Microsoft Business Solutions

Navision Security Hardening Guide

Дата публикации: октябрь 2004 г.

Microsoft

Содержание

Введение

Microsoft® Windows® обеспечивает поддержку сложных систем безопасности сетей, основанных на промышленных стандартах. В широком понимании безопасность предполагает тщательное планирование и учет компромиссов. Например, компьютер можно закрыть в охраняемом помещении, разрешив физический доступ к нему только одному системному администратору. Этот компьютер может быть физически защищен, но без связи с другими компьютерами он будет бесполезен. Таким образом, нужно решить, как сделать сеть как можно более безопасной, не принося при этом в жертву удобство в работе.

В большинстве организаций осознают опасность внешних атак и применяют различные конструкции брандмауэров, однако многие компании даже не задумываются о том, как смягчить последствия нарушения системы безопасности в случае преодоления брандмауэра злоумышленниками. В клиентской среде меры безопасности будут хорошо восприниматься и работать, если пользователям для ведения своего бизнеса безопасным способом не придется выполнять слишком много процедур и шагов. Реализация политик безопасности должна быть по возможности простой для пользователей, в противном случае они будут склонны искать более простые, но менее безопасные способы выполнения своих функций.

Так как размер установок Navision может варьироваться в широких пределах, важно тщательно проанализировать потребности каждого заказчика и взвесить эффективность мер безопасности в сравнении с потенциальными затратами. Исполнитель проекта как доверенный советник заказчика должен произвести необходимые исследования и рекомендовать политику безопасности, которая в наибольшей степени удовлетворит потребности заказчика, не создавая трудностей, которые могут, в конечном счете, побудить его прекратить использовать эту политику.

Советы и рекомендации по обеспечению безопасности в среде Navision

Следующие общие правила помогут повысить уровень безопасности среды Navision:

- Чтобы в качестве службы запустить сервер базы данных Navision или при запуске сервера использовать параметр командной строки *installasservice*, необходимо, чтобы служба работала под учетной записью NT Authority\Network Service. Учетная запись NT Authority\Network Service существует только на Windows™ XP и Windows Server™ 2003. При работе на Windows 2000 Server следует создать учетную запись с минимальными привилегиями для службы, либо службе будет назначена учетная запись «Локальная система». Эта учетная запись должна иметь не больше привилегий, чем обычные учетные записи пользователей, или быть учетной записью домена без административных привилегий в домене или на локальном компьютере.

  Чтобы пользователи могли подключаться к базе данных, учетной записи NT Authority\Network Service или учетной записи пользователя, под которой работает сервер, необходимо предоставить доступ для чтения и записи к файлам базы данных.

  Чтобы предоставить доступ для чтения и записи к файлам базы данных учетной записи NT Authority\Network Service ▫ Windows XP, выполните следующие действия:

  1. В Проводнике Windows перейдите в папку, содержащую файл базы данных.
  2. Выберите базу данных, щелкните ее правой кнопкой мыши и выберите команду «Свойства».
  3. В окне ***Свойства*** откройте вкладку ***Безопасность*** и ниже поля ***Группы и пользователи*** нажмите кнопку «Добавить».
  4. В диалоговом окне ***Выбор: Пользователи, Компьютеры или Группы*** введите *Network Service* и нажмите кнопку «ОК».
  5. NETWORK SERVICE будет добавлено в поле ***Группы и пользователи*** в окне ***Свойства***.
  6. Выберите NETWORK SERVICE и в поле **Разрешения** добавьте разрешения *Чтение* и *Запись*.

- По умолчанию служба сервера приложений Navision работает как учетная запись NT Authority\Network Service, что позволяет ей обращаться к серверу базы данных Navision локально. Однако, если требуется иметь доступ к серверу базы данных в сети, служба сервера приложений Navision должна работать как учетная запись домена Windows, которая распознается сервером базы данных Navision. Эта учетная запись не должна быть администратором в домене или на любом из локальных компьютеров.

- Если используется SQL Server Option для Navision, Microsoft SQL Server™ работает как служба. Для SQL Server Option для Navision требуется, чтобы сервер SQL Server был способен просматривать каталог Active Directory для получения списков групп пользователей Windows в целях проверки подлинности. Поэтому служба SQL Server должна работать как учетная запись NT Authority\Network Service.

  Чтобы служба работала как учетная запись NT Authority\Network Service, выполните следующие действия:

  1. На компьютере с SQL Server найдите службу MSSQLSERVER, щелкните ее правой кнопкой мыши и в контекстном меню выберите «Свойства».
  2. В окне ***Свойства*** откройте вкладку ***Вход в систему***.
  3. На вкладке ***Вход в систему*** выберите вариант «С этой учетной записью», введите *NT Authority\NetworkService и* нажмите кнопку «ОК».

Дополнительные сведения по безопасности SQL Server см. на следующих веб-узлах:

http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

и

http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx.

- В случае использования приложения электронного бизнеса, такого как Navision Commerce Gateway, сервер Commerce Gateway Request Server должен быть правильно установлен со стандартными параметрами учетной записи для служб. Стандартный параметр учетной записи называется *CGRSUser* и обеспечивает серверу Commerce Gateway Server доступ к минимально необходимому набору других служб, включая службу *MSSQLSERVER* и *BizTalk Service BizTalk Group: BizTalkServerApplication,* и не содержит каких-либо глобальных параметров учетной записи, как, например, учетная запись *Local System*.
- Всегда используйте сложные пароли. Дополнительные сведения о сложных паролях см. в разделе «Сложные пароли».
- Используйте учетные записи Windows. Navision позволяет создавать два вида учетных записей – для подключения к базе данных и для входа в Windows. Рекомендуется использовать учетную запись для входа в Windows, так как при этом применяется проверка подлинности Windows и надлежащая политика доступа по паролю.
- Выбранный пароль должен использоваться только в одном месте. Очень часто пользователи используют один и тот же пароль в разных системах и доменах. Например, администратор, ответственный за два домена, может создать в каждом из них учетные записи администратора домена с одним паролем и даже задать один и тот же пароль для локальных администраторов на всех компьютерах домена. В данном случае проникновение в систему через одну учетную запись или компьютер поставит под угрозу весь домен.
- После установки Navision и создания или обновления базы данных следует создать учетную запись для входа в Windows и в Navision присвоить ей роль SUPER. Этот пользователь SUPER будет осуществлять администрирование базы данных, управлять безопасностью и так далее. Назначьте этой учетной записи сложный пароль. Этот пароль следует хранить в секрете. Он должен гарантировать такую же степень защиты, что и пароль системного администратора в SQL Server. Весь доступ к базе данных управляется ролью SUPER и требует самого высокого уровня защиты. Пароль пользователя SUPER должен быть известен только системным администраторам.
- Все остальные пользователи, имеющие доступ к базе данных Navision, должны работать с малыми привилегиями. Это означает, что в Navision им должны быть присвоены роли, которые дают им доступ только к функциям и возможностям, необходимым для выполнения их обязанностей в организации.
- Только те пользователи, которым поручено это делать в организации, должны иметь возможность импортировать FOB-файлы, перестраивать объекты, а также создавать архивные копии и восстанавливать базы данных.
- Регулярно выполняйте резервное копирование базы данных Navision, не забывая тестировать архивные копии, чтобы гарантировать возможность успешного восстановления из них базы данных.
- Храните архивные копии в безопасном месте, чтобы ограничить опасное воздействие на них факторов окружающей среды – огня, дыма, пыли, высокой температуры, грозовых разрядов и стихийных бедствий (например, землетрясений).

