УНИВЕРСИТЕТ «УНИВЕРСИТЕТ»Построению безопасных локальных компьютерных сетей и закрытых баз данных должно предшествовать определение угроз безопасности локальных компьютерных сетей и закрытых баз данных. Для формирования модели угроз требуется определить характеристики безопасности защищаемых объектов (в первую очередь, автоматизированных и информационных систем), а также всех объектов, которые были определены как возможные объекты угроз.

Характеристики безопасности защищаемой информации

Основными (классическими) характеристиками безопасности информации являются [1]:

Конфиденциальность – обеспечение доступа к информации только авторизованным пользователям.

Целостность – обеспечение сохранности, неизменности и полноты информации и методов ее обработки.

Доступность – обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости.

В дополнение к перечисленным выше основным характеристикам безопасности могут рассматриваться также и другие характеристики безопасности:

Неотказуемость – способность доказать, что действие или событие произошло таким образом, что факт действия или события не может быть опровергнут (ИСО 7498–2:99 и ИСО 13888–1:2004).

Учетность (подконтрольность) – свойство, обеспечивающее однозначное отслеживание собственных действий любого логического объекта (ИСО 7498–2:99); обеспечение того, что действия субъекта по отношению к объекту могут быть прослежены уникально по отношению к субъекту.

Аутентичность (достоверность) – свойство обеспечения идентичности субъекта или ресурса заявленной идентичности. Аутентичность применяется к таким субъектам как пользователи, процессы, системы и информация (ISO/IEC 13335–1:2004).

Адекватность – свойство соответствия преднамеренному поведению и результатам (ISO/IEC 13335–1:2004).

Важно отметить, что, так как угроза безопасности объекта есть возможное нарушение характеристики безопасности объекта, то перечень всех характеристик безопасности для всех возможных объектов угроз, по сути, определяет модель угроз верхнего уровня.

Классификация нарушителей безопасности

Различают шесть основных типов нарушителей [2], нумеруя их по степени возрастания несомой ими угрозы: 1, 2, ... , 6. При этом возможности нарушителя типа i+1 включают в себя возможности нарушителя типа i (i от 1 до 5).

Тип 1 – нарушитель, использующий документированные возможности программно-аппаратной среды и работающий удалённо (модель “обычный пользователь”).

Тип 2 – нарушитель, имеющий право входа в контролируемую зону, но не имеющий права доступа к ЭВМ (модель “уборщица”).

Тип 3 – нарушитель, имеющий право доступа в контролируемую зону и являющийся зарегистрированным пользователем СКЗИ (модель “сотрудник”).

Тип 4 – лицо или группа лиц, использующие недокументированные возможности системы (модель “хакер”).

Тип 5 – лицо или группа лиц, имеющие возможность проведения лабораторных исследований СКЗИ и компонентов СФК (модели “НИИ” либо “разработчик”).

Тип 6 – спецслужбы и представители специальных органов (контролирующих, правоохранительных, надзорных и т.п.) имеющие возможность применять специальные средства и способы атак, а также специализирующиеся в области анализа СКЗИ и СФК (модель “АНБ”).

Безопасность локальных компьютерных сетей

В 1994 году Совет по архитектуре Интернет (IAB) выпустил отчёт «Безопасность архитектуры Интернет». Он посвящался в основном способам защиты от

несанкционированного мониторинга, подмены пакетов и управлению потоками данных. В этом документе описывались основные области применения дополнительных средств безопасности в сети Интернет, а именно защита от несанкционированного мониторинга, подмены пакетов и управления потоками данных[3]. В числе первоочередных и наиболее важных защитных мер указывалась необходимость разработки концепции и основных механизмов обеспечения целостности и конфиденциальности потоков данных. Поскольку изменение базовых протоколов семейства TCP/IP вызвало бы полную перестройку сети Интернет, была поставлена задача обеспечения безопасности информационного обмена в открытых телекоммуникационных сетях на базе существующих протоколов. Таким образом, начала создаваться спецификация Secure IP, дополнительная по отношению к протоколам IPv4 и IPv6 (в числе которых и IPsec). Первоначально он включал в себя три базовые спецификации, описанные в документах: RFC1825, 1826 и 1827. Однако впоследствии рабочая группа IP Security Protocol IETF пересмотрела их и предложила новые стандарты: RFC2401 — RFC2412, используемые и в настоящее время. Эти спецификации представляют собой набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP. Они позволяют осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или 8 шифрование IP-пакетов, включают в себя протоколы для защищённого обмена ключами в сети Интернет и применяются в основном для организации vpn-соединений. Модель OSI В 1984 Международный институт стандартизации ISO предложил модель OSI (model of open system interconnections). Она состоит из следующих уровней, представленных на рисунке 1:

