Основы информационной безопасности

Информационная безопасность (ИБ) – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

Безопасность информации, которая обрабатывается в организации, – это комплекс действий, направленных на решение проблемы защиты информационной среды в рамках организации. При этом информация не должна быть ограничена в использовании и динамичном развитии для уполномоченных лиц.

Требования к системе защиты ИБ

Защита информационных ресурсов должна быть:

1. **Постоянной.** Злоумышленник в любой момент может попытаться обойти модули защиты данных, которые его интересуют.
2. **Целевой.** Информация должна защищаться в рамках определенной цели, которую ставит организация или собственник данных.
3. **Плановой.** Все методы защиты должны соответствовать государственным стандартам, законам и подзаконным актам, которые регулируют вопросы защиты конфиденциальных данных.
4. **Активной.** Мероприятия для поддержки работы и совершенствования системы защиты должны проводиться регулярно.
5. **Комплексной.** Использование только отдельных модулей защиты или технических средств недопустимо. Необходимо применять все виды защиты в полной мере, иначе разработанная система будет лишена смысла и экономического основания.
6. **Универсальной.** Средства защиты должны быть выбраны в соответствии с существующими в компании каналами утечки.
7. **Надежной.** Все приемы защиты должны надежно перекрывать возможные пути к охраняемой информации со стороны злоумышленника, независимо от формы представления данных.

Модель системы безопасности

Информация считается защищенной, если соблюдаются три главных свойства.

Первое – **целостность** – предполагает обеспечение достоверности и корректного отображения охраняемых данных, независимо от того, какие системы безопасности и приемы защиты используются в компании. Обработка данных не должна нарушаться, а пользователи системы, которые работают с защищаемыми файлами, не должны сталкиваться с несанкционированной модификацией или уничтожением ресурсов, сбоями в работе ПО.

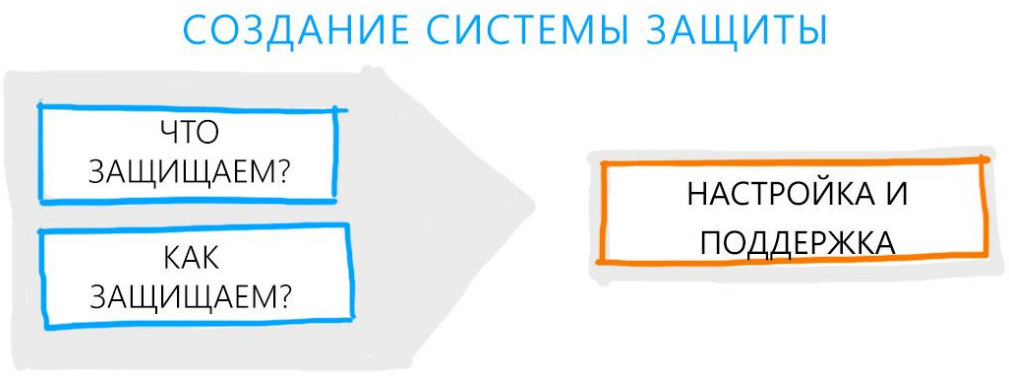
Второе – **конфиденциальность** – означает, что доступ к просмотру и редактированию данных предоставляется исключительно авторизованным пользователям системы защиты.

Третье – **доступность** – подразумевает, что все авторизованные пользователи должны иметь доступ к конфиденциальной информации.

Достаточно нарушить одно из свойств защищенной информации, чтобы использование системы стало бессмысленным.

Этапы создания и обеспечения системы защиты информации

На практике создание системы защиты информации осуществляется в три этапа.



На первом этапе разрабатывается базовая модель системы, которая будет функционировать в компании. Для этого необходимо проанализировать все виды данных, которые циркулируют в организации и которые нужно защитить от посягательств со стороны третьих лиц. Планом работы на начальном этапе являются четыре вопроса:

Какие источники информации следует защитить?

Какова цель получения доступа к защищаемой информации?

