УДК 004

Кириллов Д.С.,
Студент магистратуры,
Казанский национальный исследовательский технологический университет
Россия, г. Казань
Молостов Д.Д.,
Студент магистратуры,
Казанский национальный исследовательский технологический университет
Россия, г. Казань
Мертинс Г.Р.,
Студент магистратуры,
Казанский национальный исследовательский технологический университет
Россия, г. Казань
Научный руководитель: Старыгина С.Д.,
кандидат педагогических наук, доцент
Казанский национальный исследовательский технологический университет
Россия, г. Казань

ТЕСТИРОВАНИЕ И ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СРЕДЫ SQL SERVER

Аннотация: *В статье объясняются различные ключевые положения и аспекты в области тестирования и обеспечения безопасности среды SQL Server. Безопасность является очень важной областью для любой среды баз данных, поэтому необходимо надлежащим образом планировать,*

развертывать и проверять меры безопасности базы данных для защиты и предотвращения от любого несанкционированного доступа к данным. В ходе анализа подробно описываются 5 уровней безопасности и способы их применения.

Ключевые слова: *SQL Server, безопасность, база данных, уровни безопасности, сетевая безопасность, физическая безопасность, безопасность операционной системы, безопасность приложений, аутентификация, авторизация, конфигурация сервера.*

Annotation: *The article explains various key provisions and aspects in the field of testing and ensuring the security of the SQL Server environment. Security is a very important area for any database environment, so it is necessary to properly plan, deploy and verify database security measures to protect and prevent from any unauthorized access to data. In the course of the analysis, 5 levels of security and how to apply them are described in detail.*

Key words: *SQL Server, security, database, security levels, network security, physical security, operating system security, application security, authentication, authorization, server configuration.*

Тестирование безопасности — это совокупность процессов, посредством которых мы пробуем скомпрометировать различные уровни безопасности приложений, баз данных, систем или отдельных компонентов системы. То есть это процесс разработки и создания специальных тестовых случаев, которые могли бы дестабилизировать безопасность системы.

Систему безопасности SQL Server, которая обеспечивает безопасность и защиту баз данных и ее экземпляров, можно условно разделить на пять уровней:

- физическая безопасность;
- сетевая безопасность;
- безопасность операционной системы;

- безопасность базы данных;
- безопасность приложений.

Физическая безопасность для систем баз данных касается защиты серверов и всех связанных с ней сетевых и аппаратных устройств, размещенных в центре обработки данных. Необходимо всегда разграничивать доступ людей к помещениям центра обработки данных, где физически размещены эти системы. Помимо этого, в обязательном порядке следует настраивать резервные копий для всех критических систем в другом центре обработки данных, чтобы защитить данные и поддерживать работоспособность системы в случае, если что-то случится с первым центром обработки данных. А также следует вести учет посещения и доступа всех лиц к оборудованию системы. Для этого обычно просто устанавливаются камеры видеонаблюдения для наблюдения за безопасностью помещения, оборудования, учета действий и людей.

Если же системы размещены в облачной среде на правах аутсорсинга, в этом случае физическую безопасность обеспечивает уже компания, предоставляющая услуги. Обычно все облачные провайдеры стараются всегда использовать передовые методы защиты своих центров обработки данных.

Далее идет сетевая безопасность, она должна гарантировать, что все коммуникации между базой данных, серверами и приложениями безопасны и надежны. Сетевая безопасность также гарантирует, что различный вредоносный сетевой трафик ограничивается и не направляется с помощью ботов или каких-либо других программ и способов на наши системы, чтобы не выводить их из строя. Таким образом задачи уровня сетевой безопасности состоят в том, чтобы убедиться, что:

- все нежелательные порты заблокированы;
- применяются верные политики брандмауэра для предотвращения вредоносного внешнего сетевого трафика;

- все конечные точки сети защищены средствами, такими как шифрование или сторонними инструментами;
- все пакеты, входящие и исходящие из системы - шифруются.

