ВВЕДЕНИЕ В БЕЗОПАСНОСТЬ СЕТЕЙ

SETI.UCOZ.RU

- Сетевая безопасность охватывает множество мер и должна рассматриваться как часть общей политики, проводимой организацией по информационной безопасности.

- В обеспечении безопасности сети занято много служб и используются различные средства.

Эффективность компьютерной сети во многом зависит от степени защищенности обрабатываемой и передаваемой информации.

Степень защищенности информации от различного вида угроз при ее получении, обработке, хранении, передаче и использовании называют ***безопасностью информации.***

Безопасная сеть обладает свойствами:

- ***конфиденциальности*** (Confidentiality), т.е. защищает данные от несанкционированного доступа, предоставляя доступ к секретным данным только авторизованным пользователям, которым этот доступ разрешен;
- ***доступности*** (Availability), что означает обеспечение постоянного доступа к данным авторизованным пользователям. Безопасная связь характеризуется свойством ***аутентичности,*** т.е. способностью отправителя и получателя подтвердить свою личность: отправитель и получатель должны быть уверены в том, что каждый из них является тем, за кого он себя выдает;
- ***целостности*** (Integrity), гарантирующей сохранность данных, которая обеспечивается запретом для неавторизованных пользователей каким-либо образом изменять, модифицировать, разрушать или создавать данные.

Политика безопасности, включающая в себя совокупность норм и правил, регламентирующих процесс обработки информации, формируется на этапе развертывания сети с учетом таких основополагающих принципов, как:

- ***комплексный подход*** к обеспечению безопасности, начиная с организационно-административных запретов и заканчивая встроенными средствами сетевой защиты;
- предоставление каждому сотруднику предприятия (пользователю компьютеров, информационной системы, сети) того ***минимального уровня привилегий*** на доступ к данным, который необходим ему для выполнения своих должностных обязанностей;
- ***принцип баланса возможного ущерба от реализации угрозы и затрат на ее предотвращение.*** Например, в некоторых случаях можно отказаться от дорогостоящих аппаратных средств защи-ты, ужесточив административные меры.

Основная задача политики безопасности состоит в защите от несанкционированного доступа к ресурсам информационной системы.

Политика безопасности является эффективным средством, заставляющим всех пользователей корпоративной сети следовать раз и навсегда установленным правилам безопасности.

Ее реализация начинается с выявления уязвимых компонентов и угроз и принятия соответствующих контрмер.

Уязвимым является такой компонент, некорректное использование или сбой которого может поставить под угрозу безопасность всей сети. К уязвимым компонентам относят пользователей сети, которые могут нанести вред сознательно, случайно или в силу отсутствия опыта.

Если информация нерегулярно резервируется, перед всей корпоративной сетью возникает вполне реальная угроза потери данных в результате умышленного или случайного повреждения основного накопителя.

Угроза — это потенциальная попытка использования недостатков уязвимого компонента для нанесения вреда. Примерами угроз могут служить взломщики, вирусы, пожары, природ-ные катаклизмы.

После оценки возможных угроз (рисков) переходят к выработке контрмер.

Под ***контрмерой*** понимают действие, позволяющее минимизировать риск от определенного уязвимого компонента или некоторой угрозы. Одной из самых эффективных контрмер минимизации риска потери данных является **создание надежной системы резервного копирования.**

Планирование безопасности сети и данных.

- Высокая степень безопасности может быть достигнута путем использования плана, предусматривающего применение различных мер и средств обе-спечения безопасности.
- **Оценка требований к безопасности** сетевых дан-ных является первым этапом разработки плана по принятию мер их защиты.

Для принятия мер по защите данных в сети нужно выявить главные источники угроз их безопасности.

Существуют следующие **виды угроз**:

- ***непреднамеренные***, к которым относятся ошибочные действия лояльных сотрудников, стихийные бедствия, ненадежность работы программно-аппаратных средств и др.;
- ***преднамеренные***, которые явно направлены на причинение ущерба информационной безопасности;
- ***внешние***, которые проявляются в таких формах, как несанк-ционированное использование паролей и ключей; атаки DoS (Denial of Service — отказ в обслуживании), направленные на разрыв сетевого соединения или приведение его в неработо-способное состояние; подмена адреса; компьютерные вирусы и черви;
- ***внутренние***, к которым можно отнести промышленный шпио-наж, интриги и недовольство служащих, случайные нарушения и т.п.

СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

- В разных программных и аппаратных продуктах, предназначенных для защиты данных, ча-сто используются одинаковые подходы, приемы и технические ре-шения, которые в совокупности образуют ***технологию безопасности***.