- Хотя Navision может работать под управлением нескольких версий Windows, рекомендуется использовать самые новые операционные системы с наиболее современными средствами безопасности. В настоящее время это Windows XP с пакетом обновления 2 (SP2) и Windows Server 2003.
- Для применения самых последних обновлений безопасности используйте службу Windows Update в Windows 2000, Windows XP и Windows Server 2003. Поддерживайте современное состояние безопасности всех клиентских компьютеров путем применения исправлений и пакетов обновления с помощью средства автоматического обновления Windows.
- Для поддержания связи между клиентами Navision и сервером базы данных Navision рекомендуется использовать защищенный протокол TCPS. TCPS – защищенная версия протокола TCP/IP, в котором используется интерфейс SSPI (Security Support Provider Interface) с включенным шифрованием и проверкой подлинности Kerberos. TCPS – стандартный протокол для сервера базы данных Navision.
- Заказчик должен иметь план восстановления после бедствий, который бы гарантировал быстрое возобновление работы служб. Планом восстановления должно предусматриваться решение следующих вопросов:
  - Приобретение нового/временного оборудования.
  - Восстановление резервных копий на новые системы.
  - Тестирование фактической работоспособности плана восстановления.

Физическая безопасность

Физическая безопасность абсолютно необходима, так как способов обеспечить некоторые ее аспекты с помощью программной защиты не существует. Например, в случае хищения жесткого диска похищены будут также данные, хранимые на этом накопителе. При разработке политики безопасности с заказчиком должны быть согласованы следующие вопросы физической безопасности:

- При установке в больших организациях с выделенными ИТ-подразделениями серверные помещения и места хранения программного обеспечения должны надежно закрываться.
- Эта категория компьютеров включает:
  - Сервер Microsoft SQL Server 2000
  - Файловый сервер, на котором располагаются исполняемые модули Navision
- Неуполномоченные пользователи не должны иметь доступ к компьютерам.
- Независимо от важности данных в помещении должна быть установлена сигнализация.
- Архивные копии критических данных должны храниться в отдельном помещении в несгораемых контейнерах.

Служащие

Рекомендуется по всем продуктам и функциям по возможности ограничивать административные полномочия. Если для выполнения должностных функций служащим не требуется больший доступ, обычно им предоставляется доступ к системным функциям только для чтения. Корпорация Майкрософт рекомендует следующий принцип минимального объема привилегий: пользователи должны иметь

минимальные привилегии, необходимые им для обращения к данным и выполнения своих обязанностей.

Рассерженные и бывшие служащие представляют угрозу сетевой безопасности. Обсуждая с заказчиками вопросы безопасности, предложите следующую политику относительно служащих:

- Всесторонне изучать служащего до его найма.
- Быть готовым к «мести» от рассерженных служащих и бывших служащих.
- После ухода служащего изменять все связанные с ним учетные записи Windows и пароли. Не удалять пользователей для упрощения отчетности. Не использовать одни и те же пароли в нескольких местах.
- Инструктировать пользователей быть бдительными и сообщать о подозрительном функционировании.
- Не предоставлять привилегии автоматически. Если пользователям не требуется доступ к конкретным компьютерам, аппаратным помещениям или наборам файлов, не давать им такого доступа.
- Приучать руководителей выявлять потенциальные проблемы служащих и реагировать на них.
- Убедиться, что служащие понимают их роль в поддержании безопасности сети.
- Распространить копии политик компании среди всех служащих.
- Запретить пользователям устанавливать программное обеспечение без ведома работодателя.

Администратор

Корпорация Майкрософт рекомендует, чтобы системные администраторы заказчиков постоянно устанавливали самые последние обновления безопасности. Злоумышленники очень изобретательны в использовании незначительных ошибок и объединении их для больших вторжений в сеть. Администраторы должны, во-первых, обеспечить максимальную защиту каждого отдельного компьютера и, во-вторых, постоянно добавлять обновления безопасности и использовать антивирусное программное обеспечение. В настоящем руководстве приведено много ссылок и ресурсов, которые помогут найти ценные сведения и практические рекомендации.

Одной из серьезных проблем в обеспечении безопасности сети может оказаться ее сложность. Чем сложнее сеть, тем труднее ее защищать и обновлять, если злоумышленнику удалось получить к ней доступ. Администратор должен тщательно документировать архитектуру сети, стремясь, насколько это возможно, упростить ее.

Безопасность по определению связана с управлением рисками. Так как технология не способна полностью гарантировать безопасность, для ее достижения приходится комбинировать технологии и политики. Иными словами, не стоит рассчитывать на появление продукта, который можно будет просто распаковать, установить в сети и сразу достичь этим абсолютной безопасности. Безопасность – результат единения

технологии и политики, то есть способов использования технологии, что, в конечном счете, определяет уровень безопасности сети. Корпорация Майкрософт обеспечивает технологии и средства безопасности, но только администратор и руководство организации могут определить подходящие для себя политики. Планировать безопасность следует начать еще на ранних этапах внедрения и развертывания сети. Исполнитель проекта должен уяснить, что хочет защитить заказчик и на что он готов пойти для реализации безопасности.

Наконец, планы работы в критических ситуациях должны быть разработаны до того, как такие ситуации наступят. Тщательное планирование и надежные технологии обеспечат заказчикам высокий уровень безопасности.

Дополнительные сведения по безопасности общего плана см. в статье «Десять непреложных правил администрирования безопасности» (на английском языке) по адресу:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

а также в статьях по управлению безопасностью на веб-узле:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx.

Организация защиты серверных операционных систем

Хотя многие мелкие заказчики не имеют серверных операционных систем, важно располагать знаниями и накопить практический опыт в области безопасности, чтобы предложить свои рекомендации крупным клиентам с более сложными сетевыми средами. Следует также отметить, что многие из политик и практических действий, описанных в настоящем документе, могут быть легко применены у заказчиков, которые эксплуатируют только клиентские операционные системы.

Основные положения этого раздела касаются как Microsoft Windows 2000 Server, так и Microsoft Windows Server 2003, хотя эти сведения были взяты в основном из справочной системы Windows Server 2003. Операционная система Windows Server 2003 обеспечивает набор надежных мер безопасности. В справочной системе Windows Server 2003 содержится полная информация относительно всех средств и процедур безопасности.

