Известия Гомельского государственного университета
имени Ф. Скорины, №4(37), 2006

УДК 681.3

Определение политики сетевого доступа

А. Б. Демуськов, В. Л. Мережа, Т. Я. Каморникова, Т. П. Бышик

Одной из политик информационной безопасности предприятия является и политика сетевого доступа [1, 4].

Как показывает опыт, имеется два вида политики сетевого доступа, которые влияют на проектирование, установку и использование систем защиты, таких как брандмауэр. Политика верхнего уровня является концептуальной и она определяет:

- доступ к каким сервисам будет разрешен или явно запрещен из защищаемой сети;
- как эти сервисы будут использоваться;
- при каких условиях будет делаться исключение и политика не будет соблюдаться.

Политика нижнего уровня описывает, как система защиты должна на самом деле ограничивать доступ и фильтровать сервисы, которые указаны в политике верхнего уровня.

Существует ряд вариантов этой политики, которые можно реализовать. Это такие как:

- запрет доступа извне;
- неограниченный доступ в Internet;
- ограниченный входящий доступ;
- ограниченный выходящий доступ [5, 6].

Политика проектирования брандмауэра [2, 3] как средства защиты в основном определяет политику сетевого доступа: чем строже политика проектирования брандмауэра, тем более строгой будет и политика сетевого доступа. Поэтому, прежде всего, нужно определиться с политикой проектирования брандмауэра.

Она специфична для конкретного брандмауэра. Она определяет правила, используемые для реализации политики доступа к сервисам. Нельзя разрабатывать эту политику, не понимая такие вопросы, как возможности и ограничения брандмауэра, угрозы и уязвимые места, связанные с TCP/IP. Как правило, реализуется одна из двух базовых политик:

- разрешить доступ для сервиса, если он явно не запрещен;
- запретить доступ для сервиса, если он явно не разрешен.

Брандмауэр, который реализует первую политику, пропускает все сервисы в сеть по умолчанию, если только этот сервис не был явно указан в политике управления доступом как запрещенный. Брандмауэр, который реализует вторую политику, по умолчанию запрещает все сервисы, но пропускает те, которые указаны в списке разрешенных сервисов. Вторая политика следует классической модели доступа, используемой во всех областях информационной безопасности.

Первая политика менее желательна, так как она предоставляет больше способов обойти брандмауэр, например, пользователи могут получить доступ к новым сервисам, не запрещаемым политикой (или даже не указанных в политике), или запустить запрещенные сервисы на нестандартных портах TCP/UDP, которые не запрещены политикой. Определенные сервисы, такие как X Windows , FTP, ARCHIE и RPC, сложно фильтровать, и для них лучше подходит брандмауэр, реализующий первую политику. Вторая политика строже и безопаснее, но ее тяжелее реализовать, и она может повлиять на работу пользователей в том отношении, что ряд сервисов, такие, как описанные выше, могут оказаться блокированными или использование их будет ограничено.

Реализация политики доступа к сервисам сильно зависит от возможностей и ограничений системы брандмауэра, а также уязвимых мест, имеющихся в разрешенных интернетовских сервисах. Например, может оказаться необходимым запретить сервисы, разрешенные политикой доступа к сервисам, если уязвимые места в них не могут эффективно контро-

лироваться политикой нижнего уровня и если безопасность сети важнее всего. С другой стороны, организация, которая сильно зависит от этих сервисов при решении своих задач, может принять этот более высокий риск и разрешить доступ к этим сервисам. Эта взаимосвязь приводит к тому, что формулирование обоих политик становится итеративным процессом.

Политика доступа к сервисам – самый важный компонент из четырех, описанных выше. Остальные три компонента используются для реализации политики. И, как отмечалось выше, политика доступа к сервисам должна отражать общую политику безопасности организации [2]. Эффективность системы брандмауэра при защите сети зависит от типа используемой реализации, от правильности процедур работы с ним и от политики доступа к сервисам.