Целью может быть ознакомление, изменение, модификация или уничтожение данных. Каждое действие является противоправным, если его выполняет злоумышленник. Ознакомление не приводит к разрушению структуры данных, а модификация и уничтожение приводят к частичной или полной потере информации.

Что является источником конфиденциальной информации?

Источники в данном случае это люди и информационные ресурсы: документы, флеш-носители, публикации, продукция, компьютерные системы, средства обеспечения трудовой деятельности.

Способы получения доступа, и как защититься от несанкционированных попыток воздействия на систему?

Различают следующие способы получения доступа:

Несанкционированный доступ – незаконное использование данных;

Утечка – неконтролируемое распространение информации за пределы корпоративной сети. Утечка возникает из-за недочетов, слабых сторон технического канала системы безопасности;

Разглашение – следствие воздействия человеческого фактора. Санкционированные пользователи могут разглашать информацию, чтобы передать конкурентам, или по неосторожности.

Второй этап включает разработку системы защиты. Это означает реализовать все выбранные способы, средства и направления защиты данных.

Система строится сразу по нескольким направлениям защиты, на нескольких уровнях, которые взаимодействуют друг с другом для обеспечения надежного контроля информации.

Правовой уровень обеспечивает соответствие государственным стандартам в сфере защиты информации и включает авторское право, указы, патенты и должностные инструкции. Грамотно выстроенная система защиты не нарушает права пользователей и нормы обработки данных.

Организационный уровень позволяет создать регламент работы пользователей с конфиденциальной информацией, подобрать кадры, организовать работу с документацией и физическими носителями данных.

Регламент работы пользователей с конфиденциальной информацией называют правилами разграничения доступа. Правила устанавливаются руководством организации совместно со службой безопасности и поставщиком, который внедряет систему безопасности. Цель – создать условия доступа к информационным ресурсам для каждого пользователя, к примеру, право на чтение, редактирование, передачу конфиденциального документа. Правила разграничения доступа разрабатываются на организационном уровне и внедряются на этапе работ с технической составляющей системы.

Технический уровень условно разделяют на физический, аппаратный, программный и математический подуровни.

физический – создание преград вокруг защищаемого объекта: охранные системы, зашумление, укрепление архитектурных конструкций;

аппаратный – установка технических средств: специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей;

программный – установка программной оболочки системы защиты, внедрение правила разграничения доступа и тестирование работы;

математический – внедрение криптографических и стенографических методов защиты данных для безопасной передачи по корпоративной или глобальной сети.

Третий, завершающий этап – это **поддержка работоспособности системы,** регулярный контроль и управление рисками. Важно, чтобы модуль защиты отличался гибкостью и позволял администратору безопасности быстро совершенствовать систему при обнаружении новых потенциальных угроз.

Виды конфиденциальных данных

Конфиденциальные данные – это информация, доступ к которой ограничен в соответствии с законами государства и нормами, которые компании устанавливаются самостоятельно.

Личные конфиденциальные данные: персональные данные граждан, право на личную жизнь, переписку, сокрытие личности. Исключением является только информация, которая распространяется в СМИ.

Служебные конфиденциальные данные: информация, доступ к которой может ограничить только государство (органы государственной власти).

Судебные конфиденциальные данные: тайна следствия и судопроизводства.

Коммерческие конфиденциальные данные: все виды информации, которая связана с коммерцией (прибылью) и доступ к которой ограничивается законом или предприятием (секретные разработки, технологии производства и т.д.).

Профессиональные конфиденциальные данные: данные, связанные с деятельностью граждан, например, врачебная, нотариальная или адвокатская тайна, разглашение которой преследуется по закону.

Угрозы конфиденциальности информационных ресурсов

Угроза – это возможные или действительные попытки завладеть защищаемыми информационными ресурсами.

Источниками угрозы сохранности конфиденциальных данных являются компании-конкуренты, злоумышленники, органы управления. Цель любой угрозы заключается в том, чтобы повлиять на целостность, полноту и доступность данных.