Дополнительные сведения по Windows 2000 Server см. на веб-узле Центра безопасности Windows 2000 по адресу:
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

а также прочитайте *Руководство по повышению безопасности Windows 2000* по адресу:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Дополнительные сведения по Windows Server 2003 см. в *Руководстве по безопасности Windows Server 2003 Security Guide* по адресу http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

Основными особенностями модели безопасности сервера Windows являются проверка подлинности, управление доступом и единая регистрация:

- Проверка подлинности – процесс проверки системой правильности сведений о подлинности пользователя путем анализа данных, введенных им при входе в систему. Имя пользователя и пароль сравниваются с утвержденным списком. При обнаружении совпадения система авторизации разрешает пользователю доступ к области, указанной в списке разрешений для данного пользователя.
- Система управления доступом ограничивает доступ пользователей к данным или вычислительным ресурсам в соответствии с подлинностью пользователей и их принадлежностью к различным группам. Управление доступом обычно используется системными администраторами для управления доступом пользователей к таким сетевым ресурсам, как серверы, каталоги и файлы. Обычно это реализуется путем предоставления пользователям и группам разрешений на обращение к определенным объектам.
- Единая регистрация позволяет пользователю, однажды войдя в домен Windows при помощи единственного пароля, регистрироваться затем на любом компьютере в домене Windows. Единая регистрация позволяет администраторам внедрить парольную проверку подлинности по всей сети Windows, обеспечив при этом простой доступ конечным пользователям.

В следующих разделах эти три главные особенности описываются более подробно.

Проверка подлинности

Проверка подлинности, фундаментальная составляющая системной безопасности, используется для подтверждения подлинности любого пользователя, пытающегося войти в домен или обратиться к сетевым ресурсам. Слабое место в большинстве систем проверки подлинности – пароль пользователя.

Пароли обеспечивают первую линию обороны против неправомочного доступа к домену и локальным компьютерам. Заказчикам следует рекомендовать следующие правила использования паролей:

- Всегда использовать сложные пароли.
- Записав пароли на бумаге, спрятать этот лист в надежном месте и уничтожить его, когда в нем отпадет необходимость.
- Никогда и никому не сообщать пароль.
- Использовать разные пароли для разных учетных записей пользователей.
- Регулярно менять пароли.
- Надежно прячьте пароли, если они хранятся на компьютерах.

Сложные пароли

Значение паролей в системе безопасности сети организации часто недооценивают и даже игнорируют. Как уже упоминалось ранее, пароли обеспечивают первую линию обороны против неправомочного доступа к сети. Поэтому следует настоятельно рекомендовать заказчикам, чтобы они требовали от своих служащих использовать сложные пароли.

Средства вскрытия паролей, однако, продолжают совершенствоваться, и для этих целей сегодня используются компьютеры, гораздо более мощные, чем ранее. При наличии достаточного количества времени программа для автоматического вскрытия паролей может узнать любой пароль. Однако сложные пароли взломать намного труднее, чем простые пароли.

Рекомендации по созданию сложных паролей, которые можно легко запомнить, см. в статьях

http://www.microsoft.com/athome/security/privacy/password.mspx

и

http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp.

Определение политики паролей

Помогая заказчику в разработке политики паролей, важно убедить его в том, что политика должна требовать использования сложных паролей для всех учетных записей пользователей. Для большинства систем достаточно следовать рекомендациям Руководства по безопасности Windows Server 2003:

- Установить параметр **Требовать неповторяемости паролей**, чтобы хранить несколько предыдущих версий паролей. Если этот параметр политики установлен, пользователи не смогут использовать пароль после истечения срока его действия.

  Рекомендуемое значение: 24

- Установить параметр **Максимальный срок действия пароля** в соответствии с требованиями клиентской среды.

  Рекомендуемое значение: от 42 (умолчание) до 90.

- Установить параметр **Минимальный срок действия пароля**, в течение которого пароли не могут быть изменены. Этот параметр политики используется совместно с параметром **Требовать неповторяемости паролей**. Если задан минимальный срок действия пароля, пользователи не смогут несколько раз подряд изменить пароли, чтобы обойти действие параметра **Требовать неповторяемости паролей и** вернуться к исходным паролям. Чтобы изменить свои пароли, пользователи должны ожидать заданное число дней.

  Рекомендуемое значение: 2.

- Установить параметр **Минимальная длина пароля**, чтобы пароли содержали не меньше заданного числа символов. Длинные пароли, из семи и больше символов, обычно труднее вскрыть, чем короткие. Если задан этот параметр,

пользователи не могут использовать пустые пароли и должны создать пароли длиной не менее заданного числа символов.

Рекомендуемое значение: 8.

- Установить параметр политики **Пароль должен соответствовать требованиям сложности**. Если установлен этот параметр, система проверяет все новые пароли на соответствие основным требованиям для сложного пароля. Этот параметр гарантирует, что пароль содержит, по крайней мере, три символа из четырех категорий (верхний регистр, нижний регистр, цифры и символы, не являющиеся алфавитно-цифровыми) и что он не содержит какую-либо часть имени учетной записи пользователя или его имя или фамилию.

  Примечание.
  Пароли, которые удовлетворяют этим требованиям, не обязательно являются очень сложными. Например, пароль «Password1» отвечает этим требованиям.

  Рекомендуемое значение: Да.

- Полный перечень этих требований см. в разделе «Пароль должен соответствовать требованиям сложности» справочной системы сервера Windows.

- Хранить пароли с помощью обратимого шифрования. Обратимое шифрование применяется в системах, где в приложениях используется доступ к открытым паролям. В большинстве реализаций это не требуется.

  Рекомендуемое значение: Нет.

Дополнительные сведения см. в Руководстве по безопасности Windows Server 2003:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx.

Определение политики блокировки учетных записей

Политику блокировки учетных записей следует продумать очень обстоятельно. Политика блокировки учетных записей никогда не должна применяться в малом бизнесе, так как в этих средах будет высока вероятность блокировки уполномоченных пользователей, что может привести к большим потерям в деловом процессе заказчика.

Если заказчик все же решит применить политику блокировки учетных записей, следует задать достаточно высокое значение параметра политики **Пороговое значение блокировки учетных записей**, чтобы уполномоченные пользователи не блокировали свои учетные записи просто потому, что несколько раз неудачно ввели пароль.

Дополнительные сведения о политике блокировки учетных записей см. в разделе «Общие сведения о политике блокировки учетных записей» электронной справки сервера Windows.

Дополнительные сведения о применении и изменении политики блокировки учетных записей см. в разделе «Применение и изменение политики блокировки учетных записей» электронной справки сервера Windows.

Управление доступом

Сеть Windows и ее ресурсы (в том числе и Navision) могут быть защищены путем распределения полномочий среди пользователей, групп пользователей и компьютеров сети. Чтобы защитить компьютер или несколько компьютеров, следует предоставить определенные права пользователям или группам. Чтобы защитить объект (например, файл или папку), следует назначить разрешения, которые позволят пользователям или группам выполнять с этим объектом определенные действия. Система управления доступом формируется из следующих ключевых составляющих:

- Разрешения
- Принадлежность объектов
- Наследование разрешений
- Права пользователей
- Аудит объектов

Разрешения

Разрешения определяют тип предоставленного пользователю или группе доступа к объекту или объектному свойству, например, файлам, папкам и объектам системного реестра. Разрешения применяются к любым защищенным объектам, таким как файлы или объекты реестра. Разрешения могут быть предоставлены любому пользователю, группе или компьютеру. Рекомендуется назначать разрешения группам.