Криптозащита. Разработкой методов преобразования ин-формации в целях ее защиты занимается *криптография*.

Преобразование об-щедоступных (понятных для всех) данных к виду, затрудняющему их распознавание, называется ***шифрованием*** (Encryption), а обрат-ное преобразование — ***дешифрованием*** (Decryption). Шифрование является доступным средством для администраторов и пользовате-лей и одним из эффективных средств обеспечения конфиденци-альности информации.

Аутентификация (Authentication).

- Это процедура установления подлинности пользователя при запросе доступа к ресурсам системы (компьютеру или сети).
- Аутентификация предотвращает доступ нежелательных лиц и разрешает доступ всем легальным пользователям.
- Объектами аутентификации могут быть не только пользовате-ли, но и различные устройства, приложения, текстовая и другая информация.

Идентификация субъектов и объектов доступа

- Идентификация предусматривает закрепление за каждым субъек-том доступа уникального имени в виде номера, шифра или кода, например, персональный идентификационный номер (Personal Identification Number — PIN), социальный безопасный номер (So-cial Security Number — SSN) и т. п. Идентификаторы пользовате-лей должны быть зарегистрированы в информационной системе администратором службы безопасности.

Авторизация (Authorization).

- Это процедура предоставления каждому из пользователей тех прав доступа к каталогам, файлам и принтерам, которыми его наделил администратор.
- Кроме того, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как установка системного времени, создание резервных копий дан-ных, локальный доступ к серверу, выключение сервера и т. п.

Система авторизации наделяет пользователя сети правами выполнять определенные действия над определенными ресурсами. Для этого могут быть использованы два подхода к определению прав доступа:

- ***избирательный***, при котором отдельным пользователям (или группам), явно указанным своими *идентификаторами*, разрешаются или запрещаются определенные операции над определенным ресурсом;
- ***мандатный***, при котором вся информация в зависимости от степени секретности делится на уровни, а все пользователи сети — на группы, образующие иерархию в соответствии с *уровнем допуска* к этой информации.

Аудит (Auditing).

- Это фиксация в системном журнале событий, связанных с доступом к защищаемым системным ресурсам. Аудит используется для обнаружения неудачных попыток *взлома* системы.

Процедура рукопожатий

- Для установления подлинно-сти пользователей широко используется процедура рукопожатий (Handshaking — согласованный обмен, квитирование), построен-ная по принципу вопрос-ответ. Она предполагает, что правильные ответы на вопросы дают только те пользователи, для которых эти вопросы предназначены.

Технологии защищенного канала

Технологии защищенного канала широко исполь-зуются в виртуальных частных сетях, которые требуют принятия дополнительных мер по *защите* передаваемой информации.

Средства безопасности, предоставляемые операционными системами

Современные ОС способны обеспечить доступ к одному компьютеру и сетевым ресурсам многим пользователям. Для этого используются отдельные учетные записи, которым присвоены разные пароли. После правильного ввода регистрационной информации пользователь может получить доступ к ОС и сети; читать, изменять ресурсы и выполнять любые другие действия, которые соответствуют правам его учетной записи, создавать желаемую конфигурацию пользовательского интерфейса (рабочую среду) и т.д.

Аппаратные средства защиты

Основой надежной защиты данных от многих неисправностей аппаратных средств является ***избыточность.***

При выходе из строя некоторого сетевого устройства начинает функционировать его резервный дублер. Потерю дан-ных при выходе из строя винчестера можно восполнить файлами, хранящимися в системе резервного копирования.

Резервное копирование данных.

Оно осуществляется с помощью специальных программ и является действенной мерой защиты от возможной их потери при регулярном выполнении этой процедуры. Наличие резервной копии позволяет быстро восстановить утерянные данные.

Отказоустойчивая система дисков.

Под ***отказоустойчивостью*** понимают способность системы к восстановлению после аварии.

Объединение (конфигурация) нескольких физических жестких дисков в отказоустойчивый набор называется ***системой RAID*** (Redundant Array of Independent Disks — избыточный набор независимых дисков).

Он может быть реализован в нескольких различных формах. В зависимости от уровня (0 — 5 и 7) предоставляются различные способы объединения дисков: RAID 0, RAID 1, RAID 2, RAID 3, RAID 4, RAID 5.

Брандмауэры позволяют организовать защиту по всему периметру АС, создавая барьер между внутренней АС и соедине-ниями с внешним миром (Internet).

Такая защищенная область может быть установлена также в подсети.

Брандмауэр может быть реализован как аппаратным, так и программным способом.

Фактически он является средством фильтрации входящих и исходящих пакетов.