ЛЕКЦИЯ №2. ПОЛИТИКА БЕЗОПАСНОСТИ

2.1 Цель лекции

Целью лекции является знакомство с принципами построения и структурой политики безопасности организации.

2.2 Теоретические сведения

2.2.1 Понятие «Политика безопасности»

Политика безопасности - это совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты КС от заданного множества угроз.

Под *политикой безопасности* организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которого реализуется деятельность в компьютерной системе организации. Вообще политика безопасности определяется используемой компьютерной средой и отражает специфические потребности организации.

Обычно КС представляет собой сложный комплекс разнородного, иногда плохо согласующегося между собой аппаратного и программного обеспечения: компьютеров, ОС, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают собственными средствами защиты, которые можно согласовать между собой. Поэтому в качестве согласованной платформы по обеспечению безопасности корпоративной системы очень важна эффективная политика безопасности. По мере роста компьютерной системы и интеграции ее в глобальную сеть, необходимо обеспечить отсутствие в системе слабых мест, поскольку все усилия по защите информации могут быть обесценены лишь одной оплошностью.

Политику безопасности нужно построить таким образом, чтобы она устанавливала, кто имеет доступ к конкретным активам и приложениям, какие цели и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают, как должны выполняться конкретные задачи безопасности. Особенности работы конкретного сотрудника могут потребовать доступа к информации, которая не должна быть доступна другим работникам. Например, менеджер по персоналу может иметь доступ к частной информации любого сотрудника, в то время как специалист по отчетности может иметь доступ только к финансовым данным их сотрудников, а рядовой сотрудник будет иметь доступ только к своей собственной персональной информации.

Политика безопасности определяет позицию организации по рациональному использованию компьютеров и сети, а также процедуры по предотвращению и реагированию на инциденты безопасности. В большой

корпоративной системе может применяться широкий диапазон разных политик от бизнес-политик до специфичных правил доступа к наборам данных. Эти политики полностью определяются конкретными потребностями организации.

2.2.2 Структура политики безопасности организации

Обычно политика безопасности организации включает:

- базовую политику безопасности;
- специализированные политики безопасности;
- процедуры безопасности.

Базовая политика безопасности устанавливает, как организация обрабатывает информацию, кто может получить к ней доступ и как это можно сделать.

Нисходящий подход, реализуемый базовой политикой безопасности, дает возможность постепенно и последовательно выполнять работу по созданию системы безопасности, не пытаясь сразу выполнить ее целиком. Базовая политика позволяет в любое время ознакомиться с политикой безопасности в полном объеме и выяснить текущее состояние безопасности в организации, структура и состав политики безопасности зависит от размера и целей компании. Обычно базовая политика безопасности организации поддерживается набором специализированных политик и процедур безопасности.

Специализированные политики безопасности. Потенциально существуют десятки специализированных политик, которые могут применяться большинством организаций среднего и большого размера. Некоторые политики предназначаются для каждой организации, другие - специфичны для определенных компьютерных окружений.

С учетом особенностей применения специализированные политики безопасности можно разделить на две группы:

- политики, затрагивающие значительное число пользователей (политика допустимого использования, политика удаленного доступа к ресурсам сети, политика защиты информации, политика защиты паролей и др.);
- политики, связанные с конкретными техническими областями (политика конфигурации межсетевых экранов, политика по шифрованию и управлению криптоключами, политика безопасности виртуальных защищенных сетей VPN, политика по оборудованию беспроводной сети и др.).

Рассмотрим подробнее некоторые из ключевых специализированных политик.

Политика допустимого использования. Ее цель - установление стандартных норм безопасного использования компьютерного оборудования и сервисов в компании, а также соответствующих мер безопасности

сотрудников для защиты корпоративных ресурсов и собственной информации.

Политика допустимого использования предназначена в основном для конечных пользователей и указывает им, какие действия разрешаются, а какие запрещены. Политика допустимого использования устанавливает:

- ответственность пользователей за защиту любой информации, используемой и/или хранимой их компьютерами;
- правомочность пользователей читать и копировать файлы, которые не являются их собственными, но доступны им;
- уровень допустимого использования электронной почты и Web-доступа.