Принадлежность объектов

При создании объекта ему назначается владелец. В Windows 2000 Server по умолчанию владельцем объекта является его создатель. В Windows Server 2003 для объектов, создаваемых членами группы «Администраторы», это правило изменено.

Когда в Windows Server 2003 член группы «Администраторы» создает объект, его владельцем становится группа «Администраторы», но не отдельная учетная запись, которая создала объект. Этот порядок можно изменить в оснастке «Локальные параметры безопасности» консоли Microsoft Management Console (MMC) установкой параметра **Системные объекты: Владелец по умолчанию для объектов, созданных членами группы «Администраторы»**. Независимо от разрешений, установленных для объекта, его владелец всегда может изменить эти разрешения.

Дополнительные сведения см. в разделе «Принадлежность объектов» электронной справки сервера Windows.

Наследование разрешений

Наследование позволяет администраторам легко присваивать разрешения и управлять ими. Эта функция обусловливает автоматическое наследование объектами в пределах контейнера всех разрешений этого контейнера, которые могут быть унаследованы. Например, при создании файлов в папке они наследуют разрешения данной папки. Наследуются только разрешения, отмеченные как предназначенные для наследования.

Права пользователей

Права пользователей обеспечивают определенные привилегии и права входа в систему для пользователей и групп в данной вычислительной среде.

Сведения о правах пользователей см. в разделе «Права пользователей» электронной справки сервера Windows.

Аудит объектов

Аудит дает возможность контролировать доступ пользователей к объектам. Собранные службой аудита сведения о связанных с безопасностью событиях затем можно просмотреть в журнале безопасности в окне просмотра событий.

Дополнительные сведения см. в разделе «Аудит» электронной справки сервера Windows.

Практические рекомендации по управлению доступом

- Присваивайте разрешения группам, а не пользователям. Так как сопровождение учетных записей отдельных пользователей неэффективно, назначать разрешения на уровне пользователей следует только в виде исключения.
- В определенных особых случаях используйте разрешения типа «Запрет». Например, запрет разрешений можно использовать для исключения некоторого подмножества пользователей из группы, которой назначены разрешения.
- Никогда не запрещайте доступ к объекту для группы «Все». Запрет разрешения на доступ к объекту коснется также администраторов, которые входят в состав группы «Все». Лучшим вариантом в данном случае будет вообще удалить группу «Все», обеспечив при этом разрешения на доступ к этому объекту другим пользователям, группам или компьютерам. Помните, что если не определено никаких разрешений, то доступ невозможен.
- Назначайте разрешения по объектам как можно выше в дереве объектной иерархии и затем применяйте наследование, чтобы распространить параметры безопасности вниз по дереву. Параметры управления доступом можно быстро и эффективно применить ко всем потомкам или поддеревьям родительского объекта. Это позволит получить самый большой эффект с наименьшими усилиями. Задаваемые параметры разрешений должны отвечать потребностям большинства пользователей, групп и компьютеров.

- Явно заданные разрешения иногда могут переопределять унаследованные разрешения. Унаследованный запрет разрешения не предотвращает доступ к объекту, если для объекта имеется явное разрешение на доступ. Явные разрешения имеют приоритет над унаследованными разрешениям – даже унаследованными разрешениями «Запрет».
- Следуйте рекомендациям относительно разрешений по объектам Active Directory®.

Дополнительные сведения см. в разделе «Рекомендации по назначению разрешений объектам Active Directory» электронной справки Windows Server 2003.

Внешний брандмауэр безопасности

Брандмауэр – это аппаратное устройство или программное обеспечение, которое предотвращает поступление пакетов данных в сеть или отправку их за пределы сети. Управление потоком трафика осуществляется открытием или закрытием портов брандмауэра для определенных пакетов данных. В каждом пакете данных брандмауэр анализирует несколько разделов информации: протокол, под которым доставлен пакет, адресат или отправитель пакета, тип содержимого пакета и номер порта, на который он направлен. Если настройкой брандмауэра предусмотрено принятие определенного протокола через определенный порт, соответствующий пакет пропускается. С сервером Microsoft Windows Small Business Server 2003 Premium Edition в качестве брандмауэра поставляется сервер Microsoft Internet Security and Acceleration (ISA) Server 2000. Сервер Small Business Server Standard Edition также содержит брандмауэр.

ISA Server 2004

Сервер Internet Security and Acceleration (ISA) Server 2000 безопасно пересылает запросы и ответы между Интернетом и клиентскими компьютерами внутренней сети.

Для клиентов локальной сети сервер ISA действует как защищенный шлюз в Интернет. Компьютер с сервером ISA работает незаметно для других объектов на магистрали связи. Пользователь Интернета не должен чувствовать присутствие сервера брандмауэра, за исключением случаев обращения к службе или перехода к веб-узлу, где компьютер с сервером ISA отвергает доступ. Сервер в Интернете, к которому выполняется обращение, интерпретирует запросы компьютера с сервером ISA, как если бы запросы исходили из приложения-клиента.

При выборе фильтрования фрагментов по протоколу Интернета (IP) фильтрование фрагментов пакета фактически выполняют службы веб-прокси и брандмауэра. При фильтровании фрагментов пакета все фрагментированные IP-пакеты удаляются. Широко известным способом маскировки сетевых атак является отправка фрагментированных

пакетов со сборкой их «на месте» таким образом, что в целом виде они могут представлять опасность для системы.

Сервер ISA содержит механизм обнаружения вторжений, который определяет время начала нападения на сеть и в случае нападения выполняет набор конфигурируемых действий (сигналов).

Если на компьютере с серверном ISA установлены службы Internet Information Services (IIS), их необходимо конфигурировать так, чтобы они не использовали порты, задействованные сервером ISA для исходящих запросов Интернета (по умолчанию – порт 8080) и для входящих запросов Интернета (по умолчанию – порт 80). Например, можно настроить в IIS контроль порта 81 и затем конфигурировать компьютер ISA так, чтобы он направлял входящие запросы из Интернета на порт 81 локального компьютера с IIS.

При возникновении конфликта между портами, используемыми сервером ISA и IIS, программа настройки останавливает службу публикации IIS. После этого можно изменить порт, контролируемый IIS, и перезапустить службу публикации IIS.

Политики сервера ISA

Имеется возможность определить политику сервера ISA, которая будет управлять входящим и исходящим доступом. Доступность веб-узлов и данных определяется правилами для узлов и содержимого. Правила для протоколов указывают, доступен ли конкретный протокол для входящей и исходящей связи.

Могут быть созданы правила для узлов и содержимого, правила для протоколов, веб-публикации и фильтрования IP-пакетов. Эти политики определяют порядок поддержания связи клиентов сервера ISA с Интернетом и тип разрешенной связи.

Защита от вирусов

Компьютерный вирус – исполняемый файл, задачи которого включают в себя следующее: саморазмножаться, стирать или разрушать файлы данных и программ, избегая при этом обнаружения. Вирусы часто переписывают и настраивают под разные среды, чтобы их нельзя было обнаружить. Чаще всего вирусы рассылаются во вложениях почтовых сообщений. Чтобы антивирусные программы могли находить новые и измененные вирусы, они должны непрерывно обновляться. Вирусы – главный способ компьютерного вандализма.