1. Физический. Работа со средой передачи, сигналами и двоичными данными.

2. Канальный. Физическая адресация. Организующий протокол для построения WAN/LAN. Два подуровня: управление логической связью (LLC–Logical Link Control) и управление доступом к среде (MAC –Media Access Control). Примеры протоколов LLC: Ethernet, Token Ring, ATM (Asynchronous Transfer Mode), FDDI (Fiber Distributed Data Interface).

3. Примеры протоколов MAC: ARP (Address Resolution Protocol), RARP (Reverse Address Resolution Protocol).

4. Сетевой. Определение маршрута и логическая адресация. Занимается вставкой в заголовок пакета информации, необходимой для правильной адресации и маршрутизации этого пакета с целью доставки правильному получателю. Примеры

протоколов: IP (Internet Protocol), IPsec (IP Security), ICMP (Internet Control Message Protocol), IGMP (Internet Group Management Protocol).

5. Транспортный. Прямая связь между конечными пунктами и надежность.

6. Сеансовый. Управление сеансом связи.

7. Уровень представления. Представление и шифрование данных.

8. Прикладной. Доступ к сетевым службам.

Рисунок 1. Модель OSI

В вопросе выбора уровня реализации защищённого канала несколько противоречивых аргументов: с одной стороны, за выбор верхних уровней говорит их независимость от вида транспортировки (выбора протокола сетевого и канального уровней), с другой стороны, для каждого приложения необходима отдельная настройка и конфигурация.

Плюсом в выборе нижних уровней является их универсальность и наглядность для приложений, минусом — зависимость от выбора конкретного протокола (например, PPP или Ethernet).

Компромиссом является защита на уровне IP: она располагается на сетевом уровне. В результате передаваемые IP-пакеты будут защищены прозрачным для сетевых приложений и инфраструктуры образом. Это делает ее более гибкой, так что она

может использоваться для защиты любых протоколов, базирующихся на TCP и UDP. В то же время обеспечивается прозрачность для большинства приложений.

Защита на уровне IP

Плюсы:

1. Возможность построения отличных от звезды топологий сетей.

2. Большое количество встроенных клиентов во всех OS.

3. При реализации защиты в сетевом экране или роутере обеспечивается безопасность для всего трафика, пересекающего периметр.

4. При такой защите не существует обходного пути, если весь входящий трафик использует IP трафик, а брандмауэр является единственной точкой входа из Интернета в организацию.

5. Защита находится ниже транспортного уровня (TCP, UDP) и поэтому является прозрачной для приложений. Вследствие этого нет необходимости изменять программное обеспечение в системе пользователя или сервера.

6. Защита может быть прозрачной для конечных пользователей. Нет необходимости обучать пользователей механизмам безопасности, выпускать ключи для каждого пользователя или отзывать ключи.

Минусы

1. Медленная производительность. Скорость в сети может падать на 10-15% даже без шифрования и туннелирования. Снижение производительности не всегда представляет серьезную проблему, но если ресурсы сервера на пределе или необходимо высокое быстродействие, то такой подход вряд ли будет лучшим решением.

2. Сложность процедуры настройки. Иногда возникает путаница между правилами, наборами правил, фильтрами и наборами фильтров.

