- исключение ошибок переписывания с доски и записи со слуха в конспектах лекций за счёт наличия лекционного материала у студентов;

- появление возможности поддержания оптимального темпа при изложении материала, позволяющего удерживать внимание студентов на предмете лекции.

4. Проблемы использования мультимедийных средств при чтении лекций.

- *эффект мелькающих картинок* – получив заранее лекционный материал, некоторые студенты относятся к демонстрации слайдов, как к просмотру мультипликационных фильмов (не вдумываются в материал, не записывают пояснения преподавателя).

Для предотвращения подобного эффекта следует постоянно вовлекать студентов в процесс анализа рассматриваемого материала;

- *эффект дробления целого* – не всегда удаётся логически связанный материал уместить на одном слайде;

- *эффект раздвоенного внимания или эха* – одновременно демонстрируется информация на слайде и прослушивается речь преподавателя.

Однако на слайд должны выноситься только основные положения. Остальной текст можно поместить в комментарии слайдов.

Заключение. В целом, можно сказать, что применение мультимедийного оборудования, а именно компьютера и проектора, существенно увеличивает эффективность чтения лекций при обучении дисциплине «Механика жидкости и газа», снижая темп лекции и высобождая до 30 % времени на разъяснение наиболее сложного материала.

Литература

1. Яроц В.В., Шабловский А.С., Кузнецов В.С. Анализ влияния на рабочие характеристики прямоточного регулятора расхода его конструктивных параметров и условий эксплуатации / Электронное научно-техническое издание «Наука и образование». Инженерный вестник. М.: МГТУ им. Н.Э. Баумана, 2013. № 1. Режим доступа: http://engbul.bmstu.ru/doc/520072.html.

2. Кузнецов В.С., Шабловский А.С., Яроц В.В. Методика профессиональной переподготовки и повышения квалификации преподавателей и специалистов в области гидропневмоприводов в МГТУ им. Н.Э. Баумана / Инженерный вестник. Электронный научно-технический журнал. № 11, ноябрь 2012. Режим доступа: http://engbul.bmstu.ru/doc/496876.html.

3. Комкова Т.Ю., Яроц В.В. Роль куратора при подготовке инженеров машиностроительных специальностей вузов / Естественные и технические науки. № 6 (108), 2017. С. 97-99.

4. Ковальчук А.К., Яроц В.В. Проектирование исполнительного механизма и расчёт мощности приводов робота специального назначения / Естественные и технические науки. № 10 (100), 2016. С. 101-106.

СОСТАВ И СОДЕРЖАНИЕ МЕР РЕАГИРОВАНИЯ НА НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Бутин Александр Алексеевич
К.ф.-м.н., доцент кафедры информационных систем и защиты информации, Иркутский государственный университет путей сообщения, г. Иркутск (информационная безопасность)

АННОТАЦИЯ. Рассмотрены вопросы методологии расследования компьютерных инцидентов. Описывается регламент подготовки в возможному инциденту. Предложен алгоритм действий уполномоченных лиц (команды реагирования) при наступлении данного события.

ABSTRACT. The questions of the methodology of the investigation of computer incidents. Describes how to prepare for a possible incident. An algorithm of actions of authorized persons (response teams) upon the occurrence of this event is proposed.

Ключевые слова: информационная безопасность; компьютерный инцидент; расследование нарушения; группа реагирования на инцидент.

Keywords: information security; computer incident; investigation of the violation; incident response team.

Введение

Необходимо признать, что компьютерные преступления (инциденты) всегда совершались, совершаются и будут совершаться. Не существует системы защиты, которую нельзя обойти или сломать при наличии достаточного количества ресурсов. Ежегодно из-за компьютерных преступлений теряются огромные финансовые средства. Узнать об этом можно только после того, как компьютерный инцидент произойдет. Тогда нужно будет направить все силы на их расследование и выявить, как и кем он был совершен. Если этого не сделать, инцидент может повториться. Ниже приводится одна из возможных технологий расследования компьютерных инцидентов (наряду с опубликованными [1]-[5]).