Антивирусное программное обеспечение предназначено специально для обнаружения и предотвращения действия вирусных программ. Так как непрерывно создаются все новые вирусные программы, многие изготовители антивирусных продуктов предлагают периодические обновления своего программного обеспечения.

Корпорация Майкрософт настоятельно рекомендует использовать антивирусное программное обеспечение в клиентской среде.

Вирусные программы обычно устанавливаются в каждом из следующих трех мест: рабочие станции пользователей, серверы и сети, куда поступает (и, в некоторых случаях, откуда отправляется) электронная почта организации.

Типы вирусов

Существует три основных типа вирусов, которые инфицируют компьютерные системы: загрузочные вирусы, файловые вирусы и троянские программы.

Загрузочные вирусы

При включении компьютера он перед загрузкой операционной системы и других файлов запуска читает загрузочный сектор жесткого диска. Загрузочный вирус заменяет информацию в загрузочных секторах жесткого диска собственным программным кодом. Если загрузочный сектор компьютера заражен вирусом, код вируса читается в память раньше других данных. Находясь в памяти, вирус может тиражироваться на любые другие диски, используемые на инфицированном компьютере.

Файловые вирусы

Наиболее часто встречающийся тип вируса – вирус, заражающий файлы, – присоединяет себя к исполняемому программному файлу, добавляя к исполняемому файлу собственный код. Вирусный код обычно добавляется таким образом, чтобы избежать обнаружения. При запуске инфицированного файла вирус может присоединяться к другим исполняемым файлам. Этим типом вируса обычно заражаются файлы с расширением .com, .exe и .sys.

Некоторые файловые вирусы предназначены для определенных программ. Мишенью вирусов часто становятся такие типы программ, как оверлейные файлы (.ovl) и файлы динамически компонуемых библиотек (.dll). Хотя эти файлы нельзя непосредственно запустить, их вызывают исполняемые файлы. Вирус передается в момент вызова файла.

Повреждение данных происходит, когда вызывается сам вирус. Вирус может быть вызван при запуске инфицированного файла или при наступлении определенных условий среды (например, определенной системной даты).

Троянские программы

Программа типа «троянский конь» сама по себе не является вирусом. Ключевое отличие троянской программы от вируса в том, что она не размножается, а только уничтожает данные на жестком диске. Троянская программа маскируется под нормальную программу широкого применения, как, например, игра или служебная программа. Тем не менее, будучи запущена, она может уничтожить или повредить данные.

Практические рекомендации по защите от вирусов

Распространение макровирусов можно предотвратить. Вот несколько советов по предотвращению заражения вирусами, с которыми следует ознакомить заказчиков:

- Установите программу вирусной защиты, которая, прежде чем передавать входящие сообщения из Интернета на маршрутизатор, проверяла бы их на наличие вирусов. Этим будет гарантироваться проверка электронной почты на известные вирусы.
- Обращайте внимание на источник полученных документов. Не открывайте документы, пришедшие от неизвестных отправителей.
- Свяжитесь с лицом, создавшим документ. В случае сомнения в безопасности документа следует связаться с его автором.
- Используйте защиту от макровирусов в Microsoft Office. Офисные приложения информируют пользователя, если документ содержит макросы. Эта функция позволяет пользователю разрешить или отключить макросы при открытии документа.
- Используйте антивирусное программное обеспечение для обнаружения и удаления макровирусов. Антивирусные программы могут находить и часто удалять макровирусы из документов. Корпорация Майкрософт рекомендует использовать антивирусное программное обеспечения, сертифицированное Международной Ассоциацией Компьютерной Безопасности (ICSA).

Для получения дополнительных сведений относительно вирусов и безопасности компьютеров посетите следующие веб-узлы корпорации Майкрософт по безопасности:

- Узел Microsoft по безопасности http://www.microsoft.com/security/default.asp.
- Документация по безопасности на Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx.

Стратегии безопасности сетей

Так как для разработки и развертывания межсетевой IP-среды необходим учет требований как частных, так и открытых сетей, брандмауэр стал ключевым компонентом обеспечения целостности сети. Брандмауэр не является каким-то единичным компонентом. Национальная Ассоциация Компьютерной Безопасности (NCSA) определяет брандмауэр как «систему или комбинацию систем, которая устанавливает границу между двумя или несколькими сетями». Хотя

используются разные термины, эту границу часто называют периферийной сетью. Периферийная сеть защищает интрасеть или корпоративную локальную сеть (ЛВС) от внешнего вторжения, управляя доступом из Интернета и других больших сетей.

На следующем рисунке показана периферийная сеть, огражденная брандмауэрами и расположенная между частной сетью и Интернетом для защиты частной сети:

Базовая периферийная сеть

В разных организациях к применению брандмауэров для обеспечения безопасности могут подходить по-разному. Фильтрование IP-пакетов обеспечивает слабую защиту, громоздко в управлении и легко преодолевается. Шлюзы приложений более защищены, чем фильтры пакетов и проще в управлении, так как они относятся только к нескольким определенным приложениям, например, к конкретной системе электронной почты. Шлюзы каналов связи наиболее эффективны, когда операции пользователя сетевого приложения имеют большее значение, чем данные, передаваемые этим приложением. Прокси-сервер – комплексное средство безопасности, которое включает шлюз приложений, безопасный доступ для анонимных пользователей и другие службы. Вот некоторые сведения об этих компонентах:

- **Фильтрование IP-пакетов**
  Фильтрование IP-пакетов – самая ранняя реализация технологии брандмауэров. В заголовках пакетов анализируются адреса источника и назначения, номера портов протокола управления передачей (TCP) и протокола пользовательских датаграмм (UDP) и прочие сведения. Фильтрование IP-пакетов – ограниченная технология, которая работает лучше всего в средах чистой безопасности, где, например, всему, что находится вне периферийной сети, не доверяют, а всему, что внутри – доверяют. За последнее время различные поставщики улучшили методы фильтрования пакетов, добавив к ядру фильтрования пакетов интеллектуальные средства принятия решений и создав, таким образом, новую форму фильтрования пакетов – *анализ протокола, изменяющего параметры своего состояния*. Фильтрование пакетов можно настроить таким образом, что будут либо пропускаться определенные типы пакетов и отвергаться другие, либо будут отвергаться определенные типы пакетов и пропускаться все остальные.
- **Шлюзы приложений**
  Шлюзы приложений используются, когда самое большое значение имеют фактические данные приложения. То, что эти компоненты специфичны для приложения, является как их преимуществом, так и их слабостью, поскольку они трудно адаптируются к изменениям технологий.

- **Шлюзы каналов связи**
  Шлюзы каналов связи представляют собой туннели, созданные в брандмауэре для соединения определенных процессов или систем на одной стороне с определенными процессами или системами на другой. Шлюзы каналов связи лучше всего подходят для ситуаций, когда пользователь, использующий приложение, представляет потенциально больший риск, чем данные, которые передает приложение. Шлюз канала связи отличается от фильтрования пакета возможностью подключения по вспомогательному каналу прикладной схемы, которая может предоставлять дополнительные данные.
- **Прокси-серверы**
  Прокси-серверы – комплексные средства защиты, включающие функциональные возможности брандмауэра и шлюза приложения, которые управляют трафиком Интернета в ЛВС и из нее. Прокси-серверы также выполняют кэширование документов и управление доступом. Прокси-сервер может повышать производительность, кэшируя и непосредственно предоставляя часто используемые данные, например, популярные веб-страницы. Прокси-сервер может также фильтровать и отвергать запросы, которые владелец не считает нужными, такие как запросы неправомочного доступа к своим файлам.

