Какие меры можно принять для обеспечения безопасности баз данных

Процесс обеспечения безопасности баз данных можно разделить на три основные направления (см. рисунок):

**1. Обеспечение базового уровня безопасности** – реализация аутентификации, авторизации и контроля доступа пользователей БД. Сюда же относится сканирование и классификация баз данных с разделением их на категории – высокой критичности, критичные и некритичные. Понимание того, какая база содержит критичную информацию, является основным требованием для построения процесса обеспечения безопасности БД. Необходимо проводить полную и регулярную инвентаризацию всех баз данных, включая те, которые находятся в непродуктивной зоне и используются для разработки, тестирования или обучения. Следует выработать соответствующие политики безопасности для БД каждой категории. Не менее важен процесс управления патчами и обновлениями СУБД. Специалисты по безопасности БД должны своевременно устанавливать патчи и обновления на все критические базы данных для устранения выявленных уязвимостей.

**2. Реализация ряда превентивных мер**,

а именно:

• применение сетевого шифрования и шифрования архивных данных для сокрытия информации от любопытных глаз, имеющих доступ к внутренней сети компании;

• маскирование персональных данных в непродуктивных базах, используемых для разработки, тестирования и обучения, с целью предотвращения несанкционированного доступа привилегированных пользователей (разработчиков и тестировщиков ПО);

• внесение в структуру данных таких изменений, которые гарантируют, что в дальнейшем только подтвержденные и разрешенные изменения будут переноситься в продуктивную среду.

В общем случае выполнение этих мер носит рекомендательный характер, но для критичных БД является обязательным требованием.

**3. Аудит, мониторинг и оценка уязвимостей** для эффективного обнаружения вторжений. Необходимо обеспечить быстрое реагирование на незапланированные изменения критичных данных или подозрительную активность, связанную с доступом к данным. Аудит БД дает ответы на такие вопросы, как «кто изменил и какие данные?» и «когда было произведено изменение?». Мониторинг активности в базах данных позволяет оповещать о событиях информационной безопасности БД в режиме реального времени и защищать критичные данные. Отчеты с оценкой уязвимостей СУБД, таких как слабые пароли или превышение привилегий, должны дополнять данные мониторинга, которые предоставляют DBA или группа мониторинга безопасности компании.

Проблема безопасности баз данных решается тем, что в СУБД для сохранения информации используется двойной подход. В части операций, как обычно, участвует операционная система компьютера, но некоторые операции сохранения происходят в обход операционной системы.

Защита базы данных

Microsoft Access обеспечивает два традиционных способа защиты базы данных: установка пароля, требуемого при открытии базы данных, и защита на уровне пользователей, которая позволяет ограничить, к какой части базы данных пользователь будет иметь доступ или какую ее часть он сможет изменять. Кроме того, можно удалить изменяемую программу Visual Basic из базы данных, чтобы предотвратить изменения структуры форм, отчетов и модулей, сохранив базу данных как файл MDE.

Установка пароля

Простейшим способом защиты является установка пароля для открытия базы данных. После того как пароль установлен, при каждом открытии базы данных будет появляться диалоговое окно, в которое требуется ввести пароль. Только те пользователи, которые введут правильный пароль, смогут открыть базу данных. Этот способ достаточно надежен (Microsoft Access шифрует пароль, так что к нему нет прямого доступа при чтении файла базы данных), но он применяется только при открытии базы данных. После открытия базы данных все объекты становятся доступными для пользователя (пока не определена защита на уровне пользователей, описанная ниже в этом разделе). Для базы данных, которая совместно используется небольшой группой пользователей или на автономном компьютере, установка пароля обычно оказывается достаточной.