Методология расследования компьютерных инцидентов. Данная методология предназначена для решения следующих задач:

- подтверждение или опровержение самого факта инцидента;
- сбор достоверной информации об инциденте;
- контроль за правильностью обнаружения и сбора фактов;
- защита гражданских прав, установленных законом и политикой информационной безопасности;
- минимизация влияния на основные операции организации;
- формирование гражданских и уголовных исков к нарушителям;
- создание точного отчета и полезных рекомендаций для будущих реакций на инциденты.

Предложенная методология реакции на инциденты состоит из следующих процедур:

Подготовка к инциденту - действия, которые позволяют подготовиться к возможным инцидентам.

Выявление инцидентов - исследование подозрительных инцидентов в системе безопасности.

Первоначальная реакция - проведение первоначального расследования, получение наиболее очевидных фактов (включая свидетельские показания) и подтверждение самого факта инцидента.

Формирование стратегии реакции на инцидент - на основе собранных фактов определяется наиболее эффективная реакция на инцидент, которая утверждается руководством компании.

Дублирование (судебное резервное копирование) - создание материалов для предоставления в судебные инстанции для расследования инцидента или получения дополнительных фактов.

Исследование - проведение подробного изучения того, что произошло, кто это сделал и как можно предотвратить подобные инциденты в будущем.

Реализация мер безопасности - активное воздействие на пострадавшую систему, предполагающее проведение мероприятий безопасности для изоляции и устранения последствий инцидента.

Сетевой мониторинг - исследование операций в сети для изучения и защиты пострадавших сетевых устройств.

Восстановление - возобновление нормального операционного состояния пострадавшей системы.

Отчет - точное документирование всех подробностей расследования и применение мероприятий безопасности.

Завершение работы - анализ предпринятых действий, изучение полученного опыта и устранение всех выявленных проблем.

Подготовка к инциденту. Компьютерные инциденты являются случайными, поэтому исследователи заранее не знают, когда произойдет очередной инцидент в системе безопасности.

При подготовке к инциденту предполагается не только получение программных инструментов и технологий, но и некоторые действия в системе и сети для предварительной подготовки к реакции на инцидент. Если исследователи могут немного контролировать компьютеры и сеть, то можно предпринять разнообразные предварительные действия, которые помогут ускорить реакцию после возникновения инцидента.

Подготовка отдельных хостов. На каждом защищаемом компьютере необходимо выполнить ряд мер, чтобы гарантировать быструю и эффективную реакцию на инцидент. Приведем несколько основных рекомендаций, которые помогут в любом исследовании наиболее эффективных методов реакции на инцидент:

- запись криптографической контрольной суммы всех важных файлов;
- усиление или разрешение аудита безопасности;
- создание индивидуальных средств безопасности каждого хоста;
- резервное копирование критически важных данных и хранение полученных архивных носителей в безопасном месте;
- обучение пользователей методом индивидуальной защиты хостов.

Кроме этого:

- необходимо убедиться, что используются последние версии операционной системы и приложений;
- следует отключить неиспользуемые службы;
- нужно внимательно отнестись к настройке конфигурационных параметров.

Подготовка сети. Многие современные средства сетевой защиты позволяют реагировать на компьютерные инциденты. При этом необходима регистрация событий, которая во многих случаях предоставит неоспоримые факты вторжения. Поэтому в реакции на инцидент важную роль играют сетевой администратор и администратор безопасности.

К мероприятиям сетевой безопасности относятся:

- установка брандмауэров (межсетевых экранов) и систем IDS (систем обнаружения вторжений);
- использование списков управления доступом в маршрутизаторах;
- создание сетевой топологии, облегчающей мониторинг;
- построение VPN (шифрование сетевого трафика).