Рекомендуйте заказчику меры защиты с помощью брандмауэра, объяснив их преимущества. Периферийную сеть следует располагать в точке сетевой топологии, где весь трафик снаружи корпоративной сети проходит через периметр, контролируемый внешним брандмауэром. Параметры управления доступом в брандмауэре можно настраивать с учетом потребностей заказчика, в том числе можно вести журнал брандмауэра с записью всех попыток неправомочного доступа.

Чтобы сократить число портов, которые требуется открыть на внутреннем брандмауэре, можно использовать брандмауэр прикладного уровня, такой как ISA Server 2000.

Дополнительные сведения о TCP/IP см. в статье «Разработка сетей TCP/IP» на веб-узле:
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp.

Беспроводные сети

По умолчанию настройка беспроводных сетей обычно допускает подслушивание беспроводных сигналов. Стандартные настройки некоторых беспроводных устройств, простая доступность беспроводных сетей и существующие методы шифрования делают беспроводные сети уязвимыми перед злонамеренным посторонним доступом. Существуют параметры конфигурации и средства, которые могут защитить от подслушивания, но они не делают ничего для защиты компьютера от хакеров и вирусов, которые могут проникнуть через подключение к Интернету. Поэтому чрезвычайно важно применить брандмауэр для защиты компьютеров от злоумышленников в Интернете.

Дополнительные сведения о защите беспроводной сети см. в статье «Как сделать беспроводную домашнюю сеть 802.11b более безопасной» на веб-узле:
http://support.microsoft.com/default.aspx?scid=kb;en-us;309369.

Примеры конфигурации безопасности сетей

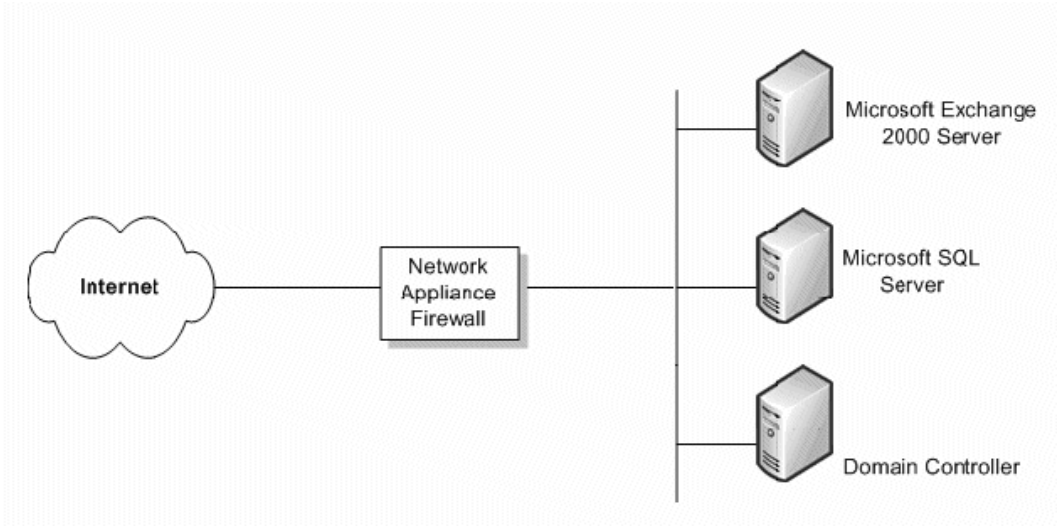
Уровень сетевой защиты, который требуется организации заказчика, зависит от нескольких факторов. Решение обычно сводится к компромиссу между бюджетными возможностями и необходимостью обеспечить безопасность данных. Очень сложную структуру безопасности, которая обеспечит самый высокий уровень сетевой защиты, можно создать и для небольших организаций, но заказчику такой уровень безопасности может оказаться просто не по карману. В этом разделе рассматриваются четыре сценария, и по каждому даются рекомендации, которые обеспечат гибкую настройку уровней безопасности.

Без брандмауэра

Если у заказчика имеется подключение к Интернету, но отсутствует брандмауэр, должны быть реализованы некоторые меры сетевой защиты. Существуют простые сетевые устройства-брандмауэры, которые обеспечивают достаточный уровень безопасности, чтобы противостоять наиболее часто встречающимся атакам хакеров.

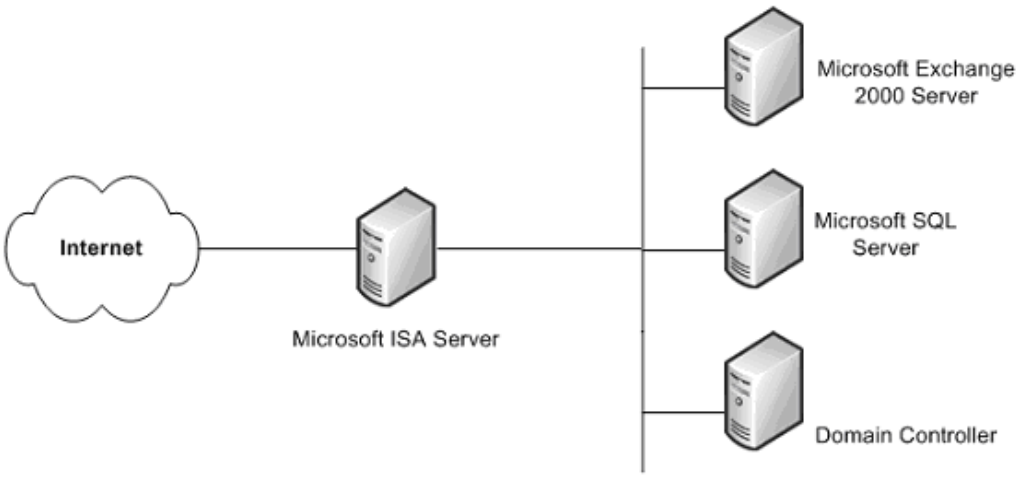
Один простой брандмауэр

Минимально допустимая защита – единственный брандмауэр между Интернетом и данными заказчика. Этот брандмауэр не сможет обеспечить какой-либо уровень комплексной защиты, его нельзя рассматривать как достаточно безопасный. Но все же это лучше, чем ничего.



Простой брандмауэр

Хорошо, когда бюджет заказчика позволяет реализовать более безопасное решение, которое сможет защитить его корпоративные данные. Одно из таких решений – сервер ISA. Несколько большая стоимость этого дополнительного сервера обеспечит намного лучшую безопасность, чем средний стандартный брандмауэр, который обычно выполняет только трансляцию сетевых адресов (NAT) и фильтрование IP-пакетов.



Брандмауэр с сервером ISA

Это решение с одним брандмауэром более безопасно, чем устройство-брандмауэр входного уровня, и поддерживает специальные службы безопасности Windows.