Угрозы бывают внутренними или внешними. ***Внешние угрозы*** представляют собой попытки получить доступ к данным извне и сопровождаются взломом серверов, сетей, аккаунтов работников и считыванием информации из технических каналов утечки (акустическое считывание с помощью жучков, камер, наводки на аппаратные средства, получение виброакустической информации из окон и архитектурных конструкций).

Внутренние угрозы подразумевают неправомерные действия персонала, рабочего отдела или управления организации. В результате пользователь системы, который работает с конфиденциальной информацией, может выдать информацию посторонним. На практике такая угроза встречается чаще остальных. Работник может годами «сливать» конкурентам секретные данные. Это легко реализуется, ведь действия авторизованного пользователя администратор безопасности не квалифицирует как угрозу.

Поскольку внутренние ИБ-угрозы связаны с человеческим фактором, отслеживать их и управлять ими сложнее. Предупреждать инциденты можно с помощью деления сотрудников на группы риска.

Попытка несанкционированного доступа может происходить несколькими путями:

- через сотрудников, которые могут передавать конфиденциальные данные посторонним, забирать физические носители или получать доступ к охраняемой информации через печатные документы;
- с помощью программного обеспечения злоумышленники осуществляют атаки, которые направлены на кражу пар «логин-

пароль», перехват криптографических ключей для расшифровки данных, несанкционированного копирования информации.

- с помощью аппаратных компонентов автоматизированной системы, например, внедрение прослушивающих устройств или применение аппаратных технологий считывания информации на расстоянии (вне контролируемой зоны).

Аппаратная и программная ИБ

Все современные операционные системы оснащены встроенными модулями защиты данных на программном уровне. MAC OS, Windows, Linux, iOS отлично справляются с задачей шифрования данных на диске и в процессе передачи на другие устройства. Однако для создания эффективной работы с конфиденциальной информацией важно использовать дополнительные модули защиты.

- Пользовательские ОС не защищают данные в момент передачи по сети, а системы защиты позволяют контролировать информационные потоки, которые циркулируют по корпоративной сети, и хранение данных на северах.
- Аппаратно-программный модуль защиты принято разделять на группы, каждая из которых выполняет функцию защиты чувствительной информации:
- Уровень идентификации – это комплексная система распознавания пользователей, которая может использовать стандартную или многоуровневую аутентификацию, биометрию (распознавание лица, сканирование отпечатка пальца, запись голоса и прочие приемы).
- Уровень шифрования обеспечивает обмен ключами между отправителем и получателем и шифрует/дешифрует все данные системы.

Правовая защита информации

Правовую основу информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, федеральными законами и подзаконными актами.

Государство также определят меру ответственности за нарушение положений законодательства в сфере ИБ. Например, глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи:

- Статья 272 «Неправомерный доступ к компьютерной информации»;
- Статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;

- Статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Советы по обеспечению информационной безопасности

Вначале уничтожим некоторые штампы.

Штампы:

1. Хакеры - взломщики. Это вообще не так, это специалисты экстра-класса. Слово произошло от глагола to hack - "топорная работа", так называли (и называют) специалистов способных выжать 120 % (и более) из софта и железа и знающие системы лучше их создателей. Хакеры не "злобные взломщики" (хотя одно другого не исключает), это именно специалисты экстра-класса независимо от того чем они занимаются.
2. Антивирусное ПО защищает компьютер. Не защищает и в принципе не может защитить компьютер от всех угроз, предел возможностей антивирусов - отсеивание отработавшей своё, но не вычищенной шушеры.
3. Есть единая система по которой можно настроить и забыть про угрозы ИБ. Не существует и не может существовать в природе.
4. Производители ПО заботятся об информационной безопасности. Поиск угроз ИБ в программных продуктах - дело требующее высокой квалификации и огромных затрат времени, а это - во-первых увеличение бюджета разработки в разы (а иногда - десятки раз), а во-вторых потребность в специалистах, коих на рынке буквально считанные единицы.
5. Можно защитится от угроз ИБ (как вариант компьютер в офф-лайн). Нельзя, не только существуют, но и активно применяются методы взлома и офф-лайн машин.

