На текущий момент под «Безопасностью» понимают особую комбинацию как технических, так и административных мер. Административные меры также включают в себя не только бумаги, рекомендации, инструкции, но и людей. Невозможно считать свою сеть «безопасной», если вы не доверяете людям, работающим с этой сетью.

Идеальная безопасность — недостижимый миф, который могут реализовать, в лучшем случае, только несколько профессионалов. Есть один фактор, который невозможно преодолеть на пути к идеальной безопасности — это человек.

Основные цели сетевой безопасности

Цели сетевой безопасности могут меняться в зависимости от ситуации, но основных целей обычно три:

- Целостность данных.
- Конфиденциальность данных.
- Доступность данных.

Рассмотрим более подробно каждую из них.

Целостность данных

Одна из основных целей сетевой безопасности — гарантированность того, чтобы данные не были изменены, подменены или уничтожены. Целостность данных должна гарантировать их сохранность как в случае злонамеренных действий, так и случайностей. Обеспечение целостности данных является обычно одной из самых сложных задач сетевой безопасности.

Конфиденциальность данных

Второй главной целью сетевой безопасности является обеспечение конфиденциальности данных. Не все данные можно относить к конфиденциальной информации. Существует достаточно большое количество информации, которая должна быть доступна всем. Но даже в этом случае обеспечение целостности данных, особенно открытых, является основной задачей. К конфиденциальной информации можно отнести следующие данные:

- Личная информация пользователей.
- Учетные записи (имена и пароли).
- Данные о кредитных картах.
- Данные о разработках и различные внутренние документы.
- Бухгалтерская информация.

Доступность данных

Третьей целью безопасности данных является их доступность. Бесполезно говорить о безопасности данных, если пользователь не может работать с ними из-за их недоступности. Вот приблизительный список ресурсов, которые обычно должны быть «доступны» в локальной сети:

- Принтеры.
- Серверы.
- Рабочие станции.
- Данные пользователей.
- Любые критические данные, необходимые для работы.
- Рассмотрим угрозы и препятствия, стоящие на пути к безопасности сети. Все их можно разделить на две большие группы: технические угрозы и человеческий фактор.

Технические угрозы:

- Ошибки в программном обеспечении.
- Различные DoS- и DDoS-атаки.
- Компьютерные вирусы, черви, троянские кони.
- Анализаторы протоколов и прослушивающие программы («снифферы»).
- Технические средства съема информации.

Человеческий фактор:

- Уволенные или недовольные сотрудники.
- Промышленный шпионаж.
- Халатность.
- Низкая квалификация.

Уволенные и недовольные сотрудники

Данная группа людей наиболее опасна, так как многие из работающих сотрудников могут иметь разрешенный доступ к конфиденциальной информации. Особенную

группу составляют системные администраторы, зачастую недовольные своим материальным положением или несогласные с увольнением, они оставляют «черные ходы» для последующей возможности злонамеренного использования ресурсов, похищения конфиденциальной информации и т. д.

Промышленный шпионаж

Это самая сложная категория. Если ваши данные интересны кому-либо, то этот кто-то найдет способы достать их. Взлом хорошо защищенной сети — не самый простой вариант. Очень может статься, что уборщица «тетя Глаша», моющая под столом и ругающаяся на непонятный ящик с проводами, может оказаться хакером весьма высокого класса.

Халатность

Самая обширная категория злоупотреблений: начиная с не установленных вовремя обновлений, неизмененных настроек «по умолчанию» и заканчивая несанкционированными модемами для выхода в Internet, — в результате чего злоумышленники получают открытый доступ в хорошо защищенную сеть.

Низкая квалификация

Часто низкая квалификация не позволяет пользователю понять, с чем он имеет дело; из-за этого даже хорошие программы защиты становятся настоящей морокой системного администратора, и он вынужден надеяться только на защиту периметра. Большинство пользователей не понимают реальной угрозы от запуска исполняемых файлов и скриптов и считают, что исполняемые файлы -только файлы с расширением «exe». Низкая квалификация не позволяет также определить, какая информация является действительно конфиденциальной, а какую можно разглашать. В крупных компаниях часто можно позвонить пользователю и, представившись администратором, узнать у него учетные данные для входа в сеть. Выход только один -обучение пользователей, создание соответствующих документов и повышение квалификации.

Методы защиты

Согласно статистике потерь, которые несут организации от различных компьютерных преступлений, львиную долю занимают потери от преступлений, совершаемых собственными нечистоплотными сотрудниками. Однако в последнее время наблюдается явная тенденция к увеличению потерь от внешних

злоумышленников. В любом случае необходимо обеспечить защиту как от нелояльного персонала, так и от способных проникнуть в вашу сеть хакеров. Только комплексный подход к защите информации может внушить уверенность в ее безопасности.

Защита данных от внутренних угроз

Для защиты циркулирующей в локальной сети информации можно применить следующие криптографические методы:

- шифрование информации;
- электронную цифровую подпись (ЭЦП).

Шифрование

Шифрование информации помогает защитить ее конфиденциальность, т.е. обеспечивает невозможность несанкционированного ознакомления с ней. Шифрование — это процесс преобразования открытой информации в закрытую, зашифрованную (что называется «зашифрование») и наоборот («расшифрование»). Это преобразование выполняется по строгим математическим алгоритмам; помимо собственно данных в преобразовании также участвует дополнительный элемент — «ключ». В ГОСТ 28147-89 дается следующее определение ключа: «Конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований». Иными словами, ключ представляет собой уникальный элемент, позволяющий зашифровать информацию так, что получить открытую информацию из зашифрованной можно только определенному пользователю или группе пользователей.

Стоит сказать, что все государственные организации РФ и ряд коммерческих обязаны для защиты данных использовать отечественный алгоритм симметричного шифрования ГОСТ 28147-89. Это сильный криптографический алгоритм, в котором пока еще не найдено недостатков за более чем 12 лет применения.

Электронная цифровая подпись

ЭЦП позволяет гарантировать целостность и авторство информации. Схема распространения ключей ЭЦП аналогична схеме асимметричного шифрования: секретный ключ должен оставаться у его владельца, открытый же распространяется всем пользователям, желающим проверять ЭЦП владельца секретного ключа. Необходимо обеспечивать недоступность своего секретного

ключа, ибо злоумышленник легко может подделать ЭЦП любого пользователя, получив доступ к его секретному ключу.