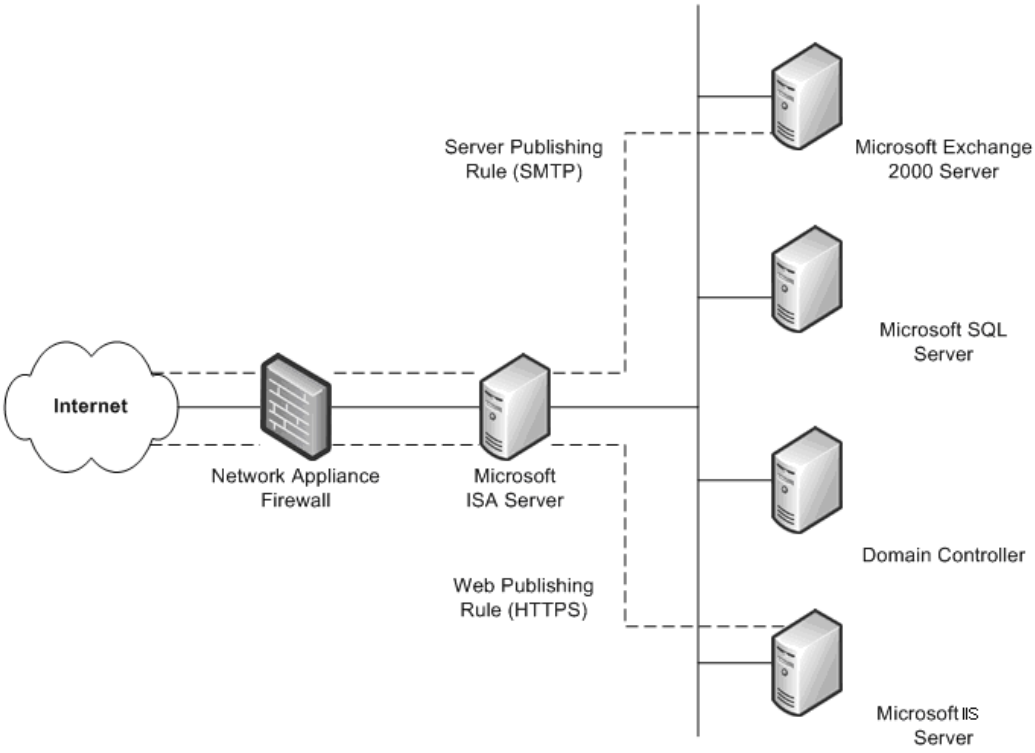
Один существующий брандмауэр

Если у заказчика уже есть брандмауэр, который отделяет его интрасеть от Интернета, полезно установить дополнительный брандмауэр, который обеспечит несколько способов настройки связи внутренних ресурсов с Интернетом.

Один из таких методов – веб-публикация. В этой конфигурации сервер ISA устанавливается перед веб-сервером организации, который обеспечивает доступ пользователям из Интернета. Получив входящий запрос из Интернета, сервер ISA может предоставлять ресурсы веб-сервера внешнему миру, выполняя запросы клиентов о получении веб-контента из своего кэша. Сервер ISA передает запрос веб-серверу только в том случае, если запросы нельзя обслужить из кэша.

Другой метод – серверная публикация. Сервер ISA разрешает публикацию в Интернете внутренним серверам, не ставя под угрозу безопасность внутренней сети. Имеется возможность настроить правила веб-публикации и серверной публикации, которые будут определять, какие запросы должны отправляться серверу локальной

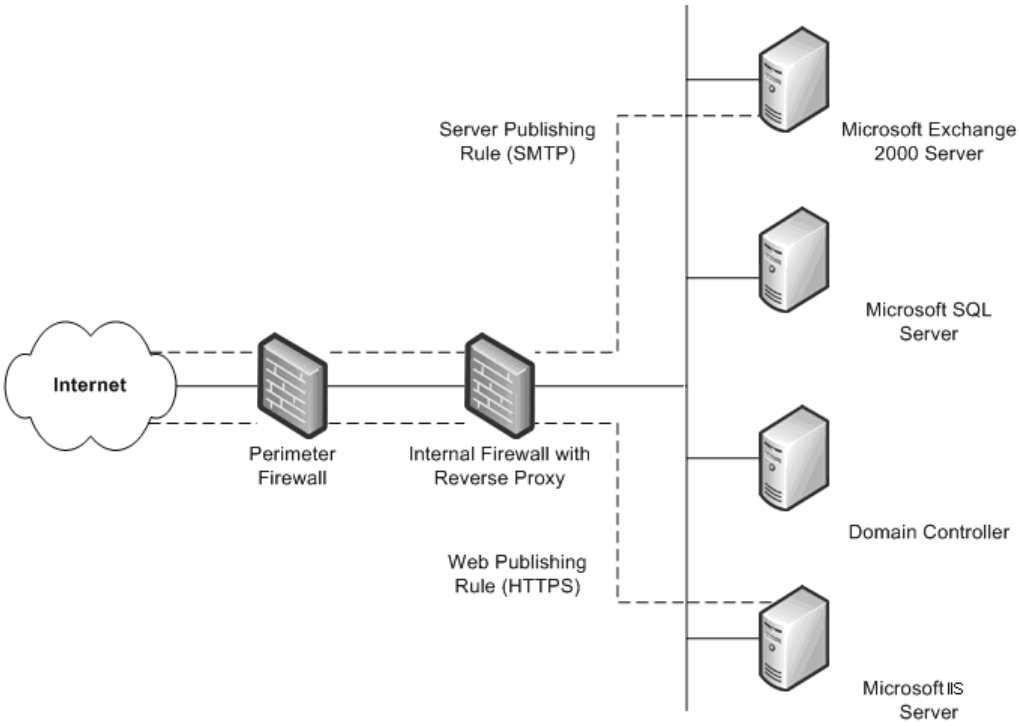
сети, обеспечивая тем самым дополнительный слой защиты внутренних серверов.



Существующий брандмауэр с добавленным сервером ISA

Два существующих брандмауэра

В четвертом сценарии организация имеет два брандмауэра, вместо полноценной периферийной сети (DMZ). Один или несколько этих серверов обеспечивает службы реверсивного представительства, чтобы клиенты в Интернете не могли обращаться непосредственно к серверам интрасети. Один из брандмауэров (в идеальном случае это внутренний брандмауэр) перехватывает сетевые запросы доступа к внутренним серверам, анализирует эти пакеты и затем пересылает их от имени удаленного компьютера Интернета.



Два существующих брандмауэра

Этот сценарий подобен предыдущему сценарию, но с добавлением второго брандмауэра. Единственное отличие в том, что внутренний брандмауэр, который поддерживает службы реверсивного представительства, не является сервером ISA. В этом сценарии необходимо тесное сотрудничество с менеджерами каждого брандмауэра при определении правил серверной публикации, которые бы полностью соответствовали политике безопасности.

