УДК 004 **Информационные технологии**

Отакулов Артур Собирович, *студент 3 курса по направлению «Информармационная безопансость», Донской государственный технический университет Россия, г. Ростов-на-Дону*

СПОСОБЫ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация: В данной работе рассматриваются вопросы, касающиеся особенностей реагирования на инциденты. Перечислены основные этапы реагирования как обнаружение, анализ, сдерживание, а также деятельность после устранения разного вида инцидента.

Ключевые слова: информационная безопасность, способы реагирования на инциденты, методы защиты информации.

Annotation: This article discusses issues related to the specifics of incident response. The main stages of the response are detection, analysis, localization, as well as measures after the elimination of various types of incidents.

Keywords: information security, how to respond to incidents, and how to protect information.

Случаи с нарушением в информационной безопасности одно из самых нежелательных и нежданных событий в любой отрасли. Такие нарушения могут скомпрометировать деловые операции и поставить под угрозу защиту любой информации, которая предназначена для определённого круга лиц.

Реагирование на инциденты является важной частью системы информационной безопасности в любой современной организации. Инциденты, связанные с нарушением информационной безопасностью в финансовых организациях, могут привести к прямым финансовым потерям. Поэтому

сотрудники отдела информационной безопасности организации должны уметь полностью выявлять и проводить анализ любых атак, свершения незаконных действий.

Реагирование на инциденты

В случае, если усилия по управлению рисками терпят неудачу, существует реагирование на инциденты, чтобы реагировать на такие события. Реагирование на инциденты должно быть в первую очередь ориентировано на те элементы, которые, по нашему мнению, могут причинить нам большие потери. Реакция на такие инциденты должна основываться, насколько это возможно или практически возможно, на документированных планах реагирования на инциденты, которые регулярно пересматриваются, тестируются и практикуются теми, от кого ожидается их принятие в случае фактического инцидента [1].

Процесс реагирования на высоком уровне состоит из:

- Подготовка;
- Обнаружение и анализ;
- Сдерживание;
- Искоренение;
- Восстановление;
- Деятельность после инцидента.

Подготовка

Подготовительный этап реагирования на инцидент состоит из всех действий, которые можно выполнить до самого инцидента, чтобы лучше справиться с ним. Это, как правило, включает в себя разработку политики и процедур, регулирующих реагирование на инциденты и их обработку, проведение обучения для тех, кто должен сообщать об инцидентах, проведение учений по реагированию на инциденты, разработку и ведение документации и многие другие подобные мероприятия.

Важность этого этапа реагирования на инциденты не следует недооценивать. Без надлежащей подготовки крайне маловероятно, что реакция

на инцидент будет успешной и/или в том направлении, в котором мы ожидаем ее развития. Время определяет, что нужно сделать, кто должен это сделать и как это сделать.

Обнаружение и анализ

Фаза обнаружения и анализа — это когда действие начинает происходить в процессе реагирования на инцидент. На этом этапе возможно обнаружить возникновение проблемы и решение, действительно ли это инцидент, чтобы можно было отреагировать на него соответствующим образом.

Часть обнаружения этой фазы часто является результатом мониторинга или оповещения на основе результатов работы инструмента или службы безопасности. Это может быть вывод из системы обнаружения вторжений, антивирусного программного обеспечения, журналов брандмауэра, прокси-журналов, оповещений от средства мониторинга информации и событий безопасности.

Аналитическая часть этой фазы часто представляет собой комбинацию автоматизации от инструмента или услуги и человеческого суждения. Хотя часто можно использовать своего рода пороговое значение, чтобы сказать, что число событий X за данный промежуток времени является нормальным или что определенная комбинация событий не является нормальной (два неудачных входа, за которыми следует успех, за которыми следует смена пароля, за которыми следует создание новой учетной записи), часто будет нуждаться в человеческом вмешательстве в определенный момент при обсуждении реакции на инцидент. Такое вмешательство человека часто включает в себя проверку журналов, выводимых различными устройствами безопасности, сети и инфраструктуры, контакт со стороной, сообщившей об инциденте, и общую оценку ситуации. Это может быть дорого, если работа происходит с командой аналитиков, поэтому автоматизация как можно большего числа функций является ключевой [2].

