Защита конфиденциальности информации

Основные понятия

Целостность

Доступность

Конфиденциальность

Апеллируемость или неотказуемость

Подотчетность

Достоверность

Аутентичность или подлинность

Угрозы доступности

Внутренние источники угроз доступности. Самыми частыми и опасными с точки зрения размера ущерба являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки являются непосредственными угрозами, например, неправильно введенные данные или ошибка в программе, вызвавшие крах системы, иногда они создают уязвимости, которыми могут воспользоваться злоумышленники.

– Отступление (случайное или умышленное) от установленных правил эксплуатации;

– Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т. п.); – Ошибки при (пере)конфигурировании системы;

– Отказы программного и аппаратного обеспечения;

– Разрушение или повреждение аппаратуры.

digital academy

Угрозы целостности

Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т.п.). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений. Соответствующие действия в сетевой среде называются активным прослушиванием

Угроза конфиденциальности

- Кражи и подлоги
- Дублирование данных
- Внесение дополнительных сообщений
- Нарушение целостности программ (внедрение вредоносного кода)

Кражи и подлоги стоят на втором месте по размерам нанесенного ущерба (после непреднамеренных ошибок пользователей). Могут быть украдены как информация, так и носители информации. Это может быть преднамеренно сделано сотрудником (копирование или изменение данных), может произойти с помощью использования вредоносных программ (троянские).

digital academy

Вредоносное программное обеспечение

Мы выделим следующие *грани вредоносного ПО*:

- вредоносная функция;
- способ распространения;
- *внешнее представление*.

Часть, осуществляющую разрушительную функцию, будем называть ***"бомбой"*** (хотя, возможно, более удачными терминами были бы "заряд" или "боеголовка"). Вообще говоря, спектр вредоносных функций неограничен, поскольку *"бомба"*, как и любая другая *программа*, может обладать сколь угодно сложной логикой, но обычно *"бомбы"* предназначаются для:

- внедрения другого *вредоносного ПО* ;
- получения контроля над *атакуемой* системой;
- *агрессивного потребления ресурсов* ;
- изменения или разрушения программ и/или данных.

По механизму распространения различают:

вирусы - код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы;

"черви" - код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (для активизации *вируса* требуется запуск зараженной программы).

digital academy

Способы защиты

Безопасность зданий, где хранится информация.

Безопасность зданий необходима для защиты от физической кражи оборудования или данных на резервных копиях, а также от физического уничтожения техники и носителей.

Контроль доступа.

Для защиты от несанкционированного доступа к информации используются пароли:

- Вход по паролю может быть установлен в программе BIOS.
- Пароль при загрузке операционной системы (может быть установлен для каждого пользователя).

Если пароль установлен в BIOS, то компьютер не начнет загрузку операционной системы, пока не будет введен правильный пароль. Преодолеть такую защиту нелегко.

При загрузке операционной системы пароль может быть запрошен у любого пользователя (даже если пользователь один).

Помимо паролей можно использовать и *биометрические системы защиты*.

К ним относятся системы идентификации по:

- Отпечаткам пальцев.
- Характеристикам речи.
- Радужной оболочке глаз.
- Изображению лица.
- Геометрии ладони руки.

digital academy

Примеры

Разграничение доступа.
От несанкционированного доступа может быть защищен каждый диск, папка или файл. Для них могут быть установлены определенные права доступа, причем они могут быть различными для разных пользователей.

Дублирование канала связи и создание резервных копий.

Дублирование канала связи необходимо для возможности переключения на резервную систему и запасной канал в случае неисправности действующих систем.

Создание резервных копий защищает от потери данных при сбое оборудования.

Криптография.

Криптография - наука об использовании методов шифрования. Криптография (шифры) используются еще со времен Цезаря и даже более ранних

Использование специальных программ.

Есть множество программ, помогающих защитить информацию на вашем компьютере.

digital academy

Советы

Менеджеры паролей:

LastPass

Knox

digital academy

Оценка защищенности

Чек лист по безопасности:

Для удалённой работы используются защищенные каналы связи, например, при помощи VPN?

При подключении к инфраструктуре пользователь проходит двухфакторную аутентификацию (токены, одноразовые пароли)?

При удалённом подключении не используются личные устройства сотрудников?

При подключении к сети компании происходит проверка удалённых устройств на наличие антивируса и его актуальности и на наличие необходимых обновлений безопасности?

В ИТ-инфраструктуре компании выполнено сегментирование и настроены разграничения доступа, пользователи имеют минимальный для работы набор прав?

– Не используйте пароли повторно
– Никому не раскрывайте свои пароли
– Соблюдайте бдительность и внимательность, совершая действия в сетях общего пользования

– Избегайте перехода по сомнительным ссылкам и загрузок файлов, содержащихся в письмах и сообщениях от незнакомых адресатов

– Избегайте перехода по сомнительным ссылкам и загрузок файлов, содержащихся в письмах и сообщениях от незнакомых адресатов

digital academy

Практическое задание

digital academy

Полезные ссылки

digital academy

Видео

https://www.youtube.com/watch?v=4GdO7SxMUFk

digital academy

Спасибо за внимание!

Присоединяйтесь к нам

Telegram

Facebook

Instagram

academy@idomarketing.io
Юнусалиева 173/2
0(990)037-037

digital academy