Возможность построения VPN

Защита на уровне IP часто используется для организации VPN-туннелей[4]. В этом случае протоколы ESP и AH работают в режиме туннелирования. Кроме того, настраивая политики безопасности определенным образом, протоколы можно

использовать для создания межсетевого экрана. Смысл межсетевого экрана заключается в том, что он

контролирует и фильтрует проходящие через него пакеты в соответствии с заданными правилами. Устанавливается набор правил, и экран просматривает все проходящие через него пакеты. Если передаваемые пакеты попадают под действие этих правил, межсетевой экран обрабатывает их соответствующим образом. Например, он может отклонять определенные пакеты, тем самым прекращая небезопасные соединения. Настроив политику безопасности соответствующим образом, можно, например, запретить веб-трафик. Для этого достаточно запретить отсылку пакетов, в которые вкладываются сообщения протоколов HTTP и HTTPS. Такого рода защиту можно применять и для защиты серверов — для этого отбрасываются все пакеты, кроме пакетов, необходимых для корректного выполнения функций сервера. Например, для Web-сервера можно блокировать весь трафик, за исключением соединений через 80-й порт протокола TCP, или через порт TCP 443 в случаях, когда применяется HTTPS.

Практические примеры применения защиты компьютерных сетей

● Связь с филиалами компании через интернет. Компания может построить защищенную виртуальную частную сеть (VPN) через Интернет или через общедоступный WAN. Это позволяет предприятию в значительной степени полагаться на Интернет и уменьшить потребность в частных сетях, экономя затраты и накладные расходы на управление сетью.

● Безопасный удаленный доступ через Интернет. Конечный пользователь, чья система оснащена протоколами безопасности IP, может получить безопасный доступ к корпоративной сети. Это снижает стоимость обслуживания сотрудников в командировках и работающих из дома.

● Создание сетей экстранет и интранет с партнерами. Защита на уровне IP может использоваться для обеспечения связи с другими организациями, обеспечения аутентификации и конфиденциальности и обеспечение механизма обмена ключами.

● Повышение безопасности электронной коммерции. Хотя некоторые приложения для электронной коммерции имеют встроенные протоколы безопасности, использование защиты на уровне IP повышает безопасность. Таким образом, все распределенные приложения, в том числе для удаленного входа (клиент-серверные приложения, электронная почта, передача файлов, доступ к Web и т.д.),

могут стать более безопасными.

Стандартизирующие документы: IETF

RFC 1825: Security Architecture for the Internet Protocol (obsoleted by RFC 2401)

RFC 1826: IP Authentication Header (obsoleted by RFC 2402)

RFC 1827: IP Encapsulating Security Payload (ESP) (obsoleted by RFC 2406)

RFC 1828: IP Authentication using Keyed MD5 (historic)

RFC 2401: Security Architecture for the Internet Protocol (IPsec overview) (obsoleted by RFC 4301).

Безопасность закрытых баз данных

Средства защиты баз данных (далее – БД) в различных системах управления данных (далее – СУБД) несколько отличаются друг от друга. На основе анализа современных СУБД Orcale и Microsoft можно утверждать, что средства защиты БД условно делятся на две группы, основные и дополнительные.