Типовыми политиками проектирования брандмауэра являются запрет всех сервисов, кроме тех, что явно разрешены, или разрешение на доступ ко всем сервисам, кроме тех, что явно запрещены. Первый тип более безопасен и поэтому предпочтителен, но он также более строг, в результате чего при нем допускается работа меньшего числа сервисов. Кроме того, примеры показывают, что системы, требующие обеспечения доступа к сервисам, не пропускаемым брандмауэром, могут быть размещены в изолированных подсетях отдельно от других внутренних систем. Ключевым моментом здесь является то, что в зависимости от требований обеспечения безопасности и гибкости, некоторые типы брандмауэров более предпочтительны, чем другие. Этот факт подчеркивает важность правильного выбора политики до начала создания брандмауэра.

Для того, чтобы правильно разработать концептуальную политику брандмауэра, а затем систему брандмауэра, которая реализует эту политику, требования безопасности рекомендуют, чтобы сначала был разработан самый безопасный вариант политики – то есть запретить все сервисы, кроме тех, что явно разрешены. Разработчики политики должны разбираться в следующих вопросах:

- какие сервисы в Internet организация планирует использовать (например, TELNET, WWW, NFS и т.д.)
- каким образом эти сервисы будут использоваться, то есть локально, через Internet, по модему из дома или из удаленных подразделений;
- дополнительные потребности, такие как шифрование и обеспечение работы по модему;
- какие риски связаны с предоставлением этих сервисов;
- какова стоимость средств защиты;
- каковы изменения в возможностях использования сети при обеспечении защиты;
- приоритеты обеспечения безопасности при использовании тех или иных сервисов по отношению к возможности использовать их.

Любая политика безопасности, связанная с доступом из Internet, сервисами Internet и доступом к сети вообще должна быть гибкой. Эта гибкость должна иметься по двум причинам: сам Internet постоянно меняется, и потребности организации могут измениться по мере появления новых сервисов в Internet и новых способов выполнения деятельности организации. Появляются новые протоколы и новые сервисы в Internet, которые предоставляют новые возможности организациям, использующим Internet, но это может привести к появлению новых проблем с безопасностью. Поэтому политика должна иметь возможности учета и включения этих новых проблем с безопасностью. Другая причина заключается в том, что риски для организации также не являются постоянными. Риск может измениться из-за больших изменений, таких как новые обязанности, возложенные на организацию, или маленьких изменений, таких как изменения конфигурации сети.

Теперь рассмотрим политику аутентификации удалённых пользователей.

Удаленные пользователи – это те пользователи, которые устанавливают соединения с внутренними системами откуда-либо из Internet. Эти соединения могут исходить от любого места в Internet, от модемных линий, от авторизованных пользователей, работающих из дома. В любом случае для всех таких соединений должны использоваться меры усиленной аутентификации брандмауэра перед предоставлением доступа к внутренним системам. В политике должно быть указано, что удаленные пользователи не могут получать доступ к си-

стемам с помощью неавторизованных модемов. Не должно быть исключений для этого правила, так как даже один перехваченный пароль или один неконтролируемый модем может открыть «проход» в обход брандмауэра.

Такая политика имеет и недостатки:

- необходимо обучать пользователей пользоваться средствами усиленной аутентификации;
- трата средств на устройства аутентификации пользователей и администрирование удаленного доступа.

Но будет ещё большей глупостью установить брандмауэр и не контролировать удаленный доступ.

Полезной возможностью для авторизованных пользователей является наличие удаленного доступа к внутренним системам, когда пользователи находятся вне сети. Такая возможность позволяет им осуществлять доступ к системам из мест, где Internet может быть и не доступен. Но эти возможности являются одним из путей получения доступа злоумышленником.

Авторизованные пользователи могут также хотеть иметь возможность исходящих звонков для доступа к системам в других местах, к которым невозможен доступ через Internet. Эти пользователи должны понимать, что они могут создать уязвимые места при небрежном обращении с модемом. Возможность исходящих звонков легко может позволить организовать и входящие звонки, если не принять соответствующие предосторожности.