Когда обработчик инцидента оценит ситуацию, он определит, является ли проблема инцидентом или нет, проведет первоначальную оценку критичности

инцидента (если таковая имеется) и свяжется с любыми дополнительными ресурсами, необходимыми для перехода к следующему этапу.

Сдерживание, искоренение и восстановление.

На этапе локализации, ликвидации и восстановления происходит большая часть работы по фактическому разрешению инцидента, по крайней мере в краткосрочной перспективе.

Сдерживание включает в себя принятие мер для обеспечения того, чтобы ситуация не причинила больше вреда, чем она уже нанесла, или по крайней мере уменьшить любой продолжающийся вред. Если проблема связана с тем, что зараженный вредоносным ПО сервер активно контролируется удаленным злоумышленником, это может означать отключение сервера от сети, введение правил брандмауэра для блокировки злоумышленника и обновление сигнатур или правил в системе предотвращения вторжений для остановки трафика от вредоносного ПО [3].

В случае с вредоносным сервером уже изолировали систему и отключили ее от командной и управляющей сети. Теперь нужно будет удалить вредоносную программу с сервера и убедиться, что она не существует в другом месте среды. Это может включать в себя дополнительную проверку других узлов в среде, чтобы убедиться, что вредоносное ПО отсутствует, а также проверку журналов на сервере и действий атакующих устройств в сети, чтобы определить, с какими другими системами зараженный сервер был в контакте. С вредоносными программами, особенно очень, это может быть сложной задачей, чтобы гарантировать. Противник постоянно разрабатывает контрмеры к самым современным инструментам и методологиям обеспечения безопасности. Всякий раз, когда возникают сомнения относительно того, действительно ли вредоносное ПО или злоумышленники были изгнаны из нашей среды, стоит проявлять осторожность, балансируя воздействие на операции. Каждое событие требует оценки риска.

Наконец, нужно восстановить лучшее состояние, в котором находилась до инцидента или, возможно, до начала проблемы, если не обнаружили

проблему сразу. Это может включать в себя восстановление устройств или данных с резервного носителя, перестройку систем, перезагрузку приложений или любые другие аналогичные действия. Кроме того, нужно смягчить вектор атаки, который был использован. Опять же, это может быть более болезненная задача, чем кажется на первый взгляд, основанная на потенциально неполном или неясном знании ситуации вокруг инцидента и того, что именно произошло. Так же стоит проверить, что носитель резервной копии на самом деле чист и свободен или заражен, носитель резервной копии может быть полностью испорчен, бит установки приложения может отсутствовать, файлы конфигурации могут быть недоступны, и любой из ряда подобных проблем.

Деятельность после инцидента

Деятельность после инцидента, как и подготовка, - В фазе активности после инцидента, часто называемой посмертной (латинское слово "после смерти"), пытаемся определить, что именно произошло, почему это произошло, и что мы можем сделать, чтобы это не повторилось. Это не просто технический обзор, поскольку могут потребоваться изменения в политике или инфраструктуре. Цель этой фазы состоит не в том, чтобы указать или возложить вину, а в том, чтобы в конечном счете предотвратить или уменьшить воздействие будущих подобных инцидентов [4].

Так же стоит отметить. Что стоит периодически производить лекционные занятия с сотрудниками организации с целью устранения ряда незаконных проникновений на данную организую.

Библиографический список:

1. Советов Б.Я., Информационные технологии Высшая школа, 2009г.
2. Мельников В.П. Информационная безопасность и защита информации. 3-е изд. Академия. 2008г.
3. Грушо А.А., Применко Э.А., Тимонина Е.Е. Анализ и синтез криптоалгоритмов. Курс лекций. 2000г.
4. Варлатая, С.К., Аппаратно-программные средства и методы защиты информации. 2007г.