ПОД- СЕКЦИЯ 14. Управление проектами и программами.

Иванова А.М.
магистрант кафедры «Информационной безопасности и передачи данных»
Одесской национальной академии связи им. А.С.Попова

МЕТОДЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мировой опыт создания различных защитных систем неизменно показывает: как только человечество открывает новые средства защиты, тут же находятся источники противодействия и разрушения. Век информатизации не стал исключением. От разработчиков новейших технологий, не отстают злоумышленники, которые стремятся найти уязвимости, создавая средства угроз и атак. Современное предприятие уже не может существовать без защищенной должным образом информационной системы. На сегодняшний день информация становится наиболее ценным ресурсом любой компании: утечка важных данных о клиентах или финансовых сведений может нанести непоправимый ущерб репутации и дальнейшей коммерческой деятельности организации.

Однако при всей значимости защитных систем, остаются неразрешенными многие проблемы. Среди них, прежде всего, стоит отметить проблему утечки корпоративной информации, и ее последующее незаконное использование третьими лицами. Угроза может исходить как от невнимательного сотрудника, так и от партнеров по бизнесу, клиентов или подрядчиков. Он для того чтобы оптимизировать защиту информационной среды и снизить число неизбежно возникающих инцидентов (инцидент – от лат. incidens – случающийся, случай, происшествие (обычно неприятное); столкновение), необходимо обратиться к методологической базе управления инцидентами, как существующей в Украине, так и зарубежному опыту.

Таким образом, ***цель*** данной статьи состоит, во-первых, в анализе методов управления инцидентами в сфере информационной безопасности, а во-вторых, в демонстрации необходимости создания методологической базы по защите информационных систем, с учетом передового международного опыта.

Для решения поставленных задач будут использованы такие общенаучные ***методы*** как – анализ, синтез, компаративистский и системный методы.

Возрастающее значение систем управления безопасностью в сфере информационных систем, порождает увеличивающийся интерес со стороны исследователей и разработчиков защитных технологий разных уровней. Вместе с тем, аналитических и теоретико-методологических работ, в которых раскрывается данная проблематика невелико. Среди наиболее интересных разработок можно указать таких авторов: Белоус С. [1], Разумовский С. [3], Суханов А. [4], Куканова Н. [2] и другие.

На сегодняшний день в международной практике разработано достаточное количество нормативных документов, регламентирующих вопросы управления инцидентами информационной безопасности. Семейство международных стандартов ISO 20000:2005 в разделе Service Delivery and Support описывает ряд

требований к организации процесса управления инцидентами. 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.

Стоит отметить, что основные сложности при управлении инцидентами вызывают следующие моменты: определение инцидента (отсутствует методика определения инцидентов, а сотрудники не знают, какие события являются инцидентами); оповещение о возникновении инцидента (сотрудники зачастую не осведомлены о том, кого и в какой форме следует ставить в известность при возникновении инцидента); регистрация инцидента (не существует специальных журналов их регистрации, а также правил и сроков заполнения); устранение последствий и причин инцидента (отсутствует документально зафиксированная процедура, описывающая действия, которые необходимо выполнить с целью устранения последствий и причин инцидента); расследование инцидента (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 (внесение дисциплинарных взысканий не всегда подчиняется утвержденным процедурам и другие действия по предотвращению повторения инцидента выполняются тоже не всегда).

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.

Сравнивая организацию систем безопасности, основанную с учетом стандартов ISO вместе с моделью PDCA и систем безопасности, построенных с помощью локальных инструментов, легко обнаружить существенные преимущества первой.

Кроме того, 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. 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 прочее.

Инцидент информационной безопасности может заметить пользователь или администратор системы. Но часто этого бывает недостаточно, поэтому необходимо обращаться автоматизированным системам. Наиболее эффективной для этих целей представляется система Snort.

Snort является свободной сетевой системой предотвращения вторжений (IPS) и сетевой системой обнаружения вторжений (IDS) с открытым исходным кодом, способной выполнять регистрацию пакетов и в реальном времени осуществлять анализ трафика в IP сетях.

Snort выполняет протоколирование, анализ, поиск по содержимому, а также широко используется для активного блокирования или пассивного обнаружения целого ряда нападений и зондирований, таких как переполнение буфера, стелс-сканирование портов, атаки на веб-приложения, SMB-зондирование и попытки определения операционной системы. Программное обеспечение в основном используется для предотвращения проникновения, блокирования атак, если они имеют место.

Система обнаружения вторжений (СОВ) – программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин – Intrusion Detection System (IDS). Системы обнаружения вторжений обеспечивают дополнительный уровень защиты информационных систем.

