Занятие 5

Проблемы безопасности для электронной коммерции

Пример

3.11.88 - Internet Worm (червь) - первая крупная вирусная атака. Создатель вируса - Robert Morris, 23 года, выпускник Корнельского университета.

Вирус поразил 6200 компьютеров (10% Internet), поглощая их ресурсы и заставляя тормозить, а иногда и падать.

Примерная оценка убытков от вируса - от 24 до 100 млн долл.

Вирус распространялся по e-mail.

Компьютерная безопасность

Защита от несанкционированного доступа, использования , изменения и разрушения информации.

- физическая безопасность
- логическая безопасность

Контрмера - процедура, физическая или логическая, которая распознает, уменьшает или уничтожает **угрозу**.

Классификация угроз и контрмер

Аспекты безопасности

Secrecy - секретность - защита против неавторизованного доступа, идентификация источника

Integrity - целостность - защита против неавторизованного изменения информации

Necessity - необходимость - защита против задержки при доставке данных или удаления их

Дополнительно: **Non-repudiation** – что это такое?

Отдельные проблемы безопасности

Интеллектуальная собственность. Причины нарушения:

- легкость доступа к информации -чтение и копирование;
- незнание законов, невежество.

Cybersquatting - практика регистрации доменного имени, которое является торговой маркой какой-либо организации, с целью продажи этого имени за большую сумму.

Политика безопасности

Любая организация должна иметь **инструкцию**, или **свод правил** безопасности, в которых четко определяется:

что защищать, **почему**, **кто** ответственный, **кто** к **чему** имеет доступ, и т.п.

Главные аспекты политики безопасности:

- физическая безопасность,
- сетевая безопасность,
- авторизация доступа,
- защита от вирусов,
- восстановление информации в случае сбоев.

Угрозы безопасности

Рассмотрим «electronic commerce chain» - путь информации от клиента до сервера. Безопасность этого пути = безопасности самого слабого звена в нем.

Классификация угроз:

- угрозы на стороне клиента
- угрозы при передаче информации через Интернет
- угрозы на стороне сервера

Клиентские угрозы

Active content (активное содержимое), может содержать скрытые опасные команды:

Java - объектно-ориентированный язык**,** разработанный Sun Microsystem (раннее название - OAK), его приверженцы верят, что это язык будущего, и java-программы будут встраиваться в микрочипы на бытовой технике (и тостер в 7.30 утра будет будить кофеварку). Плюсы:

- платформонезависимость
- «разрабатываем однажды, применяем везде»

Java-applets.

Специальная модель безопасности - «Java sandbox», применяется для всех untrusted applets (запрещаются ввод-вывод, удаление файлов).

Trusted и Signed applets

Клиентские угрозы

JavaScript -производный от Java язык, разработанный Netscape, может также содержать опасные инструкции, разрушительные для компьютера и нарушающие секретность.

ActiveX (только в Windows) - написанные на ООЯ программы (C++, VB), заключенные в соответствующую оболочку (dll, exe).

Графика и plug-ins

E-mail attachments.

Cookies

Web-bugs – что это такое, в чем опасность и как бороться?

Угрозы при передаче информации

Интернет по своей сути не является безопасной сетью. Любое сообщение проходит через цепочку маршрутизаторов, и эта цепочка не всегда одна и та же.

Sniffer-программы - ”подслушивающие" программы, способные копировать информацию, проходящую через маршрутизаторы от источника к месту назначения.

Другая опасность возникает если, например, мы набрали конфиденциальную информацию, отослали ее (методом GET), и не дождавшись ответа, переместились на другой сайт. Если этот сайт собирает информацию о предыдущих страницах, то он сможет прочитать наши конфиденциальные данные.

Угрозы при передаче информации

Против предыдущей угрозы можно бороться с помощью анонимных прокси-серверов. Например, **Anonomizer.com** - портал анонимности, работает как firewall. Ставит свой адрес перед любым URL, исключая тем самым вышеуказанную угрозу.

Masquerading или **spoofing** (маскировка) - претензия быть чем-то или кем-то, кем вы на самом деле не являетесь (например, отправление почтового сообщения от чужого имени или подмена настоящего Web-сайта ложным).

С маскировкой тесно связано понятие **Fishing –** размещение в письмах или web-страницах поддельных ссылок на сайт злоумышленников.

Задержка или **отказ** в доставке данных, например, вследствие ddos-атак (1 Интернет-час = 10 секундам реального времени)

Серверные угрозы

Главная проблема - **ошибки** и **дыры** в системе безопасности.

Уровни доступа. Super User. Web-сервер не должен иметь высокий уровень доступа. Любой программе, выполняемой на сервере, нужно давать минимальные права, необходимые для ее работы.

Не следует предоставлять доступ к **просмотру** каталогов через браузер. Следует либо явно запрещать доступ (ошибка 403), либо создавать файл по умолчанию (Index.html и др.),

Логины и пароли - как их передавать, как их хранить (хэш-значения).

Серверные угрозы

Серверные сценарии (ASP, Perl, PHP и т.п.)

Логические бомбы

SQL-инъекции

Cross-site scripting **((пример)**

DDOS - что это такое, в чем опасность и как бороться?

Buffer overflow (переполнение буфера оперативной памяти)