Содержание:

ВВЕДЕНИЕ

Информационные системы часто подвергаются различным типам угроз, которые могут привести к различным видам ущерба, также к значительным финансовым потерям. Повреждения информационной безопасности могут варьироваться от небольших потерь до полного уничтожения информационной системы. Эффекты различных угроз значительно различаются: некоторые влияют на конфиденциальность или целостность данных, а другие влияют на доступность системы. В настоящее время организации изо всех сил пытаются понять, каковы угрозы их информационным ресурсам и как получить необходимые средства для борьбы с ними, которые по-прежнему создают проблему. В данной курсовой работе рассматриваются различные критерии классификации рисков безопасности информационных систем и дается обзор большинства моделей классификации угроз.

Информационная безопасность является наиболее сложным аспектом обработки информации. Организации, правительства и отдельные лица сталкиваются со многими рисками информационной безопасности. Для обеспечения эффективной защиты информации более эффективная идентификация, понимание и оценка угрозы безопасности и их характеристик имеют решающее значение для руководителей системной безопасности.

В данной курсовой работе рассматриваются политики безопасности в контексте требований к информационной безопасности и условия, в которых эти требования должны соблюдаться, рассматриваются общие принципы управления и анализируются типичные системные уязвимости.

Цель данной работы состоит в определении видов угроз информационной безопасности и их состава.

Для достижения поставленной цели необходимо решить следующий перечень задач:

1. Рассмотреть общие концепции ИБ

2. Изучить классификацию уязвимостей ИБ

3. Выделить основные источники, угрожающие ИБ

4. Рассмотреть вредоносное ПО как угрозу ИБ

Глава 1. Концепции информационной безопасности

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ - это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств». (Закон РФ «Об участии в международном информационном обмене»)

Угрозы информационной безопасности классифицируются по нескольким признакам:

по составляющим информационной безопасности (доступность, целостность, конфиденциальность), против которых, в первую очередь, направлены угрозы;

по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, персонал);

по характеру воздействия (случайные или преднамеренные, действия природного или техногенного характера);

по расположению источника угроз (внутри или вне рассматриваемой информационной системы).

Организации и люди, использующие компьютеры, могут описывать свои потребности в информационной безопасности и доверии к системам с учетом трех основных требований:

• Конфиденциальность: контроль над тем, кто получает информацию;

• Целостность: обеспечение того, что информация и программы изменяются только в установленном и разрешенном порядке; а также

• Доступность: обеспечение того, чтобы авторизованные пользователи продолжали доступ к информации и ресурсам.

Структура, в рамках которой организация стремится удовлетворить свои потребности в информационной безопасности, кодируется как политика безопасности. Политика безопасности является кратким изложением, лица, ответственные за систему (например, высшего руководства), информационных ценностей, ответственности по защите, а также организационные обязательства. Можно реализовать эту политику путем принятия конкретных мер, руководствующихся принципами управления, и использования конкретных стандартов, процедур и механизмов безопасности. И наоборот, выбор стандартов, процедур и механизмов должен руководствоваться политикой, чтобы быть наиболее эффективной.

Чтобы быть полезным, политика безопасности должна не только указывать необходимость безопасности (например, для конфиденциальности - данные должны раскрываться только уполномоченным лицам), но также учитывать диапазон обстоятельств, при которых эта потребность должна быть удовлетворена, и соответствующие операционные стандарты. Без этой второй части политика безопасности настолько универсальна, чтобы быть бесполезной (хотя вторая часть может быть реализована с помощью процедур и стандартов, установленных для реализации политики). В любом конкретном случае некоторые угрозы более вероятны, чем другие, и разумный разработчик политики должен оценивать угрозы, задавать для них уровень озабоченности и формулировать политику, с точки зрения которой следует противостоять угрозам. Например, до недавнего времени большинство политик безопасности не требовали удовлетворения требований безопасности перед лицом вирусной атаки, потому что эта форма атаки была необычной и не получила широкого распространения. Поскольку вирусы перешли от гипотетической к обычной угрозе, возникла необходимость переосмыслить такую политику в отношении методов распространения и приобретения программного обеспечения. Неявным в этом процессе является выбор руководством уровня остаточного риска, с которым он будет жить, уровень, который варьируется среди организаций.

ПОЛИТИКА БЕЗОПАСНОСТИ - ОТВЕТ НА ТРЕБОВАНИЯ К КОНФИДЕНЦИАЛЬНОСТИ, ЦЕЛОСТНОСТИ И ДОСТУПНОСТИ

Вес, придаваемый каждому из трех основных требований, описывающих потребности в информационной безопасности - конфиденциальности, целостности и доступности, сильно зависит от обстоятельств. Например, неблагоприятные последствия отсутствия системы должны быть частично связаны с требованиями времени восстановления. Система, которая должна быть восстановлена в течение часа после сбоя, представляет и требует более сложный набор политик и средств контроля, чем аналогичная система, которая не нуждается в восстановлении в течение двух-трех дней.

1.1.1 Конфиденциальность

Конфиденциальность - это требование, целью которого является предоставление конфиденциальной информации от неавторизованных получателей.

Секреты могут быть важны по соображениям национальной безопасности (данные ядерного оружия), правоохранительные органы, конкурентные преимущества (производственные издержки или планы торгов) или личная конфиденциальность (кредитные истории).

Поскольку масштаб угрозы очень широк в этом контексте, политика требует, чтобы системы были надежными перед лицом множества различных атак.

Оперативный контроль, который военные разработали в поддержку этого требования, включает автоматизированные механизмы обработки информации, которая имеет решающее значение для национальной безопасности. Такие механизмы требуют, чтобы информация была классифицирована на разных уровнях чувствительности и в изолированных отделениях, которые должны быть помечены этой классификацией и обрабатываться людьми, очищенными для доступа к определенным уровням и / или отделениям. В каждом уровне и купе человек с соответствующим разрешением должен также иметь знание, чтобы получить доступ. Эти процедуры являются обязательными: необходимо также разработать сложные процедуры для рассекречивания информации.