Формирование команды реагирования на инцидент.

Целями команды реагирования на инциденты являются:

- реакция на все явные и предполагаемые компьютерные инциденты в организации и проведение установленной процедуры расследования;
- беспристрастное и полное расследование инцидента;

- быстрое подтверждение или опровержение факта нарушения безопасности систем;
- определение ущерба и области действия инцидента;
- контроль и подавление последствий инцидента;
- сбор фактов и документирование инцидента;
- прослеживание цепочки взаимосвязанных событий (защита фактов во время сбора информации об инциденте);
- привлечение дополнительных сил (при необходимости);
- защита гражданских прав, установленных законом и/или корпоративной политикой;
- обеспечение взаимодействия с органами правопорядка и судебными инстанциями;
- проведение сбора свидетельских показаний;
- предоставление руководству рекомендаций, основанных на фактах, выявленных при расследовании инцидента.

Все исследователи компьютерных инцидентов должны быть знакомы с соответствующими технологиями, а также иметь необходимую квалификацию для оценки преимуществ и недостатков различных стратегий реагирования. Руководитель команды реагирования должен оценить необходимые ресурсы еще до начала формирования команды.

Выявление инцидентов. Выявление является первым этапом реакции на инциденты. Перед выявлением исследователь должен быть уведомлен о возможности инцидента.

Предполагаемый инцидент может быть обнаружен различными программно-аппаратными средствами и организационными мерами. Вне зависимости от метода выявления инцидента, необходимо зафиксировать все полученные сведения. Необходимо зафиксировать очевидные факты, к которым относятся:

- текущие дата и время в момент совершения инцидента;
- список активных субъектов из числа персонала (пользователей);
- как получены сведения об инциденте (контактная информация лиц, обнаруживших инцидент);
- природа инцидента (как произошел инцидент);
- участвовавшее в инциденте технические средства и программное обеспечение.

Заполнив список уведомлений, следует привлечь команду реагирования на инцидент и обратиться в соответствующее подразделение компании.

Первоначальная реакция. Факты об инциденте являются ключевой информацией для выбора командой реагирования ответной реакции и методов восстановления после инцидента.

Команда реагирования обязана проверить сам факт инцидента, выявить системы, на который прямо или косвенно влияет инцидент, и оценить потенциальное влияние инцидента на функционирование организации. На основе этой информации можно принять правильное решение о реакции на инцидент.

Формирование стратегии реакции на инцидент. На данной фазе расследования уже собрано достаточно информации, чтобы точно подтвердить или опровергнуть сам факт инцидента.

Стратегия реагирования - это план для разрешения инцидента. В ней следует учесть различные факторы: тип атаки, политику организации, функции системы жертвы и т.д. Подобные факторы определяют тип реакции на инцидент, от реконфигурации системы до полного судебного дублирования (что обычно предпочтительнее).

Необходимо выбрать оптимальные методы реакции на инцидент. Такая стратегия должна учитывать технические и организационные аспекты, и в обязательном порядке должна быть утверждена руководством организации. При выборе стратегии необходимо оценить следующие аспекты: сколько ресурсов потребуется для реакции на инцидент, где создавать дублирующие данные для судебных органов. Кроме того, надо знать:

- насколько критическими были воздействия на системы (ущерб от инцидента в финансовым выражении);
- стали ли сведения об инциденте достоянием общественности;
- уровень доступа, полученный атакующим;
- предполагаемая квалификация атакующего;

Инциденты бывают разными, соответственно, различаются и стратегии реакции на инциденты. Следует учитывать факторы, не связанные с самим инцидентом. По большей части, к таким факторам относятся имеющиеся в организации финансовые и технические ресурсы, политические аспекты, действующее законодательство и т.д.

После получения некоторых сведений об атаке и доступных ресурсах для устранения ее последствий необходимо выбрать наиболее эффективную стратегию реакции на инцидент. Очевидно, что стратегия реакции на инцидент зависит от последствий самого инцидента (возможного/реального ущерба).