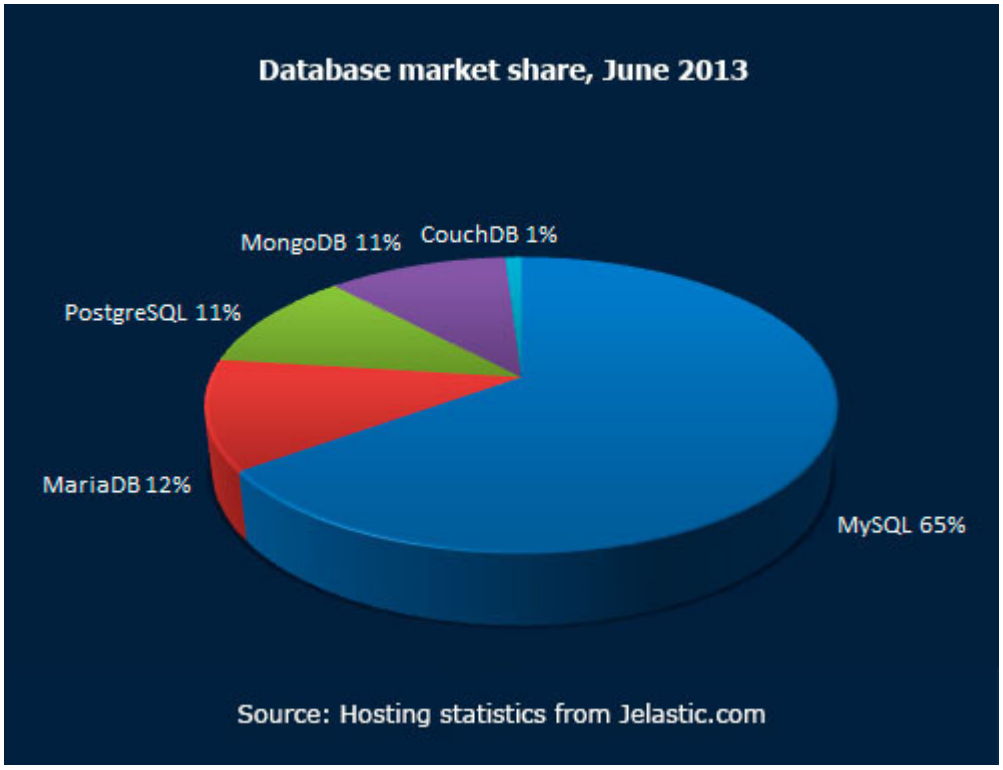

Рисунок 2.Статистика применения баз данных [6]

К основным средствам защиты информации можно отнести следующие средства [5]:

- парольная защита;

- шифрование данных и программ;

- установление прав доступа к объектам БД;

- защита полей и записей таблиц БД.

Парольная защита представляет простой и эффективный способ защиты БД от несанкционированного доступа. Пароли устанавливаются конечными пользователями или администраторами БД. Учет и хранение паролей производится самой СУБД. Обычно пароли хранятся в определенных системных файлах СУБД в зашифрованном виде. Поэтому просто найти и определить пароль невозможно. После ввода пароля пользователю СУБД предоставляются все возможности по работе с защищенной БД.

Шифрование данных (всей базы или отдельных таблиц) применяется для того, чтобы другие программы не могли прочитать данные. Шифрование исходных текстов программ позволяет скрыть от несанкционированного пользователя описание соответствующих алгоритмов.

В целях контроля использования основных ресурсов СУБД во многих системах имеются средства установления прав доступа к объектам БД. Права доступа определяют возможные действия над объектами. Владелец объекта (пользователь, создавший объект), а также администратор БД имеют все права. Остальные пользователи к разным объектам могут иметь различные уровни доступа.

По отношению к таблицам в общем случае могут предусматриваться следующие права доступа.

- просмотр (чтение) данных;

- изменение (редактирование) данных;

- добавление новых записей;

- добавление и удаление данных;

- все операции, в том числе изменение структуры таблицы.

Принципы разработки безопасного программного обеспечения для баз данных

Хотя все эти принципы поодиночке не могут обеспечить безопасной разработки программного обеспечения, их общий обзор может помочь в поэтапном понимании различных практических приемов такой разработки. Некоторые из самых ранних принципов были предложены Зальтзером (Saltzer) в 1974 и потом были отредактированы им в 1975. Эти восемь принципов представлены ниже:

1. Экономия на разработке. Оставляйте проектирование максимально простым и минималистическим, насколько это возможно. Этот хорошо известный принцип используется во всех аспектах проектирования систем и программного обеспечения.

Он является особенно уместным в сфере безопасности, поскольку механизмы безопасности должны быть относительно небольшими и простыми, чтобы далее они могли быть с легкостью внедрены и верифицированы (например, ядро системы безопасности).

2. Отказоустойчивые настройки по умолчанию. Базовые установки по предоставлению доступа являются более предпочтительными, чем отказ в таком доступе. Это означает, что по умолчанию доступ запрещен и схема защиты выявляет условия, при которых доступ разрешен. Если происходит сбой механизма по предоставлению доступа, то такая ситуация легко фиксируется и корректируется.

3. Проверка каждого разрешения на доступ. Каждый вход в каждый объект системы должен быть проверен на наличие полномочий на такой доступ. Для этого требуется, чтобы источник каждого запроса должен быть положительно идентифицирован и авторизован для получения доступа к ресурсу.

