«МЕНЕДЖМЕНТ ИНЦИДЕНТОВ В СИСТЕМЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

Анна Милованова, *IT&IS Management SRL*
(Республика Молдова)

Одним из важных процессов в системах управления ИТ-деятельностью является управление инцидентами, оказывающих непосредственное влияние на стабильность работы информационных систем. Это обусловлено увеличением масштаба и функционала систем. Даже после внедрения защитных мер в большинстве случаев остаются слабые места, что делает обеспечение информационной безопасности неэффективным, и, следовательно, инциденты - возможными.

Управление инцидентами обеспечивает уменьшение/ исключение отрицательного воздействия нарушений в предоставлении ИТ-услуг, что является актуальным в особенности для финансово-кредитных организаций и телекоммуникационных компаний. Решение данной задачи требует тесного взаимодействия с пользователями клиентами посредством функции Service Desk.

Сам процесс управления инцидентами связан со многими другими процессами, например, управлением рисками, мониторингом/ аудитом, управлением изменениями, управлением доступом, управлением непрерывностью. Другими словами, процесс управления инцидентами является своеобразным «мотором» жизненного цикла системы безопасности.

Исходя из практики, можно отметить тот факт, что основными типами инцидентов являются:

- функциональная неработоспособность основных модулей или информационных систем целиком;
- недоступность к значимым сервисам, приложениям или к информационным системам в целом;
- ошибочная обработка информации в информационных системах и приложениях;
- сбои в работе приложений, влияющих на эффективность ведения деятельности;
- неисправность, выход из строя аппаратных средств;
- отсутствие доступа к открытым Интернет-ресурсам;
- некорректная работа информационных систем;
- перегрузка в сети.

При управлении инцидентами по всем выявленным инцидентам следует проводить анализ потенциального или реального негативного

воздействия инцидента информационной безопасности на деятельность организации. В качестве примеров основных категорий последствий, которые могут повлечь за собой инциденты, можно отметить:

- финансовые убытки/разрушение бизнес-операций;
- ущерб коммерческим и экономическим интересам;
- ущерб для информации, содержащей персональные данные;
- нарушение правовых и нормативных обязательств;
- потеря/ущерб репутации организации.

Для любой организации, серьезно относящейся к информационной безопасности, основой менеджмента инцидентов должно быть применение структурного и планового подходов с целью минимизации рисков информационной безопасности. Суть данных подходов заключается в осуществлении следующих действий:

- обнаружение, оповещение об инцидентах информационной безопасности и их оценка;
- реагирование на инциденты информационной безопасности, включая применение защитных мер для предотвращения, уменьшение последствий и восстановление после негативных воздействий;
- извлечение уроков из инцидентов информационной безопасности, введение превентивных защитных мер и улучшение общего подхода к управлению инцидентами информационной безопасности.

Менеджмент инцидентов информационной безопасности включает следующие этапы:

- обнаружение и регистрация инцидентов - осуществляется на основании показаний систем мониторинга доступности ИТ-услуг, обращений пользователей, а также осуществляется в системе регистрации и обработки инцидентов;
- классификация и приоритезация инцидентов - идентификация причин инцидента и соответствующих действий для его решения, и определение критичности инцидента для деятельности компании;
- эскалация инцидентов – осуществляется помощь в своевременном разрешении инцидента;
- обработка инцидентов – разрешение инцидента и восстановление ИТ-услуг;
- мониторинг инцидентов – осуществляется контроль качества обработки и разрешения инцидентов с целью выявления несоответствий и подготовки рекомендацией по управлению инцидентами;
- закрытие инцидентов.

Этапы менеджмента инцидентов могут меняться каждой органи-

зацией в зависимости от ее внутренних потребностей ведения бизнеса. Рекомендуется руководствоваться требованиями по управлению инцидентами, прописанными во многих международных стандартах и практиках, среди которых можно отметить следующие:

- ISO 17799 Информационная технология - методики Безопасности - Практическое руководство для информационного управления безопасности;
- ISO 18044-2007 Информационная технология – Методы и средства обеспечения безопасности – Менеджмент инцидентов информационной безопасности;
- лучшие практики IT Infrastructure Library (Библиотека передового опыта организации ИТ).

Применение данных стандартов и практик позволит сократить возможные последствия и снизить риски, возникающие при реализации инцидентов, что еще раз доказывает важность вопросов менеджмента инцидентов в рамках управления ИТ функциями. Это обеспечивает необходимость принятия эффективных мер по сокращению появляющихся инцидентов. Эффективность управления инцидентами должна выражаться в измеряющихся и оценивающихся показателях. Такими показателями, например, могут выступать:

- тенденции в изменении общего количества инцидентов;
- среднее фактическое время, затраченное на разрешение инцидента;
- процент инцидентов, обработанных в рамках согласованного времени реакции;
- средние затраты на решение инцидента;
- процент инцидентов, закрытых без обращения к специализированным группам поддержки;
- количество и процент инцидентов, разрешенных удаленно.

Таким образом, эффективный менеджмент инцидентов позволит обеспечить быстрое восстановление нормального функционирования информационных систем, минимизировать неблагоприятное воздействие на бизнес, снизить финансовые потери, а также поддерживать процессы управления рисками.

Литература и интернет источники:

1. IT Infrastructure Library (Библиотека передового опыта организации ИТ);
2. www.iso27000.ru;
3. www.itsec.ru;
4. www.connect.ru.