Некоторые коммерческие фирмы, например, классифицируют информацию как ограниченную, конфиденциальную и неклассифицированную. Даже если организация не имеет собственных секретов, она может быть обязана по закону или общей вежливости сохранять конфиденциальность информации о физических лицах. Например, медицинские записи могут требовать более тщательной защиты,

чем большинство конфиденциальных сведений. Таким образом, больница должна выбрать подходящую политику конфиденциальности, чтобы отстаивать свою фидуциарную ответственность в отношении записей пациентов.

В коммерческом мире конфиденциальность обычно охраняется механизмами безопасности, которые являются менее жесткими, чем механизмы безопасности сообщества национальной безопасности. Например, информация присваивается «владельцу», который контролирует доступ к нему. Такие механизмы безопасности способны справляться со многими ситуациями, но не настолько устойчивы к определенным атакам, как и механизмы, основанные на классификации и маркировки, отчасти потому, что нет возможности рассказать, где могут протекать копии информации. Например, при атаках троянских червей даже законные и честные пользователи могут быть обмануты раскрытием секретных данных. Коммерческий мир воспользовался этими уязвимостями в обмен на большую гибкость работы и производительность системы, которые в настоящее время связаны с относительно слабой безопасностью.

1.1.2 Целостность

Целостность - это требование, предназначенное для того, чтобы информация и программы были изменены только определенным и уполномоченным образом. Возможно, важно сохранить согласованные данные (например, в бухгалтерском учете в двух экземплярах) или разрешить изменение данных только в утвержденном порядке (как при снятии с банковского счета). Также может потребоваться указать степень точности данных.

Некоторые политики обеспечения целостности отражают озабоченность по поводу предотвращения мошенничества и заявляются с точки зрения управления. Например, любая задача, связанная с возможностью мошенничества, должна быть разделена на части, которые выполняются отдельными людьми, подход, называемый разделением обязанностей. Классическим примером является система закупок, которая состоит из трех частей: заказ, получение и оплата. Кто-то должен подписаться на каждом шаге, один и тот же человек не может подписаться на два шага, и записи могут быть изменены только фиксированными процедурами - например, счёт дебетовой карты и чек, написанный только для суммы одобренного и полученного заказа. В этом случае, хотя политика заявляется оперативно, то есть с точки зрения конкретных элементов управления, также явно

раскрывается модель угрозы.

Другие политики целостности отражают проблемы для предотвращения ошибок и упущений, а также контроля за последствиями изменения программы.

1.1.3. Доступность

Доступность - это требование, предназначенное для обеспечения бесперебойной работы систем и предоставления услуг авторизованным пользователям. С оперативной точки зрения это требование относится к адекватному времени отклика и / или гарантированной пропускной способности. С точки зрения безопасности он представляет собой способность защищать и восстанавливать повреждающее событие. Наличие надлежащим образом функционирующих компьютерных систем (например, для маршрутизации междугородных звонков или переадресации авиакомпаний) имеет важное значение для работы многих крупных предприятий, а иногда

для сохранения жизни (например, управление воздушным движением или автоматизированные медицинские системы).

Планирование на случай непредвиденных обстоятельств связано с оценкой рисков и разработкой планов по предотвращению или восстановлению от неблагоприятных событий, которые могут сделать систему недоступной.

Традиционное планирование на случай непредвиденных обстоятельств для обеспечения доступности обычно включает ответы только на стихийные бедствия (например, землетрясения) или случайные антропогенные события (например, утечка токсичного газа, препятствующая проникновению в объект). Тем не менее, планирование на случай непредвиденных обстоятельств должно также включать в себя предоставление ответов на злонамеренные действия, а не просто стихийные бедствия или несчастные случаи, и как таковые должны включать явную оценку угрозы, основанной на модели реального противника, а не на вероятностной модели природы.

Например, простая политика доступности обычно указывается следующим образом: «В среднем терминал должен опускаться менее 10 минут в месяц». Конкретный терминал (например, автоматический банкомат или клавиатура и экран агента бронирования) поднимается, если он отвечает

правильно в течение одной секунды стандартным запросом на обслуживание; в противном случае он не работает. Эта политика означает, что время ожидания на каждом терминале, усредненное по всем терминалам, должно составлять не менее 99,98 процента.

Политика безопасности для обеспечения доступности обычно принимает другую форму, как в следующем примере: «Никакие входы в систему любым пользователем, который не является авторизованным администратором, должны заставить систему прекратить обслуживать другого пользователя». Обратите внимание, что эта политика ничего не говорит о сбоях системы, за исключением случаев, когда они могут быть вызваны действиями пользователя. Вместо этого он идентифицирует определенную угрозу, злонамеренный или некомпетентный поступок обычного пользователя системы и требует, чтобы система выдержала это действие. В нем ничего не говорится о других способах, с помощью которых враждебная сторона может отказать в обслуживании, например, путем сокращения телефонной линии; для каждой такой угрозы требуется отдельное утверждение, указывающее, в какой степени сопротивление этой угрозе считается важным.

1.1.4. Примеры требований безопасности для разных приложений

Точные требования безопасности систем будут варьироваться от приложения к приложению даже в рамках одного приложения. В результате организации должны понимать свои приложения и анализировать соответствующие варианты для достижения соответствующего уровня безопасности.

Например, банкомат должен хранить конфиденциальные личные идентификационные номера (ПИН) как в хост-системе, так и во время передачи транзакции. Он должен защищать целостность учетных записей и отдельных транзакций. Защита конфиденциальности важна, но не критически. Наличие принимающей системы важно для экономического выживания банка, хотя и не для его фидуциарной ответственности.

