вычислительные системы Научно-производственное объединение

Imperva SecureSphere 8.0

Управление безопасностью систем прикладного уровня

О продукте

Imperva SecureSphere 8.0 - комплекс средств защиты серверов баз данных, Web-серверов и файловых серверов представляет собой единую платформу, обеспечивающую защиту от несанкционированного доступа к базам данных (БД), Web-приложениям и файлам, располагающихся в сети организации.

Комплекс прошел успешную сертификацию во ФСТЭК России и может использоваться для создания автоматизированных систем до класса защищенности 1Г включительно и для защиты информации в информационных системах обработки персональных данных до 2 класса включительно.

Назначение комплекса:

1. контроль и регистрация доступа к серверам БД, Web-серверам и файловым серверам, обрабатывающим конфиденциальную информацию, в частности, персональные данные;

2. анализ защищенности элементов сетевой инфраструктуры (операционных систем и программного обеспечения серверов БД и Web-серверов) на наличие уязвимостей;

3. обнаружение вторжений на элементы сетевой инфраструктуры (серверы БД и Web-серверы) информационной системы.

Основные компоненты комплекса:

- **Сервер мониторинга;**
- **Программный агент, при необходимости устанавливаемый на сервере СУБД;**
- **Сервер управления серверами мониторинга.**

Схема работы:

- В сети организации устанавливается сервер мониторинга и сервер управления
- На сервере управления серверами мониторинга создаётся политика безопасности, реализуемая сервером мониторинга.
- На основе политик безопасности сервер мониторинга проверяет корректность запросов к серверам прикладных систем и выдаёт предупреждения в случае обнаружения отклонений от политики безопасности.
- В зависимости от настроек профиля, при обнаружении несоответствия политикам, установленным на сервере управления, сервер мониторинга сбрасывает текущую сессию пользователя путём отправки команды TCP Reset на защищаемый сервер

Основные выполняемые функции:

- идентификация неправомерных действий пользователей и администраторов БД и web-приложений путем сопоставления их текущих запросов с данными, хранимыми в профилях;
- идентификация пользователей, осуществляющих запросы к базам данных, как напрямую, так и через промежуточные web-приложения, агрегирующие их запросы от имени единой учетной записи (connection pooling);
- обнаружение работающих в сети серверов систем управления базами данных (СУБД) и чувствительных данных (номера кредитных карточек, номера карточек социального страхования и др.);
- оценка конфигурации серверов СУБД на наличие уязвимостей;
- обеспечение полноценнуой защитуы данных платежных пластиковых карт;
- составление отчетов по требованиям основных стандартов (PCI DSS, SOX, HIPAA) и отчетности по внутрикорпоративным стандартам;
- перехват запросов к базам данных с консоли или сессий telnet/SSH с помощью программного агента, устанавливаемого непосредственно на сервере СУБД;
- осуществление противодействие HTTP-атакам, включая атаки на переполнение буфера, действия вредоносных программ и злоумышленников;
- обеспечение защиты данных приложений SAP, PeopleSoft и Oracle

Отличительные особености:

Ключевыми отличиями Imperva SecureSphere 8.0 от аналогичных систем других производителей является наличие в составе комплекса средства динамического профилирования - Dynamic Profiling, снимающего с администраторов баз данных рутинные обязанности по обновлению политик безопасности при каждом изменении ролей пользователей, а также системы Intrusion-Prevention System, позволяющей сканировать сервер баз данных на предмет наличия уязвимых мест и действовать в качестве системы предотвращения вторжений.

Кроме этого сервер мониторинга производства компании Imperva выгодно отличается от остальных устройств обеспечения безопасности баз данных подробной классификацией правил и детальными сигнатурами. Набор встроенных сигнатур можно обновлять и модифицировать.

Соответствие требованиям PCI DSS:

Требования PCI DSS	Imperva SecureSphere 8.0
Создание и сопровождение конфигурации межсетевого экрана для защиты данных держателей карт	+
Неиспользование выставленных по умолчанию производителями системных паролей и других параметров безопасности.	+
Обеспечение защиты данных держателей карт в ходе их хранения	+
Обеспечение шифрования данных держателей карт при их передаче через общедоступные сети	
Использование и регулярное обновление антивирусного программного обеспечения	
Разработка и поддержка защищенных систем и приложений	+
Разграничение доступа к данным по принципу служебной необходимости	+
Присвоение уникального идентификационного номера каждому лицу, располагающему доступом к компьютеру	+
Ограничение физического доступа к данным держателей карт	
Отслеживание всех сеансов доступа к сетевым ресурсам и данным владельцев карт	+
Регулярное тестирование систем и процессов обеспечения безопасности	+
Наличие и исполнение в организации политики информационной безопасности	

Сведения о сертификации:

Сертификат соответствия №2255 подтверждает соответствие комплекса Imperva SecureSphere 8.0 требованиям ФСТЭК России, предъявляемым к безопасности информации.


СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

СЕРТИФИКАТ СООТВЕТСТВИЯ № 2255

Сертификат выдан на основании результатов сертификационных испытаний, проведенных испытательной лабораторией ЗАО «Документальные системы»
Дата выдачи сертификата - 18.01.2011

Практическое применение:

Использование комплекса Imperva SecureSphere 8.0 представляет особый интерес для крупных предприятий телекоммуникационной и банковской отраслей, работающих с большим объемом конфиденциальной информации (персональные данные клиентов, счета, кредитные карты) и предъявляющих повышенные требования к безопасности своего бизнеса.

О компании ООО «НПО ВС»:

ООО «Научно-производственное объединение вычислительных систем» (ООО «НПО ВС) - российский разработчик и поставщик продуктов и комплексных решений в области информационных технологий.
Деятельность ООО «НПО ВС» направлена на решение задач, которые стоят перед любым развивающимся бизнесом. Спектр услуг, решений и сервисов компании способен удовлетворить запросы различных категорий заказчиков: крупных корпораций, компаний малого и среднего бизнеса, а также частных пользователей.

В 2009 году в целях проведения сертификационных испытаний средств защиты информации по требованиям безопасности информации была создана испытательная лаборатория ООО «НПО ВС». В лаборатории разработана система контроля качества, которая обеспечивает и поддерживает необходимый уровень всех работ по сертификации средств защиты информации. Лаборатория признана технически компетентной для проведения сертификационных испытаний на соответствие требованиям, установленным в нормативных документах по безопасности информации и документах системы ГАЗПРОМСЕРТ.

Контакты:

420088, г. Казань,
Ул. Журналистов, 30
Телефон: (843) 567-57-58
Факс: (843) 279-51-73