# Что такое политика безопасности?

Вопрос безопасности всегда стоял перед компьютерными сетями, но сегодня как никогда растет осознание того, насколько важна безопасность компьютерных сетей в корпоративных инфраструктурах. В настоящее время для каждой корпоративной сети необходимо иметь четкую политику в области безопасности. Эта политика разрабатывается на основе анализа рисков, определения критически важных ресурсов и возможных угроз.

Политикой безопасности можно назвать и простые правила использования сетевых ресурсов, и детальные описания всех соединений и их особенностей, занимающие сотни страниц. Определение RFC 2196 (которое считается несколько узким и ограниченным) описывает политику безопасности следующим образом: "Политика безопасности - это формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и информации".

Важно понять, что сетевая безопасность - это эволюционный процесс. Нет ни одного продукта, способного предоставить корпорации полную безопасность. Надежная защита сети достигается сочетанием продуктов и услуг, а также грамотной политикой безопасности и ее соблюдением всеми сотрудниками сверху донизу. Можно заметить, что правильная политика безопасности даже без выделенных средств защиты дает лучшие результаты, чем средства защиты без политики безопасности.

Политика безопасности сети предприятия является результатом оценки риска и определения важных средств и возможных угроз. Средства сети в себя включают:

* Хосты сети (такие как ПК; включает операционные системы, приложения и данные хостов)
* Устройства сети (такие как маршрутизаторы, коммутаторы и межсетевые экраны)
* Данные сети (данные, которые передаются по данной сети)

Вы должны установить, как средства Вашей сети, так и степень, в которой каждое из этих средств должно быть защищено. Если устройства сети или данные подвергнуты риску, приведет ли это к затруднению или краху? Чем больше вероятность краха, тем строже должна быть политика обеспечения безопасности.

Базовыми элементами политики в области безопасности являются идентификация, целостность и активная проверка. Идентификация призвана предотвратить угрозу обезличивания и несанкционированного доступа к ресурсам и данным. Целостность обеспечивает защиту от подслушивания и манипулирования данными, поддерживая конфиденциальность и неизменность передаваемой информации. И наконец, активная проверка (аудит) означает проверку правильности реализации элементов политики безопасности и помогает обнаруживать несанкционированное проникновение в сеть и атаки типа DoS.

Механизмы идентичности необходимо внедрять осторожно, т.к. даже самая продуманная политика может быть расстроена, если сложно использовать усовершенствования. Классическим примером является запись пароля на клочке бумаги и прикрепление его к монитору компьютера - что является выходом для потребителя, который должен помнить множество паролей для получения доступа к меняющимся составным частям сети. Обременительные или чрезмерно дублированные системы верификации и авторизации могут расстроить пользователей, поэтому их следует избегать. Методы идентификации могут основываться на протоколе S/Key или осуществляться при помощи специальных аппаратных средств (token password authentication). А в среде модемного доступа часто применяется механизм идентификации по протоколу Point-to-Point Protocol (PPP), который включает использование протоколов Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP) и Extensible Authentication Protocol (EAP).

Целостность - это элемент, который включает безопасность устройства инфраструктуры сети (физический и логический доступ), безопасность периметра и конфиденциальность данных. Безопасность физического доступа может выражаться в размещении оборудования сети в специально созданных для этого оборудования шкафах, которые имеют ограниченный доступ.

Безопасность логического доступа главным образом относится к обеспечению механизмов идентичности (идентификации и авторизации) перед тем, как дать доступ для сети связи Telnet или для терминала к компонентам инфраструктуры общей сети (например, маршрутизаторам или межсетевым экранам). Безопасность периметра связана с функциями межсетевых экранов, определяющих, какой трафик разрешен или запрещен от различных зон сети, обычно - между сетью Интернет и главным комплексом или между пользователями удаленного доступа и главным комплексом.