С другой стороны, система коммутации телефонных аппаратов не имеет высоких требований к целостности отдельных транзакций, поскольку длительный ущерб не будет понесен из-за временной потери звонка или платежной записи. Однако

целостность программ управления и записей конфигурации имеет решающее значение. Без них функция переключения будет побеждена, а самый важный атрибут доступности - будет скомпрометирован. Телефонная система коммутации также должна сохранять конфиденциальность отдельных вызовов, не позволяя одному вызывающему абоненту подслушать другое.

Потребности в безопасности определяются больше тем, для чего используется система, чем тем, чем она является. Например, система набора должна будет обеспечить конфиденциальность, если она используется для публикации корпоративного запатентованного материала, целостности, если она используется для публикации законов и доступности, если она используется для публикации ежедневной газеты. Ожидается, что система совместного использования времени общего назначения обеспечит конфиденциальность, если она будет обслуживать разнообразную клиентуру, целостность, если она используется в качестве среды разработки для программного обеспечения или инженерных проектов, и доступность в той мере, в которой ни один пользователь не может монополизировать услугу, и что потерянные файлы будут восстановлены.

1.1.5. Выбор средств для безопасной информации и операций

Установление политики безопасности является основной обязанностью руководства внутри организации. Руководство несет ответственность за сохранение и защиту активов и поддержание качества обслуживания. С этой целью он должен обеспечить, чтобы операции проводились разумно перед лицом реалистичных рисков, связанных с надежными угрозами. Эта обязанность может быть выполнена путем определения высокоуровневых политик безопасности, а затем перевода этих политик в конкретные стандарты и процедуры для выбора и воспитания персонала, для проверки и аудита, для создания планов на случай непредвиденных обстоятельств и т. д. Благодаря этим действиям руководство может предотвращать, обнаруживать и восстанавливать убытки. Восстановление зависит от различных форм страхования: резервных записей, резервных систем и сайтов обслуживания, самострахования по резервам наличности и приобретенного страхования для компенсации стоимости восстановления.

1.1.6. Предотвращение нарушений основных принципов безопасности

Элементы управления управлением предназначены для того, чтобы вести операции в правильных направлениях, предотвращать или обнаруживать вредные и вредные ошибки, и давать раннее предупреждение об уязвимостях. Организации почти в каждой линии усилий создали механизмы контроля, основанные на следующих ключевых принципах:

Индивидуальная подотчетность,

Аудит и

Разделение долга.

Эти принципы, признанные в той или иной форме на протяжении веков, являются основой пред компьютерными рабочими процедурами, которые очень хорошо поняты.

Индивидуальная подотчетность отвечает на вопрос: кто несет ответственность за это заявление или действие? Его цель - следить за тем, что произошло, кто имел доступ к информации и ресурсам и какие действия были предприняты. В любой реальной системе существует много причин, по которым фактическая операция может не всегда отражать первоначальные намерения владельцев: люди делают ошибки, система имеет ошибки, система уязвима для определенных атак, широкая политика не была переведена правильно в подробные спецификации, владельцы передумали, и так далее. Когда все идет не так, нужно знать, что произошло, и кто является причиной. Эта информация является основой для оценки ущерба, восстановления утраченной информации, оценки уязвимости и инициирования компенсационных действий, таких как судебное преследование, вне компьютерной системы.

Чтобы поддерживать принцип индивидуальной отчетности, требуется услуга, называемая *аутентификацией пользователя*. Без надежной идентификации не может быть никакой ответственности. Таким образом, аутентификация является важной основой информационной безопасности. Многие системы были проникнуты, когда слабые или плохо управляемые службы аутентификации были скомпрометированы, например, путем угадывания неправильно выбранных паролей.

Основной услугой, предоставляемой аутентификацией, является информация о том, что конкретный пользователь сделал заявление или действие. Иногда, однако, необходимо обеспечить, чтобы пользователь не смог впоследствии утверждать, что заявление, приписываемое ему, было подделано и что он так и не сделал этого. В мире бумажных документов это цель нотариального удостоверения; нотариус предоставляет независимые и заслуживающие доверия доказательства, которые будут убедительными даже после многих лет, что подпись является подлинной и не подделанной. Эта более строгая форма аутентификации, предлагается сегодня несколькими компьютерными системами, хотя юридическая потребность в ней может быть предусмотрена, поскольку компьютерные операции становятся более распространенными в бизнесе.

Аудиторские услуги поддерживают подотчетность и, следовательно, ценны для руководства и для внутренних или внешних аудиторов. Учитывая реальность, что каждая компьютерная система может быть взломана изнутри,

и что многие системы также могут быть скомпрометированы, если можно получить скрытый доступ, подотчетность является крайне важным последним средством. Службы аудита составляют и ведут учетные записи, необходимые для поддержки отчетности. Обычно они тесно связаны с аутентификацией и авторизацией (служба для определения того, доверяет ли пользователь или система для данной цели), так что каждая аутентификация записывается, как и каждый попытка доступа, независимо от того, разрешено или нет. Учитывая критическую роль аудита, аудиторские устройства иногда являются первой целью злоумышленника и должны соответственно защищаться.

Записи аудита системы, которые часто называют аудиторским следом, имеют другие потенциальные возможности, помимо установления подотчетности. Возможно, например, можно проанализировать контрольный журнал для подозрительных шаблонов доступа и таким образом обнаружить неправильное поведение как законных пользователей, так и маскарадов. Основными недостатками являются обработка и интерпретация данных аудита.

Системы могут постоянно меняться, когда персонал и оборудование приходят и уходят, а приложения развиваются. С точки зрения безопасности, изменяющаяся система вряд ли будет улучшающейся системой. Чтобы принять активное участие в постепенной эрозии мер безопасности, можно добавить динамически собранный контрольный журнал (который полезен для выяснения произошедшего) со

статическими аудитами, которые проверяют конфигурацию, чтобы убедиться, что она не открыта для атаки. Статические службы аудита могут проверить, что программное обеспечение не изменилось, правильные настройки контроля доступа к файлам, устаревшие учетные записи пользователей были отключены, что входящие и исходящие линии связи правильно включены, что пароли трудно догадаться и так далее. Наряду с вирусными шашками на рынке существует несколько статических инструментов аудита.