Системы обнаружения вторжений используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей).

Система предотвращения вторжений (англ. Intrusion Prevention System) – программная или аппаратная система сетевой и компьютерной безопасности, обнаруживающая вторжения или нарушения безопасности и автоматически защищающая от них.

Системы IPS можно рассматривать как расширение Систем обнаружения вторжений (IDS), так как задача отслеживания атак остается одинаковой. Однако, они отличаются в том, что IPS должна отслеживать активность в реальном времени и быстро реализовывать действия по предотвращению атак. Возможные меры – блокировка потоков трафика в сети, сброс соединений, выдача сигналов оператору. Также IPS могут выполнять дефрагментацию пакетов, переупорядочивание пакетов TCP для защиты от пакетов с измененными SEQ и ACK номерами.

После обнаружения инцидента, наступает важный этап реагирования на инцидент. Вся формальная модель процесса реагирования на инциденты определятся документом: ISO/IEC TR 18044 Information security incident management. Целями следования этой модели является уверенность в том, что:

– события и инциденты информационной безопасности выявляются и обрабатываются эффективным образом, в особенности в части классификации событий;

– выявленные инциденты информационной безопасности в организации учитываются и обрабатываются наиболее подходящим и эффективным образом;

– последствия инцидентов информационной безопасности могут быть минимизированы в процессе реагирования на инциденты, возможно с привлечением

процессов восстановления после сбоев и аварий (DRP/BCP);

– за счет анализа инцидентов и событий повышается вероятность предотвращения будущих инцидентов, улучшаются механизмы и процессы обеспечения информационной безопасности.

Процесс реагирования на инциденты состоит из нескольких этапов. В эти этапы в обязательном порядке входят следующие элементы.

1. Планирование и подготовка. На данном этапе разрабатывается схема реагирования на инциденты, подготавливаются и утверждаются ряд организационно-регламентирующих документов, выделяются человеческие и материальные ресурсы, проводится необходимое обучение и апробация выбранной схемы реагирования на инциденты.

2. Эксплуатация. Собственно обнаружение инцидента информационной безопасности, его идентификация, предварительный анализ и начальное реагирование.

3. Анализ. Проводится углубленный анализ инцидента, на его основе делаются выводы и составляются рекомендации по улучшению процесса обеспечения информационной безопасности и реагирования на инциденты. Формируется отчет об инциденте.

4. Улучшение. На данном этапе реализуются рекомендации, выработанные на этапе анализа.

В итоге, вся система защиты информационных систем приобретает завершенный и целостный вид. Подобная методологическая база, построенная на основе ведущих мировых стандартов защиты информации и с использованием специализированного программного обеспечения, способна если не полностью предотвратить, то значительно уменьшить число инцидентов и минимизировать вызываемые ими последствия.

Таким образом, можно заключить, что поставленные в статье задачи были выполнены, а к наиболее значимым ***выводам*** проделанной работы можно отнести следующие положения:

первое, без учета мирового опыта по разработке методологической базы управления инцидентами в сфере защиты информационных систем, невозможно организовать должные меры безопасности, необходимость которых определяется современным развитием технических средств и глобализацией информационного пространства;

второе, международные стандарты управления информационной безопасностью могут способствовать снижению количества инцидентов, а их соблюдение помогает перейти на новый уровень управления информационной безопасностью;

третье, для автоматизации защиты информационных систем оптимально использовать систему Snort, которая является свободной сетевой системой предотвращения вторжений (IPS) и сетевой системой обнаружения вторжений (IDS).

Дальнейшие направления в разработке данной проблематики очевидны: это, прежде всего усилия, направленные на формирования необходимой методологической базы управления инцидентами, создание оптимальных условий по внедрению международных стандартов и принципов работы в сферу

информационной безопасности.

Литература:

1. Белоус С. Улучшение процесса управления инцидентами, 2007. – Способ доступа: http://itsmportal.com.ua/art011.html

2. Куканова Н. Управление инцидентами информационной безопасности // Открытые системы, №10, 2006. – Способ доступа: http://www.osp.ru/os/2006/10/3910101/

3. Разумовський С. Концепція управління IT-послугами // Відкриті системи, № 12, 2002. – Способ доступа: http://www.osp.ru/os/2002/12/182252/

4. Суханов А. Аналіз ризиків в управлінні інформаційною безпекою // Інформзахист, №11(120), 2008. – Способ доступа: http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskami-informacionnoi-bezopasnosti/analiz-riskov-v-upravlenii-informacionnoi-bezopasnostyu