Конфиденциальность данных может обеспечиваться протоколами безопасности на транспортном уровне SSL и Secure Shell Protocol (SSH), которые осуществляют безопасную передачу данных между клиентом и сервером. Безопасный протокол передачи гипертекста (S-HTTP) предоставляет надежный механизм Web-транзакций, однако в настоящее время наиболее популярным средством является SSL. Средство SOCKS является рамочной структурой, позволяющей приложениям клиент/сервер в доменах TCP и UDP удобно и безопасно пользоваться услугами сетевого межсетевого экрана. Протокол безопасности IP (IPSec) представляет собой набор стандартов поддержки целостности и конфиденциальности данных на сетевом уровне (в сетях IP). X.509 является стандартом безопасности и идентификации, который поддерживает структуры безопасности электронного информационного транспорта.

Последним главным элементом системы безопасности является аудит, который необходим для слежения и верификации процесса исследования политики безопасности. Для испытания эффективности инфраструктуры системы безопасности, аудит безопасности должен происходить часто, через равные промежутки времени. Он также должен включать проверки установки новой системы, методы для определения возможной вредительских действий кого-либо из внутреннего персонала и возможного наличия особого класса проблем (нападения типа "отказ в сервисе"), а также общее следование политике безопасности объекта.

При разработке политики безопасности необходимо учитывать требование сбалансировать легкость доступа к информации и адекватный механизм идентификации разрешенного пользователя и обеспечения целостности и конфиденциальности данных. Политика безопасности должна внедрятся принудительно как технически, так и организационно - тогда она будет по-настоящему эффективна

Основу стабильности сети составляют надежность ЭВМ и сетевого оборудования, а также устойчивость каналов связи. Каналы связи, особенно если речь идет о проводных, достались нам от проклятого царизма, их создатели давно умерли и спросить не с кого. Начинать надо с того, что в вашей власти, а это прежде всего правильная конфигурация узла, разумное распределение ответственности и качество сетевого питания (стабильность напряжения и частоты, амплитуда помех). Для решения последней проблемы используют специальные фильтры, мотор-генераторы и UPS (Uninterruptable Power Supply). Выбор того или иного решения зависит от конкретных условий, но для серверов использование UPS крайне желательно (ведь вы не хотите восстанавливать дисковую систему, которая разрушилась из-за отключения питания в момент записи в FAT или dir). При снижении напряжения сети переменного тока ниже определенного уровня UPS (около 208v) отключает потребителя от сети и осуществляет питание ЭВМ от ~220v, получаемого от аккумулятора самого UPS. Учитывая нестабильность напряжения сети в России, можно считать полезным применение активных стабилизаторов на входе UPS.

При выборе UPS нужно учесть суммарную потребляемую мощность оборудования, подключаемого к источнику питания, и время, в течение которого UPS способен работать без напряжения в сети. При этом главная задача UPS - обеспечение завершения операций обмена с диском до того, как произойдет полное обесточивание сервера, или когда будет произведено переключение на резервный канал питания. Это осуществимо при использование специального интерфейса и соответствующего программного обеспечения, работающего согласно протокола SNMP(см. рис. 6.1.1).

Рис. 6.1.1. Схема подключения UPS.

При исчезновении первичного напряжения ~220V спустя некоторое время UPS выдает сигнал shutdown вычислительной машине. Современный UPS может мониторировать не только напряжение питание, но температуру окружающей среды, своевременно осуществляя спасение жизненно важных файлов до наступления чрезмерного перегрева системы. При этом значение напряжения питания и температуры можно считывать с использованием протокола SNMP. Некоторые продвинутые системы автономного питания допускают подключение агентов SNMP непосредственно к локальной сети, что открывает дополнительные возможности дистанционного управления и мониторинга.

Указанный интерфейс обеспечит блокировку начала новых операций обмена или выполнит shutdown, если напряжение в сети упало ниже допустимого уровня. К UPS не следует подключать дисплеи (эти приборы не столь критичны к питанию, как диски и оперативная память) и принтеры (лазерные принтеры запрещено подключать к UPS из-за мощных печек, входящих в состав этих приборов). Сетевые фильтры являются желательными при работе с любыми ЭВМ, так как сеть в России сильно засорена высокочастотными помехами.

