16 апреля 2025

Ошибки в настройке CRM, которые могут стоить бизнесу миллионы: рекомендации от MONS

Компания MONS, поставщик ИТ-решений и услуг в области информационной безопасности, часть группы компаний «Корус Консалтинг» обращает внимание ритейлеров на критически важные аспекты защиты CRM-систем, особенно на платформе Битрикс24. В условиях роста киберугроз правильная настройка корпоративных порталов становится не просто рекомендацией, а обязательным условием ведения бизнеса.

ПОЧЕМУ CRM-СИСТЕМЫ СТАНОВЯТСЯ ГЛАВНОЙ МИШЕНЬЮ ДЛЯ АТАК?

CRM-системы содержат «золотую жилу» для злоумышленников: персональные данные клиентов, финансовую информацию, коммерческие тайны. По данным исследований, более 60% утечек данных происходят из-за неправильной настройки или устаревшего ПО.

Мы часто сталкиваемся с ситуациями, когда компании инвестируют в дорогостоящие системы защиты периметра, но при этом оставляют базовые уязвимости в своих CRM.

ОПАСНЫЕ ОШИБКИ В НАСТРОЙКЕ БИТРИКС24

1. **Устаревшие компоненты** (использование End-of-Life версий CentOS, устаревших библиотек jQuery или неактуальных версий открывает сотни известных уязвимостей)
2. **Стандартные пути и настройки** (URL типа /bitrix/admin/, отображение версий платформы и другие «заводские» параметры значительно облегчают работу злоумышленников)
3. **Слабые механизмы аутентификации** (отсутствие двухфакторной аутентификации, использование простых паролей и доменных учетных записей для администрирования)
4. **Избыточные права у сервисных пользователей** (например, www-data с административными правами — это как оставить ключи от сейфа на ресепшн)
5. **Отсутствие сегментации** (совместное размещение веб-сервера, сервера приложений и БД на одной машине без должного разграничения)

Современные CRM-системы — это центральный узел, в котором сосредоточены ключевые бизнес-процессы и критически важные данные компании. Однако их сложная архитектура требует особого внимания к вопросам безопасности. Компания MONS предлагает комплексный подход, который выходит за рамки простого устранения уязвимостей и обеспечивает долгосрочную защиту от постоянно эволюционирующих угроз.

Основу защиты составляет актуальность всех компонентов системы. Регулярное обновление программного обеспечения закрывает известные уязвимости и значительно снижает риски взлома. При этом важно учитывать не только саму платформу, но и всю связанную инфраструктуру — от серверных компонентов до вспомогательных библиотек.

Особое внимание уделяется контролю доступа. Многоуровневая аутентификация, включающая дополнительные проверки при входе, позволяет предотвратить несанкционированный доступ даже в случае компрометации учетных данных. Современные методы защиты учетных записей и гибкие политики блокировки подозрительной активности существенно повышают безопасность системы.

Административные интерфейсы требуют специальных мер защиты. Изменение стандартных параметров доступа, ограничение по IP-адресам и сокрытие служебной информации затрудняют злоумышленникам сбор данных для атаки. Эти меры особенно важны для CRM-систем, где административные панели часто становятся главной мишенью для взлома.

Грамотная настройка серверной инфраструктуры играет ключевую роль в обеспечении безопасности. Внедрение современных протоколов защиты данных и правильная конфигурация веб-серверов создают дополнительный барьер для киберугроз.

Логическое разделение компонентов системы и постоянный мониторинг завершают комплекс мер по защите CRM. Разнесение функциональных блоков по разным серверам или сегментам сети ограничивает возможный ущерб при нарушении безопасности. Системы мониторинга позволяют оперативно выявлять и пресекать подозрительную активность.

Помимо защиты CRM-систем, MONS предлагает полный спектр услуг по информационной безопасности:

1. Проведение аудитов и penetration testing
2. Разработка стратегий защиты информации
3. Внедрение SIEM-систем и решений класса EDR
4. Организация VPN-доступов с двухфакторной аутентификацией
5. Создание систем резервного копирования и аварийного восстановления

Безопасность — это не разовое мероприятие, а непрерывный процесс. Мы помогаем заказчикам не только закрыть текущие уязвимости, но и выстроить систему постоянного мониторинга и улучшений.