бизнес-процессы восстановлены, дальнейшие действия по расследованию инцидента и осуществлению корректирующих и превентивных мер не выполняются.

*Реализация действий, предупреждающих повторное возникновение инцидента.* Как правило, если компании был нанесен какой-либо ущерб, то к виновным в возникновении инцидента (которые определены без необходимых в таких случаях процедур) все же применяются различные взыскания, однако внесение дисциплинарных взысканий не всегда подчиняется утвержденным процедурам и другие действия по предотвращению повторения инцидента выполняются тоже не всегда.

Управление инцидентами — одна из важнейших процедур управления информационной безопасностью. Прежде всего, важно правильно и своевременно устранить последствия инцидента, а также иметь возможность проконтролировать, какие действия были выполнены для этого. Необходимо также расследовать инцидент, что включает определение причин его возникновения, виновных лиц и конкретных дисциплинарных взысканий. Далее, как правило, следует выполнить оценку необходимости действий по устранению причин инцидента, если нужно — реализовать их, а также выполнить действия по предупреждению повторного возникновения инцидента. Кроме этого, важно сохранять все данные об инцидентах информационной безопасности, так как статистика инцидентов информационной безопасности помогает осознавать их количество и характер, а также изменение во времени. С помощью информации о статистике инцидентов можно определить наиболее актуальные угрозы для компании и, соответственно, максимально точно планировать мероприятия по повышению уровня защищенности информационной системы компании.

Здесь приведены только основные причины необходимости создания отдельной документированной и утвержденной процедуры управления инцидентами информационной безопасности, но и их достаточно, чтобы осознать всю важность данной процедуры. Об этом также говорят и стандарты по управлению безопасностью ISO 27001:2005 и ISO 17799:2005.

*Как управлять инцидентами информационной безопасности*? Какие конкретно действия необходимо выполнить для разработки процедуры управления инцидентами информационной безопасности?

Для начала необходимо, чтобы процесс разработки процедуры (как и всех процедур в компании) был инициирован ее руководством. Как правило, процедура управления инцидентами разрабатывается в рамках общей системы управления информационной безопасностью, поэтому важна позиция руководства по вопросу ее создания и функционирования. На данном этапе важно, чтобы все сотрудники компании понимали, что обеспечение информационной безопасности в целом и управление инцидентами в частности являются основными бизнес-целями компании.

Затем следует разработать необходимые нормативные документы по управлению инцидентами. Как правило, такие документы должны описывать:

* определение инцидента информационной безопасности, перечень событий, являющихся инцидентами (что в компании является инцидентом);
* порядок оповещения ответственного лица о возникновении инцидента (необходимо определить формат отчета, а также отразить контактную информацию лиц, которых следует оповещать об инциденте);
* порядок устранения последствий и причин инцидента;
* порядок расследования инцидента (определение причин инцидента, виновных в возникновении инцидента, порядок сбора и сохранения улик);
* внесение дисциплинарных взысканий;
* реализация необходимых корректирующих и превентивных мер.

Определение перечня событий, являющихся инцидентами, — важный этап разработки процедуры управления инцидентами. Следует понимать, что все события, которые не войдут в указанный перечень, будут рассматриваться как штатные (даже если они несут угрозу информационной безопасности). В частности, инцидентами информационной безопасности могут быть:

* отказ в обслуживании сервисов, средств обработки информации, оборудования;
* нарушение конфиденциальности и целостности ценной информации;
* несоблюдение требований к информационной безопасности, принятых в компании (нарушение правил обработки информации);
* незаконный мониторинг информационной системы;
* вредоносные программы;
* компрометация информационной системы (например, разглашение пароля пользователя).

В качестве примера инцидентов можно привести такие события, как неавторизованное изменение данных на сайте компании, оставление компьютера незаблокированным без присмотра, пересылка конфиденциальной информации с помощью корпоративной или личной почты. В общем случае инцидент информационной безопасности определяется как единичное, нежелательное или неожиданное событие информационной безопасности (или совокупность таких событий), которое может скомпрометировать бизнес-процессы компании или угрожает ее информационной безопасности (ISO/IEC TR 18044:2004).