Создавая сеть, следует сразу закладывать некоторые элементы, обеспечивающие безопасность. Так прокладку сетевых кабелей желательно производить в металлических коробах или трубах, что сделает подключение к ним более затруднительным. Повторители и концентраторы нужно размещать в запираемых шкафах. Некоторые концентраторы контролируют MAC-адреса пакетов. Такое оборудование позволяет блокировать порт, если обнаруживаются пакеты с неизвестным MAC-адресом, а также выявлять случаи подключения одного и того же MAC-адреса к разным портам. Определенную угрозу сетевой безопасности может представлять возможность присвоение хакером “чужого” MAC-адреса своей сетевой карте. Современные концентраторы запрещают подключенному к порту узлу передавать кадры с MAC-адресом, не совпадающим с определенным администратором для данного порта. Это обеспечивает дополнительную надежность канального уровня.

Активные разработки в последнее время ведутся в области систем идентификации, базирующихся на распознавания отпечатков пальцев, ладони, подписи, голоса или радужки глаз. Для этих целей используются новейшие достижения в области быстрых Фурье-преобразований, нейронных сетей и пр. В качестве вводных устройств используются оптические сканеры, а также резистивные экраны. Для ввода подписи служат специальные планшеты, а также изощренные методы сравнения и установления идентичности. К числу таких устройств следует отнести также генераторы разовых ключей доступа и карты доступа. В последнее время в этот ряд встали и мобильные телефоны, которые позволяют идентифицировать владельца (здесь имеются в виду многопараметрические системы аутентификации).

Так как современные системы шифрования предполагают использование довольно трудоемких вычислений, которые заметно замедляют процесс, разрабатываются специальные микросхемы. Такие системы могут использоваться, например, в VPN. При этом ключи могут быть встроенными или внешними. В некоторых особо важных случаях применяется криптографическая защита всего диска FDE (Full Disc Encription) на самой машине.

Поскольку абсолютная надежность недостижима, одним из средств сохранения информации является дублирование носителей (напр. дисков), копирование и сохранение копий в надежном месте. Если раньше для этой цели годились гибкие диски или магнитные ленты, сегодня их пригодность может быть подвергнута сомнению. Конечно, ленты типа Exabyte емкостью 2.5-10Гбайт (2000 год) еще достаточно широко используются, высокая стоимость таких накопителей ограничивает их применимость (да и скорость записи на них оставляет желать лучшего). Альтернативой им могут стать накопители с перезаписываемыми DVD, где стоимость устройства несколько ниже. Не исключено, что в скором времени основным средством сохранения информации станет ее дублирование на независимом жестком диске. Это может произойти при широком внедрении компактных жестких дисков емкостью 1 Тбайт и более (появились в 2009 году).

Мало периодически выполнять резервное копирование носителей, хранящих существенную информацию. Важно разумно организовать сохранность этих копий. Даже если они хранятся в суперсейфе в том же помещении, что и сервер ваша система резервного копирования уязвима в случае пожара или залива помещения водой. По этой причине резервные копии желательно хранить в другом здании. Другой важной стороной работы с резервными копиями является свод правил доступа к ним и методов использования. Особенно важно, чтобы резервные копии с конфиденциальными данными не могли попасть в чужие руки (потеря или кража laptop'а с резервной копией может быть хорошей иллюстрацией такого рода проблем). Для конфиденциальной информации должен действовать строгий запрет резервного копирования на носитель рабочей станции при знакомстве с документом. Это с неизбежностью приведет к неконтролируемому распростанению конфиденциальных данных. Одним из путей повышения безопасности является криптографическая защита данных.