4. Несекретная конструкция. Безопасное проектирование не должно полагаться на малограмотность потенциальных атакующих или закрытость программного кода.

Например, системы шифрования и механизмы управления доступом должны иметь возможность быть размещенными в открытом доступе для рецензирования и оставаться при этом защищенными. Обычно это достигается за счет отделения ключей или паролей от механизма защиты. Это дает значительные преимущества – возможность тщательной проверки этого механизма без возможности компрометации ключей/паролей.

5. Разграничение привилегий. Если это осуществимо, то защитный механизм, которому требуются два ключа для вскрытия, является более устойчивым и гибким, чем тот, который предоставляет доступ к предъявителю только одного ключа. Схема с двухфакторной аутентификацией есть пример использования разделения привилегий: что-то у вас есть и что-то вы знаете. Разделение привилегий часто сбивает с толку разработчиков программ, состоящих из подсистем, основанных на требуемых привилегиях. При таком подходе разработчики умудряются создавать мелкомодульные приложения с минимальным набором привилегий.

6. Минимальная привилегия. Каждая программа и каждый пользователь системы должен работать с минимальным количеством привилегий, достаточных для выполнения работы. Когда происходит эксплуатация уязвимой программы, вредоносный код работает с привилегиями, имеющимися у программы в настоящий момент. Принцип минимальной привилегии предполагает, что процессы должны выполняться с минимальными правами, требуемыми для проведения безопасных операций и любые превышенные права должны поддерживаться в течении минимального времени. Такой подход резко снижает шансы злоумышленников исполнить произвольный код с более высокими привилегиями.

7. Минимальное количество механизмов. Минимизируйте число механизмов, являющихся общими для более, чем одного пользователя и которые зависят от всех пользователей, поскольку они представляют потенциальный риск безопасности.

Если враждебный пользователь управляет нарушением безопасности одного из таких механизмов, у атакующего может быть возможность для доступа или модификации данных других пользователей путем введения вредоносного кода в процесс, зависящий от ресурса. Любой процесс должен быть связан только со своей программой и не может быть использован другими приложениями.

8. Психологическая приемлемость. Существенным является то, чтобы спроектированный интерфейс взаимодействия с человеком обеспечивал простоту применения и пользователь самым рутинным и автоматизированным образом мог бы правильно обратиться к механизмам защиты. Современным понятием для пояснения данного принципа является практичность; это другой атрибут качества, который часто является альтернативой обеспечению безопасности. Однако практичность часто является формой безопасности, поскольку пользовательские ошибки часто приводят к нарушениям безопасности (например, путем установки неправильных настроек доступа).

Вывод

Таким образом, в данном эссе представлены практико-ориентированные рекомендации по обеспечению безопасности локальных компьютерных сетей и закрытых баз данных с опорой на действующие на данный момент законодательные и иные нормативно-правовые акты, актуальные учебно-методические материалы и ресурсы интернета. С учетом роста различных киберугроз, совершенствования методов конкурентной разведки и повсеместной информатизации обеспечение защиты локальных компьютерных сетей и закрытых баз данных является необходимой составляющей управления кадровой безопасностью организации.

Список используемых источников:

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
2. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
3. Информатика: Учеб. пособие для студ. пед. вузов / А.В. Могилев, Н.И.Пак, Е.К.Хеннер; Под ред. Е.К.Хеннера. - 3-е изд., перераб. и доп. - М.: Издательский центр«Академия», 2015. - 848 с.
4. Комплексная защита информации в компьютерных системах: Учебное пособие. Завгородний В.И. - М.: Логос; ПБОЮЛ Н.А. Егоров, 20171. - 264 с.: ил.
5. Пирогов, В.Ю. Информационные системы и базы данных: организация и проектирование: Учебное пособие / В.Ю. Пирогов. - СПб.: БХВ-Петербург, 2018. - 528 с.
6. http://bb3x.ru/blog/statistika-primeneniya-baz-dannyih-serverov-versiy-java-i-php-v-oblake/