Специального формата для политики допустимого использования не существует: должно быть указано имя сервиса, системы или подсистемы (например, политика использования компьютера, электронной почты, компактных компьютеров и паролей) и описано в самых четких терминах разрешенное и запрещенное поведение, а также последствия нарушения ее правил и санкции, накладываемые на нарушителя.

Политика удаленного доступа. Ее цель - установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании. Эта политика касается всех сотрудников, поставщиков и агентов компании при использовании ими для удаленного соединения с сетью компании компьютеров или рабочих станций, являющихся собственностью компании или находящихся в личной собственности.

Политика удаленного доступа:

- намечает и определяет допустимые методы удаленного соединения с внутренней сетью;
- существенна в большой организации, где сети территориально распределены;
- должна охватывать по возможности все распространенные методы удаленного доступа к внутренним ресурсам.

Политика удаленного доступа определяет:

- какие методы разрешаются для удаленного доступа;
- ограничения на данные, к которым можно получить удаленный доступ;
- кто может иметь удаленный доступ.

Процедуры безопасности являются необходимым и важным дополнением политикам безопасности. Политики безопасности только описывают, что должно быть защищено и каковы основные правила защиты. Процедуры безопасности определяют, как защитить ресурсы и каковы механизмы выполнения политики, т. е. как реализовывать политики безопасности.

По существу процедуры безопасности представляют собой пошаговые инструкции для выполнения оперативных задач. Часто процедура является тем инструментом, с помощью которого политика преобразуется в реальное действие. Например, политика паролей формулирует правила

конструирования паролей, правила о том, как защитить пароль и как часто его заменять, процедура управления паролями описывает процесс создания новых паролей, распределения, а также процесс гарантированной смены паролей на устройствах.

Рассмотрим несколько важных процедур безопасности, которые необходимы почти каждой организации.

Процедура реагирования на события является необходимым средством безопасности для большинства организаций. Организация особенно уязвима, когда обнаруживается вторжение в ее сеть или когда она сталкивается со стихийным бедствием.

Практически невозможно указать отклики на все события нарушений безопасности, но нужно стремиться охватить основные типы нарушений, которые могут произойти. Например: сканирование портов сети, атака типа «отказ в обслуживании», компрометация хоста, НСД и др.

Данная процедура определяет:

- обязанности членов команды реагирования;
- какую информацию регистрировать и прослеживать;
- как обрабатывать исследование отклонений от нормы и атаки вторжения;
- кого и когда уведомлять;
- кто может выпускать в свет информацию, и какова процедура выпуска информации;
- как должен выполняться последующий анализ и кто будет в этом участвовать.

Процедура управления конфигурацией обычно определяется на корпоративном уровне или уровне подразделения. Эта процедура должна определить процесс документирования и запроса изменений конфигурации на всех уровнях принятия решений.

Процедура управления конфигурацией определяет:

- кто имеет полномочия выполнить изменения конфигурации аппаратного и программного обеспечения;
- как тестируется и инсталлируется новое аппаратное и программное обеспечение;
- как документируются изменения в аппаратном и программном обеспечении;
- кто должен быть проинформирован, когда случаются изменения в аппаратном и программном обеспечении.

Процесс управления конфигурацией важен, так как документирует сделанные изменения и обеспечивает возможность аудита; документирует возможный простой системы; дает способ координировать изменения так, чтобы одно изменение не помешало другому.

Политика безопасности определяет стратегию управления в области информационной безопасности, а также меру внимания и количество ресурсов, которые считает целесообразным выделить руководство.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для КС организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п.

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого конкретными документами специализированных политик и процедур безопасности.

2.3 Вопросы к лекции

2.3.1 Что понимается под политикой безопасности организации?

2.3.2 Какова структура политики безопасности организации?

2.3.3 Что характерно для базовой политики безопасности?

2.3.4 Что характерно для специализированной политики безопасности?

2.3.5 Охарактеризуйте ключевые специализированные политики.

2.3.6 Для чего предназначены процедуры безопасности?

2.3.7 Охарактеризуйте наиболее важные процедуры безопасности.