Повысить уровень безопасности может географическая привязка машин, содержащих конфиденциальную информацию (GPS)

Объем копируемых данных растет от года к году. Сегодня (2009 год) объемы резервных копий в крупных вычислительных центрах достигают петабайт. Но в любых центрах многие файлы хранятся в разных машинах, а иногда и на одной машине можно обнаружить несколько копий одного и того же файла. Система резервного копирования, исключающая дублирование, может существенно поднять эффективность системы копирования. Смотри eGuide: How to Get Started with Data Deduplication. Распознавание файлов осуществляется с помощью контрольных сумм (MD5 - 128 бит и SHA-1 - 160 бит). Разные программные продукты используют различные алгоритмы распознавания файлов. Дедубликация материала позволяет сэкономить объем на носители в 14-18 раз. При этом удается сократить и время копирования до двух раз.

Новым направлением резервного копирования является SaaS (Software as a Service). В этой схеме резервное копирование производится удаленно, а все файлы шифруются с помощью ключа владельца, так что их несанкционирование прочтение не возможно. Этот метод формирования backup становится новым направлением ИТ-бизнеса, который позволяет более экономно использовать ресурсы как клиента, так и фирмы, предоставляющей услуги.

В последнее время широкое распространение получают панели касания, способные распознавать людей по отпечатку пальца или ладони (см. http://elce.quarta.msk.ru/UCC/t\_scrb\_e.htm). Сходные устройства используются для непосредственного ввода подписи клиента (устройство типа планшет, иногда совмещаемое с дисплеем) и сверки ее с имеющимся образцом.

К аппаратным средствам безопасности можно отнести внедрение NX-бит (флагов - не исполнять), в процессорах, которые после загрузки ОС препятствуют модификации текста программы (смотри раздел 6.3.1 данного сервера). Этот прием делает менее вероятной атаку типа переполнения буфера

Решение многих задач безопасности не требует присутствия IT-эксперта.

Из-за непрерывного появления Интернет-червей, вирусов и других компьютерных угроз сетевая безопасность считается главной заботой владельцев предприятий, даже тех, где используются простые сети.

## Хорошая новость: вы и ваши сотрудники можете справиться со многими мероприятиями по обеспечению безопасности самостоятельно, без помощи IT-специалиста. Приведенные ниже действия по обеспечению сетевой безопасности упорядочены по степени сложности. Начните с легких задач и продвигайтесь дальше, как вам позволяют ваше время, ресурсы и уровень квалификации.

| Защита сети малого предприятия |
| --- |
| Простые задачи | Более сложные задачи | Задачи, требующие привлечения профессионалов |
| Установите антивирусное программное обеспечение | Ограничьте доступ к оборудованию | Установите аппаратный брандмауэр |
| Используйте средства обновления программного обеспечения | Установите уровни полномочий | Настройте виртуальную частную сеть |
| Установите защиту от «шпионских» программ | Отключите сетевой доступ для бывших сотрудников | Настройте средства безопасности беспроводной сети |
| Установите программный брандмауэр | Создайте политики для электронной почты и Интернета | Создайте процедуры резервного копирования и восстановления данных |
| Установите программное обеспечение для фильтрации нежелательных сообщений | Требуйте от сотрудников использования сложных паролей | Настройте параметры безопасности базы данных |

##

## Простые задачи

Если вы когда-либо устанавливали программы или настраивали принтер, вам будет нетрудно выполнить эти задачи.

Установите и обновляйте антивирусное программное обеспечение

Установить антивирусное программное обеспечение не трудно. Оно постоянно выполняет проверки для предотвращения заражений, которые могут повредить или уничтожить данные в пределах сети. Но имейте в виду, что хакеры постоянно создают новые вирусы и ваше антивирусное программное обеспечение эффективно только в том случае, если оно способно обнаружить новейшие угрозы. Поэтому при установке антивирусного программного обеспечения настройте его на автоматическую загрузку обновлений для выявления новых вирусов. Если вы купили компьютер с антивирусным программным обеспечением, установленным на испытательный срок, зарегистрируйтесь по истечении бесплатного срока, чтобы продолжить получать обновления, или купите другой антивирусный продукт.