Важно отметить, что процедура управления инцидентами тесно связана со всеми другими процедурами управления безопасностью в компании. Поскольку инцидентом, в первую очередь, является неразрешенное событие, оно должно быть кем-то запрещено, следовательно, необходимо наличие документов, четко описывающих все действия, которые можно выполнять в системе и которые выполнять запрещено. Например, в одной из компаний сотрудник хранил на мобильном компьютере конфиденциальные сведения компании без применения средств шифрования. После работы он забрал компьютер домой и забыл его в машине, которую оставил под окнами дома, а ночью машину взломали, и компьютер был украден. Злоумышленники получили доступ к конфиденциальной информации компании и могли продать ее конкурентам. Кроме этого, на компьютере хранилась ценная информация, которая не была зарезервирована на другом носителе. Такой инцидент мог произойти в результате того, что в компании не были разработаны процедуры обращения с мобильными компьютерами и хранения на них информации. Вынос компьютера за пределы офиса компании, отсутствие средств шифрования и резервного копирования информации — возможные нарушения, а следовательно, причины инцидентов. Однако пока документально не зафиксировано, что это нарушения (т.е. в соответствующих документах не описано, что это запрещено), сотрудника невозможно привлечь к ответственности и предотвратить повторное выполнение неправомерных действий.

Важно, чтобы были налажены такие процедуры, как мониторинг событий, своевременное удаление неиспользуемых учетных записей, контроль и мониторинг действий пользователей, контроль над действиями системных администраторов и пр. В одной из компаний был зафиксирован следующий инцидент: при увольнении с работы системный администратор украл разрабатываемый в компании программный продукт и передал его конкурентам, которые выпустили программу на рынок под своим товарным знаком. Кроме этого, он внес изменения в информационную систему, в результате которых после его ухода функционирование определенных ее компонентов было нарушено. Привлечь администратора к ответственности в данном случае оказалось невозможно, так как, во-первых, не выполнялась регистрация его действий, во-вторых, администратор мог удалить все доказательства своих неправомерных действий и, в-третьих, не была налажена процедура сбора улик об инциденте. Кроме этого, в компании просто не знали, как следует поступать в таких случаях (например, можно было обратиться в специализированную компанию по расследованию инцидентов или подать заявление в суд).

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 (см. рисунок).

*Обнаружение и регистрация инцидента*. Инцидент информационной безопасности может заметить пользователь или администратор системы. Как правило, администраторы знают, что следует делать в случае обнаружения инцидентов, чего не всегда можно сказать о пользователях. Для пользователей следует разработать инструкцию, которая, как правило, содержит описание, в каком виде сотрудник должен сообщить о возникновении инцидента, координаты ответственных лиц, а также перечень действий, которые сотрудник может выполнить самостоятельно (или предупредить о том, что выполнять какие-либо действия самостоятельно запрещено). Такой отчет должен содержать подробное описание инцидента, перечисление сотрудников, вовлеченных в инцидент, фамилию сотрудника, зафиксировавшего инцидент и дату возникновения и регистрации инцидента. Таким образом, каждый сотрудник получает инструкцию, определяющую, каковы должны быть его действия, например, в случае, если он продолжил работу с документом и заметил, что с прошлого раза в его документ были внесены изменения, не соответствующие действительности, при этом автор изменений неизвестен.

Далее требуется разработать инструкцию для специалиста, в обязанности которого входит регистрация инцидента. Сотрудник, обнаруживший инцидент, связывается с сотрудником, ответственным за регистрацию инцидента и выполнение дальнейших действий. В небольших компаниях сотрудники обращаются напрямую к специалисту, который может устранить последствия и причины инцидента (например, к системному администратору или администратору безопасности). В достаточно крупных компаниях, как правило, выделяют сотрудника, который регистрирует инцидент и передает информацию об инциденте соответствующим специалистам. Такая инструкция может содержать, например, правила и срок регистрации инцидента, перечень необходимых первоначальных инструкций для сотрудника, обнаружившего инцидент, кроме того, описание порядка передачи информации об инциденте соответствующему специалисту, порядок контроля за устранением последствий и причин инцидента.

*Устранение причин, последствий инцидента и его расследование*. Инструкция по устранению причин и последствий инцидента включает описание общих действий, которые необходимо предпринять (конкретные действия для каждого вида инцидента определять трудоемко и не всегда целесообразно), а также сроки, в течение которых следует устранить последствия и причины инцидента. Сроки устранения последствий и причин инцидента зависят от уровня инцидента. Следует разработать классификацию инцидентов — определить количество уровней критичности инцидентов, описать инциденты каждого уровня и сроки их устранения. Документ, определяющий, какие события в компании следует считать инцидентом, также может описывать и уровни инцидентов.