Безопасность операционной системы включает в себя безопасность на уровне платформы и предотвращает любой несанкционированный доступ к системе баз данных. Безопасность операционной системы:

- повышает безопасность управления доступом за счет применения сложных политик паролей и многофакторной аутентификации;
- защищает систему с помощью брандмауэров для ограничения нежелательных системных вызовов;
- включает в себя защиту двоичных файлов SQL Server или любых системных файлов и файлов приложений, хранящихся на машине;
- включает в себя сканирование уязвимостей и применение обновлений для устранения угроз безопасности операционной системы и SQL Server;
- ограничивает нежелательные службы, путем ограничения контактной зоны SQL Server.

Следующим уровнем является безопасность базы данных, на этом этапе мы защищаем базу данных и ее объекты, путем применения мер контроля доступа внутри самой системы базы данных. Можно разделить безопасность базы данных на следующие 4 категории:

- аутентификация;
- авторизация;
- защита данных;
- правильная настройка конфигурации SQL-сервера.

Аутентификация — это первый шаг к подключению к базе данных. Это процедура проверки подлинности пользователя для подключения к базе данных. Если пользователь не прошел аутентификация, то он не сможет подключиться к базе данных.

Ниже приведены несколько принципов, которые следует учитывать, производя аутентификацию системы:

- Обязательно определите политику паролей, всегда лучше выбирать сложные пароли и менять пароли через определенные промежутки времени.
- Назначьте всем пользователям обязательную многофакторную аутентификацию во всех подсистемах, где это возможно.
- Предоставляйте только необходимые разрешения и ограничивайте любые нежелательные привилегии пользователей.
- Не позволяйте никому использовать общие учетные записи. Необходимо следить за этим и оперативно удалять или отключать их.

Авторизация — это процесс предоставления пользователям доступа к объектам. Вы можете ограничить или разрешить кому-либо доступ к объектам и подсистемам базы данных. Например, чтобы некоторые группы пользователей не могли записывать, обновлять или изменять конкретные объекты базы данных, которые не являются частью их специализации, поэтому с помощью авторизации можно отказать в этих правах на указанный объект.

Защита данных — это очень популярный в наши дни вариант защиты данных с помощью шифрования от несанкционированного использования. Он используется для шифрования наших данных как в состоянии покоя, так и при передаче для баз данных SQL Server. SQL Server предлагает несколько вариантов применения шифрования и маскирования для различных типов данных, например, прозрачное шифрование данных, постоянное шифрование, маскирование данных и т.д. Резервные копии базы данных также могут быть зашифрованы для предотвращения несанкционированного доступа к их данным.

Последний этап - тщательная и правильная настройка конфигурации SQL-сервера, чтобы никакие данные не могли быть скомпрометированы каким-либо образом. Для этого необходимо рассмотреть возможность

изменения порта SQL Server по умолчанию на другой порт, отключить нежелательные службы SQL-сервера, такие как служба браузера SQL, удалить общие учетные записи, а также в определённых системах можно отключить некоторые системные объекты, такие как xp_cmdshell и т.д.

Безопасность приложений — это последний пятый уровень обеспечения безопасности, на котором нам необходимо применить все возможные меры, чтобы установить безопасное соединение с сервером базы данных и предотвратить несанкционированное удаленное выполнение кода. На этом уровне также классифицируются и обрабатываются атаки SQL Injection, которые предотвращают вставку любого вредоносного кода в прикладную программу и выполнение ее в базе данных для повреждения данных.

Таким образом, мы рассмотрели базовые основы мер безопасности и политики безопасности на различных уровнях баз данных SQL Server, которые мы можем предпринять для защиты баз данных и систем, на которых они размещены. Однако не стоит забывать о том, что после применения этих мер и процедур, вы также должны время от времени тестировать их, чтобы убедиться, что все стабильно работает в соответствии с ожиданиями и положениями.

Использованные источники:

1. Бергер, А.Б. Microsoft SQL Server 2005 Analysis Services. OLAP и многомерный анализ данных / А.Б. Бергер. - М.: БХВ-Петербург, 2010. - 701 с.

2. Дунаев, В.В. Базы данных. Язык SQL для студента / В.В. Дунаев. - М.: БХВ-Петербург, 2009. - 150 с.

3. Партыка, Т.Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: ИНФРА-М, 2009. - 368 с.

4. Степанов, Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРА-М, 2011. – 304 с.