Используйте средства обновления программного обеспечении.

Компании-разработчики программного обеспечения (такие как корпорация Майкрософт) имеют бесплатные средства, которые можно использовать для обновления программного обеспечения, чтобы гарантировать его безопасность. Например, требуется всего лишь несколько щелчков мышью, чтобы настроить функцию автоматического обновления системы Windows XP или Windows Small Business Server. Это средство позволяет системе Windows автоматически подключаться к Интернету, находить и устанавливать последние обновления, чтобы ликвидировать угрозы системе безопасности. После включения службы автоматического обновления с вашей стороны не требуется никаких дальнейших усилий. Программное обеспечение будет обновляться самостоятельно. Пакет Microsoft Office также имеет средство для автоматического обновления.

Установите защиту от «шпионского» программного обеспечения.

Установите и регулярно обновляйте программное обеспечение, которое выполняет поиск «шпионских» программ, пытающихся собирать ваши пароли и номера банковских счетов. Корпорация Майкрософт предлагает бесплатную программу Windows Defender (бета-версия 2) и Средство для удаления вредоносных программ, которые можно использовать для освобождения компьютеров от нежелательного программного обеспечения.

Установите программный брандмауэр.

Брандмауэр проверяет входящие в вашу сеть данные и не пропускает их, если они не удовлетворяют определенным критериям. Программные брандмауэры, такие как встроенный в Windows XP Professional брандмауэр Windows, защищают только компьютер, на котором работают, но являются хорошим дополнением к аппаратным брандмауэрам. Включить брандмауэр Windows легко.

Установите программное обеспечение для фильтрации нежелательных сообщений.

Нежелательные сообщения — это незатребованные коммерческие сообщения, которые могут заполнить почтовые ящики и вынудить сотрудников тратить время на сортировку их содержимого. Хотя чаще всего нежелательные сообщения просто вызывают раздражение, они представляют опасность, если содержат вложения, которые при открытии могут запустить вирус. К тому же некоторые такие сообщения предназначены для фишинга — получения от пользователей пароля и прочей ценной информации обманным путем, что может поставить безопасность предприятия под угрозу. Установка продукта для фильтрации нежелательных сообщений или настройка фильтров программы Outlook 2003 поможет значительно снизить количество нежелательной почты.

## Более трудные задачи

Задачи из данной группы могут быть более сложными. Они требуют более широких технических знаний или постоянного управления вашими политиками и процедурами безопасности.

Ограничьте доступ к оборудованию.

Вы можете усовершенствовать систему безопасности за счет ограничения физического доступа к вашим серверам и сетевому оборудованию, например маршрутизаторам и коммутаторам. По возможности переместите эти компьютеры в запираемую комнату и выдайте ключи только работающим с оборудованием сотрудникам. Это сведет к минимуму вероятность того, что кто-то неподготовленный сможет вмешиваться в работу сервера или пытаться «исправить» проблему.

Установите уровни полномочий.

Вы можете назначить пользователям различные уровни полномочий в сети с помощью системы Windows Small Business Server 2003. Вместо того чтобы предоставлять всем пользователям права администратора, предоставьте им доступ только к конкретным программам и определите, какие полномочия дают возможность доступа к серверу. Например, вы можете разрешить некоторым пользователям читать определенные хранящиеся на сервере файлы, но не изменять их. Только администраторы сети должны иметь доступ ко всем системным файлам и службам.

Отключите сетевой доступ для бывших сотрудников
Исключите возможность входа в сеть бывших сотрудников. Удалить их права доступа нетрудно, но если вы слишком долго ждете, то можете дать возможность раздраженным бывшим сотрудникам повредить или украсть файлы.