Таким образом, инструкция по устранению последствий и причин инцидента может включать: описание действий, предпринимаемых для устранения последствий и причин инцидента, сроки устранения и указание на ответственность за несоблюдение инструкции.

Расследование инцидента включает в себя определение виновных в его возникновении, сбор доказательств и улик инцидента, определение соответствующих дисциплинарных взысканий. В крупных компаниях, как правило, выделяют комиссию по расследованию инцидентов информационной безопасности (в состав которой может входить сотрудник, регистрирующий инциденты). Инструкция по расследованию инцидентов должна описывать: действия по расследованию инцидента (в том числе определение виновных в его возникновении), правила сбора и хранения улик (особенно в случае, если может потребоваться использование улик в судебных органах) и правила внесения дисциплинарных взысканий.

*Корректирующие и превентивные действия*. После устранения последствий инцидента и восстановления нормального функционирования бизнес-процессов компании, возможно, потребуется выполнить действия по предотвращению повторного возникновения инцидента. Для определения необходимости реализации таких действий следует провести анализ рисков, в рамках которого определяется целесообразность корректирующих и превентивных действий. В некоторых случаях последствия инцидента незначительны по сравнению с корректирующими и превентивными действиями, и тогда целесообразно не совершать дальнейших шагов после устранения последствий инцидента.

Мы рассмотрели все этапы модели PDCA применительно к процессу управления инцидентами информационной безопасности. Далее, для того чтобы процедура выполнялась правильно и эффективно, 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 улучшение.

Во многих крупных компаниях внедрена служба поддержки Service Desk, в обязанности которой входит управление инцидентами в области информационных технологий. Процедура управления ИТ-инцидентами регулируется стандартом ISO/IEC 20000:2005, пришедшим на смену BS 15000:2002, который, в свою очередь, взял за основу библиотеку ITIL. Заметим, что все ISO/IEC серий 9000, 14000, 20000, 27000 и другие стандарты ISO/IEC, описывающие правила создания систем управления различными процессами, гармонично сочетаются друг с другом. Все они в качестве основы управления подконтрольными процессами используют процессный подход, который рассматривает управление как процесс, а именно как набор взаимосвязанных непрерывных действий. Процессный подход акцентирует внимание на достижении поставленных целей, а также на ресурсах, затраченных для этого. Кроме этого, стандарты указанных серий используют модель PDCA как структуру жизненного цикла всех процессов системы управления.

Естественно, что ISO 20000, описывает как систему управления ИТ-сервисами, так и процедуру управления инцидентами, но также рассматривает ИТ-инциденты. Сама процедура управления инцидентами ИТ очень близка к процедуре управления инцидентами информационной безопасности с той лишь разницей, что в последнем случае больший упор делается на его расследование, сбор улик, наказание виновных (вплоть до обращения в суд).

Управление инцидентами информационной безопасности, как правило, возлагается на службу поддержки, обрабатывающую инциденты ИТ (в том случае, если такая служба существует в компании). Это еще раз доказывает то, что целесообразно разработать одну систему управления всеми процессами в компании, так как управление схожими процессами в разных областях ее деятельности часто выполняется по одной схеме

Важно, чтобы ни один инцидент не остался незамеченным, было проведено расследование, выявлены виновные, и, самое главное, выполнены корректирующие и превентивные действия. Главной особенностью инцидентов в области информационной безопасности является то, что они не всегда заметны (не всегда мешают в работе пользователей), однако возможный ущерб от таких инцидентов сложно недооценить. Следовательно, необходима четкая процедура регистрации и расследования инцидентов безопасности, а также информирование пользователей о правилах определения инцидентов.

Необходимо понимать, что управление инцидентами не предупреждает нанесение ущерба компании (как правило, компания уже понесла ущерб, связанный с инцидентом), однако расследование инцидента и своевременное внедрение превентивных и корректирующих мер снижает вероятность его повторения (и, следовательно, вероятность повторения нанесения ущерба). Отметим также, что статистика инцидентов информационной безопасности представляет особую ценность для компании как показатель эффективности функционирования системы управления информационной безопасностью. Статистику инцидентов следует регулярно анализировать в рамках аудита системы управления информационной безопасностью.