Устоявшаяся практика *разделения обязанностей* указывает, что важные операции не могут выполняться одним человеком, но вместо этого требуется согласие (по крайней мере) двух разных людей. Таким образом, разделение обязанностей укрепляет безопасность, предотвращая любые односторонние подрывные действия органов управления. Это также может помочь уменьшить ошибки, обеспечив независимую проверку действий одного человека другим.

Разделение долга является примером более широкого класса средств контроля, которые пытаются определить, кому доверяют для данной цели. Такой тип управления обычно известен как *авторизация* пользователя. Авторизация определяет, является ли конкретный пользователь, который был аутентифицирован как источник запроса, чтобы что-то сделать, доверен для этой операции. Авторизация может также включать элементы управления в то время, когда что-то может быть сделано (только в рабочее время) или компьютерный терминал, с которого он может быть запрошен (только тот, который находится за столом менеджера).

Точно так же, как цель индивидуальной отчетности требует механизма более низкого уровня для аутентификации пользователей, так и контроль авторизации, такой как разделение обязанностей, требует механизма более низкого уровня для обеспечения что пользователи имеют доступ только к правильным объектам. Внутри компьютера эти механизмы обеспечения обычно называются *механизмами контроля доступа*.

1.1.7. Ответ на нарушения безопасности

Элементы управления восстановлением предоставляют средства для реагирования на нарушения безопасности, а не для предотвращения. Использование механизма восстановления не обязательно указывает на недостаток системы; для некоторых угроз обнаружение и восстановление могут быть более экономичными, чем

попытки полной профилактики. Восстановление от нарушения безопасности может включать в себя принятие дисциплинарных или юридических мер, уведомление о побочных эффектах или изменение политики, например. С технической точки зрения нарушение безопасности имеет много общего с отказом, который возникает из-за неисправности оборудования, программного обеспечения или операций. Обычно некоторые работы должны быть отброшены, и некоторые или все системы должны быть возвращены в чистое состояние.

Нарушения безопасности обычно влекут за собой дополнительные усилия по восстановлению. В отличие от пресловутой молнии, нарушения безопасности могут рассчитываться дважды, если только маршрут компромисса не будет отключен. Должны быть установлены причины. Были ли скомпрометированы пароли? Являются ли резервные копии чистыми? Повлияли ли некоторые действия пользователя на компромисс системы? И, возможно, потребуется сделать дополнительную работу - сменить все пароли, пересоздать систему из оригинальных копий, отключить определенные каналы связи или ввести процедуры аутентификации на них или провести обучение пользователей - для предотвращения повторения.

Глава 2. Риски и уязвимости.

Риски возникают из-за того, что атака может использовать некоторую уязвимость системы. То есть каждая уязвимость системы отражает потенциальную угрозу с соответствующими рисками.

2.1 Классификация уязвимостей безопасности

Угрозы информационной безопасности не проявляются независимо, а путем возможного контакта с пробелами в системе защиты или факторами уязвимости. Угроза приводит к сбою в работе систем на конкретном носителе.

Основные уязвимости вызваны следующими факторами:

Недостатки программного обеспечения или оборудования

Различные характеристики структуры автоматизированных систем в информационном потоке

Некоторые операционные процессы системы неадекватны

Неточность протоколов обмена информацией и интерфейса

Трудные условия эксплуатации и условия, в которых находится информация.

Чаще всего источники угроз запускаются, чтобы получить незаконную выгоду после повреждения информации. Однако также возможен случайный эффект угроз из-за недостаточной защиты и массового нападения угрожающего фактора.

Уязвимость может быть:

Случайная

Объективная

Субъективная

Если устранить или, по крайней мере, уменьшить влияние уязвимостей, то можно избежать значительной угрозы, которая может повредить систему хранения.

Случайные уязвимости

Эти факторы различаются в зависимости от непредвиденных обстоятельств и особенностей информационной среды. Их практически невозможно предсказать в информационном пространстве, но мы должны быть готовы быстро их устранить. Инженерно-технические исследования или ответная атака помогут смягчить следующие проблемы:

1. Системные сбои:

Вызывается сбоями технических средств на разных уровнях обработки и хранения информации (в том числе ответственных за производительность системы и доступ к ней).

Неисправности и устаревшие элементы (размагничивание носителей данных, таких как дискеты, кабели, линии подключения и микрочипы).

Неисправности различного программного обеспечения, которое поддерживает все ссылки в цепочке хранения и обработки информации (антивирусы, приложения и сервисные программы).

Неисправности вспомогательного оборудования информационных систем (сбои передачи электроэнергии).

2. Факторы, ослабляющие информационную безопасность:

Повреждение коммуникаций, таких как водоснабжение, электричество, вентиляция и канализация.

Неисправности ограждающих устройств (ограждения, стены в зданиях, корпус оборудования, где хранится информация).

Объективные уязвимости

Они зависят от технической конструкции оборудования, которое установлено на объекте, требующем защиты, а также его характеристик. Невозможно избежать всех этих факторов, но их частичное устранение может быть достигнуто с помощью технических приемов в следующих случаях:

1. Что касается технических средств эмиссии:

Электромагнитные методы (побочная эмиссия и сигналы от кабельных линий, элементы технических средств).

Звуковые версии (акустические или с вибрационными сигналами).

Электрическое (проскальзывание сигналов в цепи электрических сетей, через индукцию в линии и проводники из-за неравномерного распределения тока).

2. Активировано:

Вредоносное ПО, незаконные программы, технологические выходы из программ, которые вместе называются «инструменты имплантатов».

Аппаратные имплантаты: вводятся непосредственно в телефонные линии, электрические сети или помещения.