Практическая информационная безопасность:

Взломщики (те кто ломают софт, сервера и пишут вирусы) делятся на 2 категории:

1. За деньги. Это те кто осуществляют атаки за деньги.
2. За идею. Те кто ломают во-первых чтобы посмотреть как оно работает (по аналогии со вскрытием лабораторных животных), во-вторых получить заслуженное уважение от коллег, в-третьих достичь каких-то личных целей.

Самая опасна для ИБ именно вторая категория. Если взломщик-идеалист заинтересуется Вашей системой, то вопрос взлома - это вопрос времени.

Поэтому первой аксиомой практической ИБ является расчет на то, что Вас уже взломали.

Давайте пойдем дальше и ответим на ключевые вопросы (которыми 99% людей даже не задается): что такое взлом и как собственно он происходит?

Взлом - несанкционированное (не разрешенное) вмешательство в работу информационной инфраструктуры, которое нарушает информацию в виде:

1. Создания информации - загрузка на атакуемые ЭВМ новой информации или программного обеспечения.
2. Изменения информации - изменение данных и программного обеспечения.
3. Копирования информации - копирование на информационные носители данных с ЭВМ жертвы.
4. Удаления информации - уничтожение информации на ЭВМ жертвы.
5. Отказа в обслуживании - произведение действий в результате которых ЭВМ жертвы не сможет выполнять возложенных задач.

Как происходит взлом (обобщение прочитанных "мемуаров" взломщиков):

Первым делом взломщик собирает информацию об атакуемой системе. Тема о том сколько всего можно узнать исследуя сетевой трафик от жертвы даже не на пост - на целую серию постов. Но в итоге у взломщика есть информация о том что именно он атакует.

Вторая стадия - создание копии атакуемой системе в виртуальной или реальной среде. Эта стадия нужна для отработки механизма атаки, хотя при некоторых условиях эта стадия отсутствует.

Третья стадия - создание инструмента взлома (или использование готового).

Четвертая стадия - тестирование инструмента на средствах антивирусной защиты. Вирус который распознается "на раз" никому не нужен, поэтому качественно подготовленный для использования в атаке инструмент спокойно пройдет любую антивирусную защиту.

Пятая стадия - подготовка атаки. На этой стадии разрабатываются способы обхода внешних защит информационной инфраструктуры и решаются проблемы доступа.

Шестая стадия - взлом. Это именно то, что показывают в фильмах - готовые инструменты используются в готовых каналах для атаки.

Седьмая стадия - использование результатов атаки.

Советы:

0. Делайте копии важной информации. Копий рабочих данных должно быть не менее 2-х, критических данных - не менее 4-х, при этом копии должны

размещаться так, чтобы не быть поврежденными/уничтоженными при атаке или при каком-либо происшествии.

1. Используйте антивирусы. Очень мало случаев, когда атака производилась чисто на одну информационную инфраструктуру. В основном атакуется некоторый сегмент в который входит атакуемый объект. При этом атака удается, а спустя некоторое время (от суток до нескольких лет) вирусы используемые при атаке попадают к антивирусным компаниям и они обновляют свои базы. Антивирус просто отсеет летающие по сети ошметки давно прошедших взломов и позволит сосредоточиться на текущих угрозах ИБ.

2. Используйте файерволы (как минимум на шлюзах). Очень рекомендуется их использовать в ручном режиме и на каждом устройстве. Рекомендуемая настройка на рабочих станциях - запрет всех входящих подключений, разрешены исходящие подключения. Рекомендуемая настройка на серверах - разрешение на конкретные порты конкретным клиентам.

3. Разграничивайте сети и закройте доступ к общим папкам. Достаточно многие вирусы могут атаковать через сеть и через общедоступные ресурсы.

4. Используйте по максимуму виртуализацию. Виртуальная машина проигрывает по производительности реальной, но является обычным файлом, который легко скопировать и при необходимости скопировать обратно. Таким образом восстановление работоспособности занимает минимальное время и снижает убытки.

