1С. ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАНЫХ

Использование решения Meridian DB Patrol

Текущее состояние

Защита персональных данных. На платформу 1С:Предприятие, версия 8.2z фирмой 1С получены сертификаты соответствия ФСТЭК о признании этих модулей программными средствами общего назначения со встроенными средствами защиты информации от несанкционированного доступа.

Фактически это означает, что в платформе всего лишь реализована возможность регистрации событий, связанных с работой с персональными данными.

Нерешенные проблемы защиты

Привилегированные пользователи (сотрудники IT департамента, системные администраторы, сотрудники службы безопасности) могут иметь полный доступ к данным, одновременно обладая возможностью скрыть свои злоумышленные действия, в особенности если имеет место преступный сговор этих лиц.

Нет защиты «от дурака»: существующие требования ФСТЭК к защите имеют отношение исключительно к технологической платформе, а не к конфигурациям. Т.е. всегда есть техническая возможность иметь «кривую» настройку платформы с такими «дырами» в защите как: неправильная раздача привилегий (например повышенных) на объекты, отсутствие «по забывчивости» контроля на вновь создаваемые объекты и т.п.

Предыдущие версии модулей 1С не имеют средств защиты.

Последствия утечек конфиденциальной информации

Возможность неконтролируемого доступа либо несанкционированного удаления истории доступа к конфиденциальной информации приводит к утечкам и создает предпосылки для полной или частичной потери бизнеса, а именно:

- приводит к раскрытию коммерческой тайны сотрудниками организации с целью ее дальнейшей передачи конкурентам или использования для шантажа или рейдерского захвата
- способствует противоправным действиям в отношении организации (кражи, хищения)

Специальная защита данных с помощью решения Meridian DB Patrol

I.**Аудит работы с данными с клиентских рабочих мест в режиме реального времени.** Система протоколирует все обращения пользователей к данным с рабочих мест сотрудников: запросы данных, добавление, изменение, удаление данных.

II.**Контроль работы привилегированных пользователей.** В состав решения входит локальный агент, который отслеживает все локальные обращения к базе данных. Это не дает скрыть свою активность даже системному администратору и администратору баз данных.

III.**Предотвращение утечки данных.** За счет комплексного контроля сетевых и локальных интерфейсов утечка данных исключена.

IV.**Формирование отчетности для обеспечения соблюдения требований безопасности.** Система имеет в своем составе рабочее место офицера безопасности, которое позволяет в удобном графическом интерфейсе осуществлять настройку правил и политик и формировать отчеты.

V.**Контроль прав доступа.** Система позволяет обнаруживать факты изменения прав доступа на объекты базы данных.

VI.**Обнаружение тематической активности при обращении к конфиденциальным данным.** Система позволяет настроить шаблоны аудита по ключевым словам в целях обнаружения активности по определенной тематике в общей массе конфиденциальной информации. Например, можно выявить активность запросов по определенному лицу, организации, номеру счета, номерам телефонов и иным атрибутам конфиденциальной информации, которые хранятся в базе данных.

VII.**Негласная установка.** Система устанавливается «рядом» с каналами связи и ничем не обнаруживает своё присутствие. Система полностью автономна, т.е. независима от IT департамента и не может контролироваться службой безопасности, сильно затрудняя их возможный преступный сговор. Об установке системы могут извещаться только самые доверенные лица.

Свяжитесь с нами:

123104, Москва, Трёхпрудный переулок 4, стр.1
+7 (495) 989-45-48
info@concerteza.ru
http://www.concerteza.ru/