Управление обновлениями безопасности

Операционные системы и приложения бывают очень сложными. Они могут состоять из миллионов строк программного кода, написанных многими программистами. Чрезвычайно важно, чтобы программы работали надежно, не ставя под угрозу безопасность или стабильность информационной среды. Чтобы сократить до минимума вероятность проблем, перед выпуском программы тщательно проверяются. Однако злоумышленники непрерывно совершенствуют способы нахождения

слабых мест в программном обеспечении, поэтому предупредить все будущие атаки невозможно.

Во многих организациях управление исправлениями составляет часть их общей стратегии управления изменениями и конфигурацией. Однако какими бы ни были характер и размер организации, жизненно важно иметь хорошую стратегию управления исправлениями, даже если организация еще не имеет эффективной стратегии управления изменениями и конфигурацией. Огромное большинство нападений на компьютерные системы злоумышленникам удается против систем, в которых не были установлены исправления безопасности.

Исправления безопасности добавляют большинству организаций лишние заботы. Выявив дефект в программном обеспечении, злоумышленники обычно распространяют эту информацию среди всего хакерского сообщества. Корпорация Майкрософт, если слабое место обнаружено в ее программном обеспечении, старается выпустить исправление безопасности как можно скорее. Тем не менее, пока исправление не развернуто в системе, безопасность, от которой зависит и на которую рассчитывает заказчик, может быть серьезно подорвана.

Исполнитель проекта должен гарантировать заказчику, что во всех местах его среды Navision будут установленные самые последние исправления безопасности. Убедитесь, что заказчик использует одну из технологий, которые сделала доступными корпорация Майкрософт. В их числе следующие:

- **Служба уведомлений Microsoft Security Notification Service**
  Служба Security Notification Service – это список адресов электронной почты, по которому рассылаются уведомления о доступности новых обновлений. Эти уведомления представляют собой важную часть превентивной стратегии безопасности. Они доступны также на веб-узле TechNet Product Security Notification: http://www.microsoft.com/technet/security/bulletin/notify.mspx.
- **Автоматические обновления Microsoft Automatic Updates**
  Windows может автоматически применять обновления безопасности к компьютерам.
- **Поисковое средство Microsoft Security Bulletin Search Tool**
  Средство поиска бюллетеней по безопасности доступно на веб-узле службы бюллетеней по безопасности на TechNet: http://www.microsoft.com/technet/security/current.aspx. Заказчик может определить потребность в обновлениях в соответствии со своей операционной системой, приложениями и установленными в данный момент пакетами обновления.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Это графическое средство анализа защищенности системы доступно на веб-узле Microsoft Baseline Security Analyzer: http://www.microsoft.com/technet/security/tools/mbsahome.mspx. Это средство сравнивает текущее состояние компьютера со списком обновлений, поддерживаемых корпорацией Майкрософт. MBSA также выполняет некоторые базовые проверки безопасности – сложность и параметры сроков действия паролей, политика гостевой учетной записи и ряд других областей. MBSA также

ищет уязвимость в Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 и Exchange Server 2003.

- **Microsoft Software Update Services (SUS)**
  Прежде известное как Windows Update Corporate Edition, это средство позволяет предприятиям применять на локальных компьютерах все критические обновления и пакеты безопасности (SRP), общедоступные на веб-узле Windows Update. Это средство работает с новым выпуском клиентов автоматического обновления (AU), создавая основу для мощной стратегии автоматической загрузки и установки. Новый набор клиентов AU включает клиента для операционных систем Windows 2000 и Windows Server 2003 и обеспечивает возможность автоматической установки загруженных обновлений. Дополнительные сведения о Microsoft SUS см. на веб-узле: http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp.
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  Пакет SMS Software Update Services Feature Pack содержит ряд инструментальных средств, предназначенных для облегчения процесса выпуска обновлений программных продуктов на предприятии. Пакет включает следующие средства: Security Update Inventory Tool, Microsoft Office Inventory Tool for Updates, Distribute Software Updates Wizard и SMS Web Reporting Tool with Web Reports Add-in for Software Updates. Дополнительные сведения по каждому средству см. на веб-узле: http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/.

Сообщите заказчикам об этих средствах и рекомендуйте их использовать. Для поддержания стабильности среды очень важно, чтобы вопросы безопасности решались как можно быстрее.

Параметры безопасности SQL Server 2000

Так как Navision работает также с SQL Server 2000, важно предпринять меры по повышению безопасности установки SQL Server 2000 заказчика. Следующие шаги помогут усилить безопасность SQL Server:

- Убедитесь, что установлены самые последние пакеты обновления и исправления операционной системы и SQL Server 2000. Последние сведения см. на веб-узле Microsoft Security http://www.microsoft.com/security/default.asp.
- Для обеспечения безопасности уровня файловой системы все данные и системные файлы SQL Server 2000 должны быть установлены в разделах NTFS. Файлы должны быть доступны только пользователям административного или системного уровня через разрешения NTFS. Это предохранит файлы от обращений пользователей, когда служба MSSQLSERVER не работает.
- Для службы SQL Server 2000 (MSSQLSERVER) используйте учетную запись домена с низкими привилегиями, такую как NT Authority\Network Service или LocalSystem (рекомендуется). Эта учетная запись должна иметь минимальные права в домене и должна помочь локализовать (но не остановить) нападение на сервер в случае нарушения безопасности. Иными словами, эта учетная запись должна иметь в домене только локальные разрешения пользовательского уровня. Если для работы служб SQL Server 2000 используется учетная запись «Администратор Домена», нарушение безопасности сервера приведет к нарушению безопасности всего домена. Изменить эту настройку можно с помощью SQL Server Enterprise Manager. Списки контроля доступа (ACL) к файлам и системному реестру и права пользователя будут изменены автоматически.

- Большинство выпусков SQL Server 2000 устанавливается с двумя стандартными базами данных – «Борей» и «Издатели». Обе базы данных – примерные базы данных, используемые для тестирования, обучения и получения общих примеров. Их не следует развертывать в производственной системе. Наличие этих баз данных в системе может поощрить злоумышленника попытаться использовать стандартные настройки и конфигурацию. Если базы данных «Борей» и «Издатели» установлены на компьютере SQL Server 2000 в производственной системе, их следует удалить.
- Аудит системы SQL Server 2000 по умолчанию отключен, поэтому никакие условия не контролируются. Это усложняет обнаружение вторжения и помогает злоумышленникам скрыть свою активность. Как минимум, необходимо включить аудит неудачных попыток входа в систему.

Самые последние сведения по безопасности SQL Server 2000 см. на веб-узле:
http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp.

Microsoft Business Solutions

Microsoft Business Solutions, отделение корпорации Майкрософт, обеспечивает широкий диапазон интегрированных, полнофункциональных бизнес-приложений и служб, предназначенных для более тесного соединения малого и среднего бизнеса и крупных корпораций с заказчиками, служащими, партнерами и поставщиками. Приложения Microsoft Business Solutions оптимизируют стратегические бизнес-процессы управления финансами, аналитики, управления трудовыми ресурсами, руководства проектами, управления взаимоотношениями с клиентами, управления выездным сервисом, управления сетью поставок, электронной коммерции, производства и управления розничной торговлей. Приложения призваны обеспечить понимание принципов достижения успеха в бизнесе. Дополнительные сведения о Microsoft Business Solutions можно найти на веб-узле: http://www.microsoft.com/BusinessSolutions/.