Предоставление руководству нескольких стратегий реакции на инцидент. В описании стратегии можно не прибегать к специальной технической терминологии, но точно отразить все "за" и "против" для каждого из предложенных вариантов стратегии, включая следующие показатели:

- время отключения сети;
- время отключения пользователей;
- обязательства организации по законодательным нормам;
- общественное мнение;
- наличие кражи интеллектуальной собственности.

Реакция на инцидент. Судебное дублирование.

Инцидент является основанием для выполнения судебного дублирования (резервного копирования для предоставления данных в органы правопорядка) поврежденных систем. Такое дублирование предполагает использование специализированного программного обеспечения, позволяющего сформировать "наилучшее копирование" материалов события. Альтернативой судебному дублированию может стать некий отчет о реакции на инцидент. Если известно местоположение файлов и, кто, когда, где и как использовал их во время инцидента, то возможно выборочное предоставление в судебные органы только относящихся к делу данных.

Многие компании, расследующие инциденты, не вполне осознают уровень тщательности сбора фактов об инциденте. Однако фаза судебного дублирования требует повышенного внимания, поскольку возникает сомнение в необходимости копирования данных по юридическим или административным причинам. Даже специалисты из государственных учреждений делают больше всего ошибок и погрешностей во время выполнения судебного дублирования, чем на остальных фазах расследования. Без подготовки к сбору необходимых данных и материалов об инциденте) компании могут сделать весьма серьезные ошибки на последующих фазах.

Как только принято решение о том, что нужно провести полномасштабное расследование, то для судебной экспертизы обычно необходимо получить изображение комппютеров, вовлеченных в инцидент. Есть несколько вариантов программного обеспечения, предназначенного для судебного дублирования; как коммерческие, так и некоммерческие инструментальные средства успешно справлялись с задачей, возложенной на них юридической системой.

Некоторые коммерческие программные средства судебного дублирования:

Продукт Safeback: практически в любом учреждении правоохранительных органов, занимающееся судебной экспертизой компьютеров, можно обнаружить, что следователи используют инструмент Safeback для судебного дублирования. Утилита Safeback, написанная для системы DOS, предназначена для резервного копирования, проверки и восстановления жестких дисков.

Утилита SnapBack первоначально была разработана как сетевая утилита резервного копирования, предназначенная для системных администраторов; однако, теперь она продается как инструмент судебного дублирования.

Продукт Norton Ghost, Personal Edition от компании Symantec, Ghost - популярный инструмент, позволяющий быстро и просто клонировать или копировать жесткие диски компьютерной системы. В дополнение к прямым изображениям в локальные файлы, Ghost может клонировать диски непосредственно между двумя компьютерами, использующими сеть, USB или параллельное подключение. Бесплатные средства позволяющие проводить судебное дублирование:

В связи с быстрым распространением операционных систем с открытым исходным кодом, типа Linux, OpenBSD, NetBSD и FreeBSD, широкой публике стал доступен целый набор инструментальных средств (и исходных текстов), которого прежде никогда не было.

Поскольку эти инструментальные средства бесплатны, а результаты, полученные их методами дублирования, можно импортировать почти в любой набор судебного анализа, можно предпочесть использование этих средств любым другим. Однако важно обратить внимание на то, что для использования этих инструментальных средств необходимо больше опыта и некоторые знания технических деталей файловой системы.

После того, как собраны улики, используя любое из средств, описанных выше, необходимо предусмотреть механизм проверки их законности. Если законность улик не заслуживает доверия, все усилия по их анализу и сбору могут рассматриваться как пустые траты. Поэтому, применяя контрольную сумму MD5 в качестве инструмента для снятия цифровых "отпечатков пальцев" для собранных улик, можно гарантировать, что данные, собранные несколько лет назад, в точности совпадают с версией, представленной в суде.