5. На компьютерах должно быть установлено минимальное количество ПО. Неуязвимого ПО нет, а в погоне за клиентом все дружно забили на ИБ, поэтому каждая программа - набор дырок в ИБ и чем меньше софта, тем меньше потенциальных проблем. Такая же позиция должна быть занята и по отношению к службам запущенных на компьютерах - только необходимые для работы.

6. Используйте сканеры файловой системы. Любая атака любым вирусом затронет файловую систему. Сканеры ФС хранят таблицу файлов и хешей и отслуживают обращения к файлам, если пошли необычные манипуляции с ФС - вы атакованы.

7. Не используйте "типовые" решения. На типовые решения есть типовые пути обхода этих решений. Думайте и фантазируйте как направить атаку с реальных машин в какую-нибудь "выгребную яму" (или в приготовленную DMZ). Позаботьтесь о достоверности "выгребной ямы", данные в ней должны быть во-первых бесполезны для взломщика, а во-вторых быть правдоподобными иначе он поймет что его наеобманули и будет менять вектор атаки.

8. Защита начинается с установки. Еще на стадии установки ОС можно обезопасить себя от очень многих типовых угроз. Во-первых готовый к эксплуатации образ ОС нужно скопировать на отдельный раздел (в случае заражения достаточно будет восстановить ОС из образа), во-вторых средствами ОС или сторонним софтом прописать "белые" исполняемые файлы

и запретить исполнение всех остальных, в-третьих отключить автозагрузку всех устройств, в четвертых минимизировать используемое ПО поставляемое с ОС.

9. Документируйте все. Никто и ничто не вечно, а память несовершенна. Грамотно составленная документация позволяет во-первых иметь четкое понимание ситуации, во-вторых иметь представление о возможных угрозах, а в-третьих спланировать устранение последствий взлома.

A. Полюбите бумагу, а не файлы. Файлы легко могут быть скопированы, а вот с бумагой проделать такое гораздо сложнее. Все критически важные пароли ни в коем случае не должны сохраняться или храниться в файлах. Пароли "второго уровня" должны храниться только в локальных менеджерах паролей, а вот пароли от "спамерских" учеток можно выписать в блокнот на рабочем столе.

B. Не доверяй никому и ничему. За единичными исключениями все что мы видим на мониторе - плод работы программ которые могут уже быть заражены. Повторить интерфейс чего-либо задача очень простая, поэтому при угрозе

C. Самая большая угроза ИБ сидит перед монитором. Самый легкий взлом - через пользователя ЭВМ, поэтому пользователь должен быть максимально ограничен в возможностях на компьютере. Есть одна папка с документами и доступ к программам используемым в работе, остальное - запрещено. Проводить разъяснения и учения по ИБ.

D. Профилактика уменьшает глубину жопы. В моей практики были случай когда два месяца напряженной работы сисадмина привели к тому, что атака инициированная поддельным письмом из ПФР для бухгалтера провалилась (при детектировании изменений файлов вырубили комп) и работоспособность была восстановлена примерно за 30 минут.

E. Считайте что Вас уже взломали. Гораздо больше времени уделяйте не защите, а способам во-первых затруднить доступ к критически важным данным и во-вторых максимально быстро восстановить работоспособность системы. Чем сложнее организован несанкционированный доступ к данным, тем больше взломщики будут в сети и тем выше шанс обнаружения вторжения, а значит выше шанс детектирования и начала противодействия. Чем быстрее можно восстановить работоспособность системы тем меньше будет простой организации и соответственно убытков. Тут есть океаны способов, которые перепробовать жизни не хватит.

F. Взломайте себя сами. Если знаешь как взломать, то соответственно будешь знать как себя защитить.

И напоследок (самое главное) - аудит. Введите себе в привычку проверять что твориться в компьютере загрузившись с "живого" образа ОС (желательно с диска восстановления антивируса) и посмотрите - все ли в порядке?

Информационная безопасность, это не единичное действие и не набор действий, а постоянный и не прерываемый процесс.

Источники: https://searchinform.ru/informatsionnaya-bezopasnost/
https://pikabu.ru/story/osnovyi_informatsionnoy_bezopasnosti_4813574