3. Из-за характеристик защищаемого объекта:

Местоположение объекта (видимость и отсутствие контролируемой зоны вокруг информационного объекта, наличие вибрации или звука, отражающих элементы вокруг объекта, наличие удаленных элементов объекта).

Организация каналов обмена информацией (использование радиоканалов, аренда частот или использование общих сетей).

4. Те, которые зависят от характеристик носителей:

Детали с электроакустическими модификациями (трансформаторы, телефонные устройства, микрофоны и громкоговорители, катушки индуктивности).

Элементы под воздействием электромагнитного поля (носители, микросхемы и другие элементы).

Субъективные уязвимости

В большинстве случаев уязвимости этого подтипа являются результатом неадекватных действий сотрудников на уровне разработки системы хранения и защиты. Устранение таких факторов возможно с помощью аппаратного и программного обеспечения:

1. Неточности и грубые ошибки, которые нарушают информационную безопасность:

На этапе загрузки готового программного обеспечения или разработки предварительного алгоритма, а также при его использовании (возможно, при ежедневном использовании или при вводе данных).

При управлении программами и информационными системами (трудности в обучении работе с системой, индивидуальная настройка служб, манипулирование информационными потоками).

Во время использования технического оборудования (во время включения или выключения используется устройство для передачи или получения информации).

2. Неисправности системы в информационной среде:

Режим защиты персональных данных (проблема может быть вызвана уволенными сотрудниками или текущими сотрудниками в нерабочее время, когда они получают несанкционированный доступ к системе).

Режим безопасности и охраны (при доступе к объектам или техническим устройствам).

При работе с устройствами (неэффективное использование энергии или неправильное обслуживание оборудования).

При работе с данными (смена информации, ее сохранение, поиск и уничтожение данных, устранение дефектов и неточностей).

Оценка уязвимости

Специалисты должны учитывать и оценивать каждую уязвимость. Поэтому важно определить критерии для оценки угрозы ущерба для защиты и вероятности ее поломки или обхода. Индикаторы рассчитываются с использованием ранжирования. Существуют три основных критерия:

Доступность - это критерий, который учитывает, насколько удобно для источника угрозы использовать определенный тип уязвимости для нарушения информационной безопасности. Индикатор включает технические данные носителя информации (такие как размеры оборудования, его сложность и стоимость, а также возможность использования неспециализированных систем и устройств для взлома информационных систем).

Фатальность - это характеристика, которая оценивает влияние уязвимости на способность программистов справляться с последствиями угрозы для информационных систем. При оценке только объективных уязвимостей необходимо определить их информационную емкость или возможность передавать в другое место полезный сигнал с конфиденциальными данными, не деформируя его.

Количество является характеристикой подсчета частей систем хранения и реализации информации, которые подвержены любой уязвимости.

Глава 3. Источники, угрожающие информационной безопасности.

Угрозы в обход защиты информационной безопасности можно разделить на несколько категорий. Концепция категорий является обязательной, поскольку она упрощает и систематизирует все без исключения факторы. Основные параметры:

1. Степень интенсивности вмешательства в систему защиты информации:

Угрозы, вызванные невольными сотрудниками в информационном измерении

Угрозы, вызванные мошенниками для личной выгоды.

2. Признаки возникновения:

Угроза искусственной информационной безопасности, вызванная человеческими руками

Природные факторы угрозы, не зависящие от систем защиты информации, вызванных стихийными бедствиями.

3. Классификация непосредственной причины угрозы. Исполнитель может быть:

Лицо, которое раскрывает конфиденциальную информацию, подкупив сотрудников компании.

Естественный фактор, такой как катастрофа или местная катастрофа.

Программное обеспечение с использованием специализированных устройств или внедрение вредоносного кода в технические средства, которые нарушают работу системы.

Случайное удаление данных, авторизованных программных и аппаратных средств, отказ операционной системы.

4. Тяжесть угроз на информационных ресурсах:

На момент обработки данных в информационном пространстве (рассылки от вирусных утилит).

Во время получения новой информации.

Независимо от производительности системы хранения информации (в случае взлома шифров или криптографической защиты информации).

Существует еще одна классификация угроз ИС. Он основан на других параметрах и также используется во время анализа сбоя системы или взлома. Учитывается следующее:

Статус источника угрозы:

В самой системе, что приводит к операционным ошибкам и сбоям.

В пределах видимости, например, использование прослушивающего оборудования, кража информации в печатной форме или кража записей от носителей данных.

Мошенничество за пределами зоны обслуживания. Информация может быть захвачена во время передачи по каналам связи, случайный захват от акустического или электромагнитного излучения устройств.

Степень воздействия:

Активная угроза безопасности, которая изменяет структуру и характер системы, например, использование вредоносных вирусов или троянов.

Пассивная угроза крадет информацию путем копирования, иногда скрывается. Он не вносит изменений в информационную систему.

возмещение убытков

Тяжесть и проявления ущерба могут быть разными:

Не денежный и денежный ущерб, причиненный лицам, чья информация была похищена.

Финансовые потери в отношении расходов, понесенных при восстановлении информационных систем.

Материальные затраты, связанные с неспособностью выполнять работу, поскольку система информационной безопасности была изменена.

Ущерб, связанный с репутацией бренда и вызывающий нарушенные отношения на глобальном уровне.

Лицо, совершившее преступление (получивший несанкционированный доступ к информации или взломанный в систему защиты), может нанести ущерб. Повреждение может также происходить независимо от субъекта, владеющего информацией, но из-за внешних факторов и воздействий (технологических и стихийных бедствий). В первом случае ответственность лежит на предмете, определяются составляющие преступления, а правонарушители наказываются в судебном порядке. Действие может быть совершено:

С преступным намерением (прямым или косвенным)

По неосторожности (без умышленного вреда).