Исследование. На фазе исследования инцидента необходимо определить, кто, как, когда, где и зачем проводил действия, приведшие к инциденту. Исследование можно проводить по результатам судебного дублирования, изучения работающей системы или по отчетам из сетевого монитора. Вне зависимости от способа выполнения исследования вы реагируете на инцидент, спровоцированный людьми.

Виновник инцидента преследует цели разрушения, кражи, доступа, сокрытия или атаки по отношению к некоторому информационному ресурсу. Поэтому на фазе исследования нужно ответить на вопрос, какие ресурсы подверглись воздействию. Поскольку идентификация нарушителя редко связана с искаженным или разрушенным ресурсом, многие организации полностью сосредоточивают все усилия только на подвергшихся нападению ресурсах и способах их восстановления. Следовательно, главной целью фазы исследования инцидента становится использование специальных методов расследования инцидентов, связанных с различными системами и приложениями**.**

Реализация мер безопасности. Целью фазы реализации мер безопасности является проведение мероприятий, предотвращающих опасность будущих инцидентов. Другими словами, нужно устранить проблему. Изоляция и ограничения необходимы для реального восстановления или повторного построения системы. Если система не защищена от атак в будущем, то нельзя гарантировать "чистоту" восстановления.

Если собраны факты о возможных административных, уголовных и гражданских действиях, следует провести анализ этих данных еще до начала внедрения мер безопасности. При этом необходимо

быстро обезопасить систему (например, за счет изменения сетевой топологии, внедрения фильтрации пакетов или установки на хосте нового программного обеспечения). Однако если не провести в необходимом объеме анализ и документирование инцидента, то теряются ниточки к источнику и причинам инцидента, столь необходимые при его расследовании. Самым важным правилом является сохранение состояния системы на момент инцидента.

На фазе изоляции и ограничения важно предотвратить дальнейшие действия атакующих. Перед началом восстановления системы следует проверить, что злоумышленники уже не смогут получить доступ к ранее скомпрометированной системе, сети или информационному ресурсу. Для этого существуют разнообразные программные инструменты и технологии. Для изоляции и ограничения инцидентов, подобных вторжению в компьютер, можно просто отключить от сети скомпрометированный компьютер. Во многих случаях это позволяет предотвратить дальнейшие удаленные атаки.

Сетевой мониторинг. Сетевой мониторинг необходим для проведения расследования и восстановления. Для большей части инцидентов мониторинг должен начинаться на фазе первоначальной реакции и проводиться до полного завершения восстановления. Он преследует две цели:

- позволяет отслеживать действия атакующего для сбора дополнительных фактов;
- гарантирует отсутствие повторения уже произошедшего инцидента.

Необходимо начать с мониторинга той подсети, где находится целевая система. Другая область потенциального проведения мониторинга включает в себя всю сеть или сеть интранет. Мониторинг в этих областях предполагает выявление незаконных действий, исходящих из внутренней или внешней сети. Все области мониторинга можно легко определить по топологической карте сети, разработанной на этапе подготовки к инциденту.

На фазе исследования должна быть получена информация для ограничения рамок мониторинга. Хотя возможен полномасштабный мониторинг всех сетевых операций, обычно существуют ограничения, связанные со свободным местом па дисках и сетевой полосой пропускания. В этом случае можно регистрировать только входящий и исходящий трафик системы жертвы. Трафик из взломанного атакующим компьютера тоже необходимо отслеживать, поскольку многие хакеры оставляют черные ходы для создания подключений к взломанным системам.

Если известны IP адреса потенциальных источников атаки, необходим мониторинг трафика таких компьютеров. Если источник атаки находится в Интернете, может потребоваться мониторинг в рамках этой глобальной сети, а не только в подсети компьютера жертвы. Мониторинг в Интернете позволит выявить все действия в подозреваемых IP адресах источника любого хоста данной глобальной сети.