Обе эти возможности должны учитываться при разработке брандмауэра и включаться при необходимости в него. Требование обязательности использования мер усиленной аутентификации при доступе через брандмауэр должно быть обязательно отражено в политике. Политика также может запрещать использование неавторизованных модемов, присоединенных к системам сети, если доступ по модему обходит средства защиты брандмауэра. Строгая политика может ограничить число используемых модемов в сети, уменьшая, таким образом, её уязвимость.

Помимо соединений через модемы, политика должна регламентировать использование соединений с помощью протоколов SLIP и PPP. Пользователи могут использовать их для создания новых сетевых соединений внутри защищенной сети. Такое соединение потенциально является способом обхода брандмауэра и может оказаться даже более опасным, чем коммутируемое соединение.

Сеть, которая предоставляет доступ к информационному серверу, должна учесть этот вид доступа при проектировании брандмауэра. Хотя информационный сервер создает специфические проблемы с безопасностью, он не должен стать уязвимым местом для сети. В политике должна быть отражена посылка, что безопасность сети не должна пострадать из-за того, что нужно иметь информационный сервер. Также необходимо учитывать, что трафик, связанный с информационным сервером, в корне отличается от трафика, связанного с работой других приложений, например, таких как электронная почта. С каждым из этих двух видов трафика связаны свои риски, и не следует их смешивать.

И наконец, для достижения положительных результатов от применения рассмотренных политик сетевого доступа необходимо, чтобы эти политики были не только декларированы, а доведены пользователю и наглядны. Наглядность помогает реализовать политику, помогая гарантировать ее знание и понимание всеми сотрудниками организации. Презентации, видеофильмы, семинары, вечера вопросов и ответов и статьи во внутренних изданиях организации увеличивают ее наглядность. Программа обучения в области компьютерной безопасности и контрольные проверки действий в тех или иных ситуациях могут достаточно эффективно уведомить всех пользователей о новой политике. С ней также нужно знакомить всех новых сотрудников организации.

Политики компьютерной безопасности должны доводиться таким образом, чтобы гарантировалась поддержка со стороны руководителей подразделений, особенно, если на сотрудников постоянно сыплется масса политик, директив, рекомендаций и приказов. Политика организации – это средство довести позицию руководства в отношении компьютерной безопасности и явно указать, что оно ожидает от сотрудников действий в тех или иных ситуациях и регистрации своих действий.

Для того, чтобы быть эффективной, политика должна быть согласована с другими существующими директивами, законами, приказами и общими задачами организации. Она также должна быть интегрирована и согласована с другими политиками предприятия (например, политикой по приему на работу).

Abstract. The problems of computer networks in the field of information safety and the principles and criteria of ensuring information safety are considered in the paper.

Литература

1. В. А. Герасименко, А. А. Малюк, Основы защиты информации, Москва, МИФИ, 1997.

2. Научная сессия МИФИ-2003. X всероссийская научная конференция «Проблемы информационной безопасности в системе высшей школы». Сборник научных трудов. Москва, МИФИ, 2003.

3. Гостехкомиссия России. Руководящий документ. Концепция защиты СВТ и АС от НСД к информации, Москва, 1992.

4. А. Б. Демуськов, Г. И. Большакова, Т. П. Бышик, Проблемы информационной безопасности в компьютерных сетях, Известия Гомельского государственного университета имени Ф. Скорины, №3(18) (2003), 124–129.

5. А. Б. Демуськов, В. А. Короткевич, Л. И. Короткевич, Политики информационной безопасности предприятий, Известия Гомельского государственного университета имени Ф. Скорины, №4(19) (2003), 31–36.

6. А. Б. Демуськов, Т. П. Бышик, Т. Я. Каморникова, О реализации политик информационной безопасности предприятия, Известия Гомельского государственного университета имени Ф. Скорины, №5(32) (2005), 110–113.

Гомельский государственный
университет имени Ф. Скорины

Поступило 15.05.06