Наказание за преступление выбирается в соответствии с действующим национальным законодательством или в соответствии с уголовным кодексом в первом случае. Если преступление совершено по неосторожности, а нанесенный ущерб мал, дело будет под гражданским, административным или арбитражным правом.

3.1. КОНФИДЕНЦИАЛЬНОСТЬ

Забота о неприкосновенности частной жизни возникает в связи с безопасностью компьютерных систем двумя разными способами:

необходимость защиты личной информации о людях, которые хранятся в компьютерных системах; а также

необходимость обеспечения того, чтобы сотрудники организации соблюдали политику и процедуры организации.

Первая необходимость в обеспечении конфиденциальности; разработка политики и механизмов обеспечения конфиденциальности должна укрепить ее. Во-вторых, однако, это случай, когда потребность не связана с конфиденциальностью; сильные меры аудита или надзора могут ущемлять неприкосновенность частной жизни тех, чьи действия наблюдаются. Важно понимать оба аспекта конфиденциальности.

Защита информации о лицах

Закон о конфиденциальности основан на пяти основных принципах, которые были общеприняты в качестве основных критериев конфиденциальности:

Не должно быть никакой системы хранения личных данных, само существование которой является тайной.

Для людей должен быть способ узнать, какая информация о них записана и как она используется.

Необходимо, чтобы люди могли предотвратить информацию

получая о них по одной цели от использования или предоставления для других целей без их согласия.

Должна быть возможность для отдельных лиц исправить или изменить запись идентифицируемой информации о них.

Любая организация, создающая, поддерживающая, использующая или распространяющая записи идентифицируемых персональных данных, должна гарантировать, что данные используются по назначению и должны принимать меры предосторожности для предотвращения неправильного использования данных.

Даже в тех случаях, когда большинство организаций предпринимают разумные, добросовестные усилия по защите конфиденциальности личной информации, находящейся в их вычислительных системах, система с возможностью компрометации и контроля доступа к данным часто позволяет нарушителям нарушать личную неприкосновенность частной жизни.

Конфиденциальность сотрудников на рабочем месте.

Необходимость работодателя обеспечить соответствие сотрудников политикам и процедурам требует некоторой проверки руководством деятельности сотрудников, связанных с использованием вычислительных ресурсов компании; сколько и какие проверки подлежат обсуждению. Общая предпосылка управления заключается в том, что, если политика или процедура не будут соблюдаться, она в конечном итоге не будет соблюдаться, что приведет к эрозии уважения и соблюдения других политик и процедур. Например, политику, в которой указывается, что вычислительные ресурсы компании будут использоваться только для надлежащих деловых целей. Пользователи удостоверяются при запуске своей работы (или при внедрении политики), которую они понимают и будут соблюдать эту политику и другие. Случайные выборочные проверки пользовательских файлов аналитиками информационной безопасности могут проводиться для обеспечения того, чтобы личные бизнес-элементы, игры и т. д. не были размещены на вычислительных ресурсах компании. Дисциплинарные меры могут возникнуть в случае обнаружения нарушений политики.

Вышеизложенная ситуация сама по себе не связана с безопасностью. Тем не менее, один из предложенных способов повышения уровня безопасности системы включает в себя мониторинг действий работников с целью выявления, например, форм деятельности, которые предполагают, что пароль сотрудника был украден. Этот уровень мониторинга дает возможность наблюдать за всеми аспектами деятельности работников, а не только с деятельностью, связанной с

безопасностью, и значительно сократить ожидаемые работники для обеспечения конфиденциальности на работе.

Некоторые руководители утверждают, что работник при выполнении связанной с работой деятельности должен ожидать произвольного надзорного наблюдения и обзора и что в этом контексте нет ожиданий конфиденциальности. Этот аргумент сочетает в себе соображения конфиденциальности с соображениями стиля управления и философии, которые выходят за рамки. Тем не менее, что имеет отношение к этому отчету, является тот факт, что компьютерные и коммуникационные технологии способствуют большему контролю и наблюдению за сотрудниками и что потребности в обеспечении безопасности компьютеров и коммуникаций мотивируют мониторинг и наблюдение, некоторые из которых могут использовать компьютерные технологии.

Отслеживая или контролируя действия компьютеров отдельных лиц, можно нарушить конфиденциальность лиц, которые не находятся в отношениях с работниками, но чаще всего являются клиентами организации или граждан страны.

Компьютерные системы как механизм не обеспечивают защиту людей в этих ситуациях; как было отмечено выше, компьютеры, даже очень безопасные компьютеры, являются всего лишь механизмом, а не политикой. Действительно, очень безопасные системы могут действительно ухудшить проблему, если присутствие этих механизмов ложно побуждает людей доверить критическую информацию таким системам.

Существует важное различие между политикой и механизмом. Компьютерная система является механизмом, но, если нет никакой принудительной политики, механизм не обеспечивает никакой защиты. Только при наличии принудительной политики может возникнуть любая защита или обеспечение. В то время как пять основных принципов, которые составляют признанную политику конфиденциальности, обобщены выше, безопасность, как она обсуждается в этом отчете, не предусматривает или не применяет такую политику, за исключением узкого смысла защиты системы от враждебных злоумышленников. Защита системы (или информации, которую она содержит) от владельца системы - совершенно другая проблема, которая станет все более важной, поскольку мы приступим к еще большему использованию компьютеров в нашем обществе.

Глава 4. Основные типы угроз компьютерной безопасности.

Программные атаки означают атаку вирусов, червей, троянских коней и т. д. Многие пользо
это все те же вещи. Но они не одинаковы и ведут себя по-разному.

Вредоносное ПО представляет собой комбинацию из двух терминов -
вредоносных и программных. Таким образом, вредоносное ПО в основном означает вредонс

1. Инфекционные методы

2. Вредоносные действия

4.1 Вредоносное ПО

Вирус. Термин «вирус» в применении к компьютерам был предложен Фредом Коэном из Университета Южной Калифорнии. Исторически первое определение, которое дал Ф. Коэн*: «Компьютерный вирус - это программа, которая может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению»*. Ключевыми понятиями в определении компьютерного вируса являются способность реплицироваться, подключая их к программе на главном компьютере, например, песни, видео и т. д., а затем они путешествуют по всему Интернету.