Восстановление. Целью фазы восстановления является воссоздание безопасного и рабочего состояния поврежденной системы. Это особенно важно для инцидентов с неавторизованным доступом, например, вторжения в компьютерные системы. Однако обычной является ситуация, когда уволившиеся из компании сотрудники оставляют для себя черные ходы в систему, сохраняют имена входа или продолжают иметь иные пути доступа к компьютерным системам. Время на выполнение фазы восстановления зависит от особенностей конкретного инцидента и выбранной стратегии восстановления. В общем случае восстановление проводится только после завершения процесса сбора фактов об инциденте и изоляции компьютера от атак в будущем.

Перед восстановлением системы следует оценить уровень компрометации, а также тип и местоположение скомпрометированной системы. На фазе исследования необходимо определить не только уровень компрометации, но и идентифицировать возможные действия атакующего внутри системы. Тип и местоположение скомпрометированной системы определяют реакцию, выполняемую в ответ на атаку. Если система находится в подсети вместе с другими хостами, придется исследовать все системы в подсети, поскольку внутренний трафик, скорее всего, был перехвачен атакующим, что может привести к компрометации остальных хостов в подсети.

Как отмечено выше, процесс восстановления сильно зависит от выбранной стратегии восстановления. В общем случае наиболее безопасным способом восстановления является переустановка системы с дистрибутивного компакт диска. Если атакующий загружал и исполнял на скомпрометированной системе неизвестный и опасный код, необходимо восстановление из "последней успешной" конфигурации, записанной в архивном носителе (так называемой "known good" конфигурации). После переустановки следует настроить систему для обеспечения ее безопасности, причем провести эту настройку еще до перевода системы в рабочее или интерактивное состояние.

Во время восстановления можно использовать резервные копии системы, но только в том случае, если известно, что инцидент произошел уже после создания архивной копии. Иначе можно восстановить не только систему, но и созданные в ней черные ходы, которые успешно были записаны в архивной копии после проведения атаки. Кроме того, восстановление из резервной копии приведет к воссозданию старых паролей, имен входа и уязвимостей скомпрометированной системы.

Отчет. Целью фазы отчета является создание набора документов об иниденте, причем, чем детальнее будет описание инцидента, тем лучше. Документирование инцидента следует начинать не в конце всего процесса, а с самого начала реакции на инцидент. В описании нужно отразить все фазы и операции реакции на инцидент.

Отчет об инциденте может стать основой для увольнения сотрудника или ареста хакера. Расследование многих компьютерных преступлений тянется годами, поэтому лучше сразу подробно и точно изложить все факты об административном, должностном или уголовном нарушении.

Фаза создания отчета предполагает действия, завершающие расследование инцидента и помогающие предотвратить их в будущем, а именно:

- участие в административном или уголовном расследовании. Возможно, субъекты, участвовавшие в расследовании инцидента, будут привлечены как свидетели для дачи показаний во время уголовного, административного или должностного следствия.
- формирование окончательного заключения об инциденте. Собранная документация поможет сформировать взвешенный и обоснованный заключительный отчет об инциденте, в котором необходимо отразить его особенности, предпринятые ответные действия, возможные причины и предложить рекомендации по их устранению в будущем;

Список литературы

1. *Домарев В.В*. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД ДС», 2001. 688 с.

2. *Кении Мандиа, Крис Просис*. Защита от вторжений: расследование компьютерных преступлений. М.: Издательство "ЛОРИ", 2005. 476 с.

3. *Козлов В. Е.* Теория и практика борьбы с компьютерной преступностью. Горячая Линия – Телеком, 2002. 336 с.

4. *Конеев И.Р., Беляев А.В*. Информационная безопасность предприятия. Спб.: БХВ-Петербург, 2005. 752 с.

5. *Скиба В. Ю., Курбатов В. А*. Руководство по защите от внутренних угроз информационной безопасности. Питер, 2008. 320 с.