Создайте политики для электронной почты и Интернета
Последние исследования показали, что 6 % сообщений электронной почты заражены вирусами и другими программами, которые могут повредить компьютеры. Создайте корпоративную политику работы в Интернете, в которую будут включены инструкции для сотрудников не открывать вложения электронной почты, которых они не ожидали. Политика также должна обращать внимание на рискованные действия в Интернете и запрещать такую деятельность, как загрузка бесплатных средств и других программ. Прикажите сотрудникам не разглашать пароли или сведения о банковском счете в случае если они получили сообщение электронной почты с просьбой об этом.

Требуйте от сотрудников использования сложных паролей
Пароли, которые легко отгадать, могут позволить не имеющим на это прав лицам получить доступ к вашей сети. Чтобы предотвратить это, ваша политика безопасности должна требовать, чтобы пароли содержали буквы, и цифры. И, хотя пароли должны меняться регулярно, не требуйте от сотрудников слишком частой их смены. Если сотрудники стараются запомнить свои пароли, они могут записать их и приклеить на свои мониторы, облегчая другим задачу взлома компьютерной системы.

## Задачи, требующие привлечения профессионалов

Эти задачи не очень технические, но чтобы с ними справиться, вы можете предпочесть нанять консультанта по компьютерам или локальным сетям. Проконсультируйтесь с одним из партнеров корпорации Майкрософт, который обладает опытом помощи в планировании и реализации проектов, требующих высокой квалификации.

Установите брандмауэр на периметре сети предприятия
Тогда как программный брандмауэр защищает компьютер, на котором он установлен, аппаратный брандмауэр подключается к сети предприятия и защищает ее целиком. Примечательная функция аппаратного брандмауэра — возможность блокировать сетевые порты. Заблокировав неиспользуемые порты, вы можете усилить вашу сетевую безопасность и пресечь попытки неавторизованного доступа, так как сетевые порты обеспечивают связь между клиентскими компьютерами и серверами. Эта задача более сложная, так что вы можете воспользоваться помощью эксперта для правильной настройки функций брандмауэра.

Настройте функции безопасности виртуальной частной сети
Подключение внешних пользователей к сети компании через Интернет позволяет им проверять электронную почту и получать доступ к общим файлам. Виртуальная частная сеть позволяет делать это более безопасно. Однако существует значительный риск для системы безопасности каждый раз, когда вы делаете вашу сеть доступной для внешних пользователей. Возможно, вам потребуется пригласить консультанта по безопасности, так как правильно настроить виртуальную частную сеть может быть сложно.

Настройте средства безопасности беспроводной сети
Любой человек в пределах действия беспроводной сети имеет потенциальную возможность принимать или передавать по ней данные. Если вы планируете использовать беспроводную сеть, пригласите IT-специалиста, чтобы гарантировать, что средства безопасности включены и средства шифрования и управления доступом в беспроводных сетях настроены правильно.

Создайте процедуры резервного копирования и восстановления данных.

Эта задача может заключаться в простой записи на компакт-диск файлов данных и хранении их в безопасном месте. Система Windows XP включает средство для резервного копирования и восстановления данных на компьютере. Однако вы можете обратиться к более сложным решениям. Если вам необходимо, чтобы данные были доступны в любое время, необходима помощь IT -специалиста, который может установить дополнительное оборудование для создания копий файлов на разных жестких дисках при каждом их сохранении. Таким образом, если один жесткий диск выходит из строя, можно использовать резервный и тем самым избежать потери данных. Рекомендуется архивировать файлы как минимум раз в неделю и периодически восстанавливать их, чтобы убедиться в том, что это возможно.

Настройте параметры безопасности базы данных.

Если вы имеете базу данных, в которой хранится информация о клиентах, продажах, ресурсах и другие важные данные, касающиеся вашей отрасли, наймите IT-специалистов, чтобы гарантировать, что эта информация хорошо защищена. Например, эксперт по базам данных может защитить сервер Microsoft SQL Server от большинства атак из Интернета, позволив подключаться к ней только прошедшим проверку пользователям. Эксперты также могут создать системы резервного копирования для восстановления данных в случае их потери