«Червь» Термин «червь» пришел из научно-фантастического романа Джона Бруннера «По бурным волнам». Этот термин используется для именования программ, которые подобно ленточным червям перемещаются по компьютерной сети от одной системы к другой.

Черви также самовоспроизводятся, но они не привязываются к программе на главном компьютере. Самая большая разница между вирусом и червями заключается в том, что черви знают сеть. Они могут легко перемещаться с одного компьютера на другой, если сеть доступна, и на целевой машине они не нанесут большого вреда, они, например, будут потреблять пространство на жестком диске, что замедляет работу компьютера.

Trojan - Понятие трояна полностью отличается от вирусов и червей. Название «Троян» происходит из сказки «Троянский конь» в греческой мифологии, в котором объясняется, как греки смогли войти в укрепленный город Трой, скрыв своих солдат в большой деревянной лошади, подаренной троянцам в качестве подарка. Трояны очень любили лошадей и слепо верили в подарок. Ночью солдаты вышли и атаковали город изнутри.

Их цель - скрывать себя внутри программного обеспечения, которое кажется законным, и когда это программное обеспечение выполняется, они будут выполнять свою задачу либо воровство информации, либо любую другую цель, для которой они предназначены.

Они часто предоставляют бэкдор- шлюз для вредоносных программ или злонамеренных пользователей для входа в систему и кражи ценных данных без ведома и разрешения. Примеры включают в себя FTP-трояны, прокси-трояны, трояны удаленного доступа и т. д.

Боты -: можно рассматривать как продвинутые для червей. Это автоматизированные процессы, которые предназначены для взаимодействия через Интернет без необходимости взаимодействия с людьми. Они могут быть хорошими или плохими. Вредоносный бот может заразить один хост, а после заражения создаст соединение с центральным сервером, который предоставит команды всем зараженным хостам, подключенным к этой сети Botnet.

4.2 Вредоносное ПО на основе действий:

Adware - рекламное ПО не является злонамеренным, но они нарушают конфиденциальность пользователей. Они отображают рекламу на рабочем столе компьютера или внутри отдельных программ. Они поставляются с бесплатным программным обеспечением, таким образом, основным источником дохода для таких разработчиков. Они отслеживают ваши интересы и отображают релевантные объявления. Злоумышленник может внедрять вредоносный код внутри программного обеспечения, а рекламное ПО может отслеживать действия системы и даже подвергать риску.

Spyware - это программа или мы можем сказать программное обеспечение, которое контролирует вашу деятельность на компьютере и раскрывает собранную информацию заинтересованной стороне. Шпионские программы обычно удаляются

троянами, вирусами или червями. Как только они упали, они устанавливаются сами и сидят молча, чтобы избежать обнаружения.
Одним из наиболее распространенных примеров шпионских программ является KEYLOGGER. Основной задачей кейлоггера является запись пользовательских нажатий клавиш с меткого времени. Таким образом, захватывая интересную информацию, такую как имя пользователя, пароли, данные кредитной карты и т. д.

Ransomware - это тип вредоносного ПО, который либо зашифрует файлы, либо заблокирует компьютер, делая его недоступным либо частично, либо полностью. Затем отобразится экран с запросом денег, т. е. выкуп в обмен.

Scareware - он маскируется как инструмент, помогающий исправить систему, но, когда программное обеспечение будет выполнено, оно заразит систему или полностью уничтожит ее. Программное обеспечение отобразит сообщение, чтобы напугать вас и заставить предпринять какие-то действия, например, оплатить их, чтобы исправить систему.

Rootkits - предназначены для получения корневого доступа, или мы можем сказать, административные привилегии в пользовательской системе. Получив доступ к корневому файлу, эксплуататор может сделать что угодно: от кражи личных файлов до личных данных.

Зомби - они работают аналогично Spyware. Механизм заражения такой же, но они не шпионят и не крадут информацию, а ждут команды от хакеров.

Кража интеллектуальной собственности означает нарушение прав интеллектуальной собственности, таких как авторские права, патенты и т. д.

Кража личных данных означает действовать кем-то другим, чтобы получить личную информацию человека или получить доступ к важной информации, к которой у них есть доступ к учетной записи компьютера или социальной сети человека, путем входа в учетную запись, используя свои учетные данные.

В наши дни кража оборудования и информации увеличивается благодаря мобильности устройств и увеличению информационной емкости.

Саботаж означает уничтожение веб-сайта компании, чтобы вызвать потерю доверия со стороны его клиента.

Вымогательство информации означает кражу имущества или информации компании для получения оплаты в обмен. Например, ransomware может блокировать файл жертв, делая их недоступными, тем самым заставляя жертву произвести платеж в обмен. Только после оплаты файлы жертвы будут разблокированы.

Это атаки старого поколения, которые продолжаются в эти дни и с каждым годом. Кроме того, существует множество других угроз. Ниже приведено краткое описание этих угроз нового поколения.

Технология со слабой безопасностью - с развитием технологий, с каждым днем на рынке выпускается новый гаджет. Но очень немногие полностью защищены и следуют принципам информационной безопасности. Поскольку рынок является очень конкурентоспособным, фактор безопасности скомпрометирован, чтобы сделать устройство более актуальным. Это приводит к краже данных / информации с устройств

Атаки в социальных сетях - в этом киберпреступники идентифицируют и заражают группу веб-сайтов, которые посещают лица определенной организации, чтобы украсть информацию.

Мобильное вредоносное ПО - есть высказывание, когда есть возможность подключения к Интернету, будет опасность для безопасности. То же самое касается мобильных телефонов, где игровые приложения предназначены для привлечения клиентов для загрузки игры и непреднамеренно они будут устанавливать вредоносное ПО или вирус в устройство.

Устаревшее программное обеспечение безопасности. С появлением новых угроз, возникающих каждый день, обновление программного обеспечения безопасности является обязательным условием для обеспечения полностью защищенной среды.

Корпоративные данные о персональных устройствах. В эти дни каждая организация следует правилу BYOD. BYOD означает, что ваше устройство, например, ноутбуки, планшеты, на свое рабочее место. Очевидно, что BYOD создает серьезную угрозу безопасности данных, но из-за проблем с производительностью организации утверждают, что они принимают это.

Социальная инженерия - это искусство манипулирования людьми, чтобы они отказались от своей конфиденциальной информации, такой как данные банковского счета, пароль и т. Д. Эти преступники могут обмануть вас в

предоставлении вашей частной и конфиденциальной информации, или они получат ваше доверие, чтобы получить доступ к вашему компьютеру, чтобы установить вредоносное программное обеспечение, которое даст им контроль над вашим компьютером. Например, электронная почта или сообщение от вашего друга, которое, вероятно, не было отправлено вашим другом. Криминал может получить доступ к вашему устройству друзей, а затем, обратившись к списку контактов, он может отправить зараженную электронную почту и сообщение всем контактам. Поскольку сообщение / адрес электронной почты от известного человека, получателя, будет определенно проверять ссылку или вложение в сообщении, таким образом, непреднамеренно заражая компьютер.

ЗАКЛЮЧЕНИЕ

В идеале комплексный спектр мер безопасности обеспечит надлежащее сохранение конфиденциальности, целостности и доступности компьютерных систем. На практике невозможно сделать железные гарантии. Единственный рецепт идеальной безопасности - отличная изоляция: ничего, ничего. Это нецелесообразно, поэтому политики безопасности всегда будут отражать компромисс между стоимостью и риском. Активы, подлежащие защите, должны быть классифицированы по стоимости, уязвимости по важности и риски по степени серьезности, а защитные меры должны быть установлены соответствующим образом. Остаточные уязвимости должны быть распознаны.

Поскольку безопасность является феноменом слабой связи, программа обеспечения безопасности должна быть многомерной. Независимо от целей политики безопасности, нельзя полностью игнорировать любое из трех основных требований: конфиденциальность, целостность и доступность, которые поддерживают друг друга. Например, для защиты паролей необходима конфиденциальность. Пароли, в свою очередь, способствуют целостности системы, контролируя доступ и обеспечивая основу для индивидуальной отчетности. Соблюдение конфиденциальности должно быть невосприимчивым к несанкционированному вмешательству. И в случае, если что-то пойдет не так, должно быть возможно, чтобы административный и обслуживающий персонал мог вмешаться, чтобы исправить ситуацию - проблема доступности.

Система представляет собой взаимозависимый набор компонентов, который можно рассматривать как единое целое. Компьютерная операционная система, приложение, такое как компьютеризированная система оплаты труда, локальная сеть инженерных рабочих станций или общенациональная сеть для электронного перевода средств, каждая может рассматриваться как система, и любая из них может зависеть от других. Все это связано с физическими элементами и людьми, а также компьютерами и программным обеспечением. Физическая защита включает в себя экологический контроль, такой как охранники, замки, двери и ограждения, а также защита от пожаров, наводнений и других природных опасностей.

Хотя программа обеспечения безопасности должна разрабатываться с целостной точки зрения, сама программа не обязательно должна быть монолитной. Лучше всего действовать по принципу «разделяй и властвуй», отражая классический принцип управления разделением обязанностей. Система, состоящая из взаимно недоверчивых частей, должна быть сильнее простой доверенной системы. В крупном масштабе линии связи определяют естественные границы недоверия. В рамках одной системы дополнительную силу можно получить за счет изоляции функций аутентификации и аудита записи в физически раздельном, более строго контролируемом оборудовании. Такая изоляция функции универсальна в серьезной криптографии.

Только технология не может обеспечить безопасность. В частности, программа обеспечения информационной безопасности мало помогает, если ее пользователи не покупают ее. Программа должна быть реалистичной и поддерживать осознание и приверженность всех участников. Кроме того, действия руководства должны сигнализировать о том, что вопросы безопасности. Когда вознаграждение распространяется только на видимые результаты (например, соблюдение сроков или экономия затрат), внимание, безусловно, будет отходить от безопасности - до тех пор, пока не произойдет стихийное бедствие.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. – Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. – 372 с.: ил., Часть 1, разделы 1, 2

2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд.- 2004. - 544 с., параграфы 1.1, 1.2

3. Галатенко В.А. Информационная безопасность. / Галатенко В.А. – М.: Финансы и статистика, 2009. –158 с.

2. Девянин П.Н. Анализ безопасности управления доступом и информационными потоками в компьютерных системах. / Девянин П.Н. – М.: Радио и связь, 2006.

3. Куприянов А.И. Основы защиты информации. Учебное пособие для студентов высших учебных заведений. / Куприянов А.И., Сахаров А.В., Швецов В.А. – М.: Издательский центр академия, 2006.

4. Маккарти Л. IT-Безопасность: стоит ли рисковать корпорацией. / Маккарти Л. – М.: Кудиц-Образ, 2004.

5. Мельников В. П. Информационная безопасность и защита информации. / Мельников В. П.– М.: Академия, 2012, - 336 стр.

6. http://library.tuit.uz/skanir_knigi/book/zashita_info/zash_info_01.htm

7. https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D

8. https://www.kp.ru/guide/informatsionnaja-bezopasnost-predprijatija.html

9. https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-obrazovatelnykh-uchrezhdenij/

10. https://netoscope.ru/ru/tips/686/

11. http://elar.urfu.ru/bitstream/10995/1357/3/1324427_schoolbook.pdf