



CASE STUDY

ИТ-среда с нуля: история создания инфраструктуры безопасности БК «Лига Ставок»



БК «Лига Ставок» – российская букмекерская компания, основанная в 2008 году. Деятельность компании направлена на развитие букмекерского бизнеса в России, поддержку национального спорта и создание новой сферы развлечений. Сегодня БК «Лига Ставок» — это 3 500 сотрудников и 500 клубов в 120 городах Российской Федерации.

БК «Лига Ставок» возглавляет Национальный рейтинг букмекеров РБК, а также является лауреатом престижных премий в области спорта и букмекерства.

Миссия БК «Лига Ставок» - это всесторонняя поддержка российского спорта. Компания принимает активное участие в развитии и популяризации различных видов спорта, сотрудничает со спортивными федерациями и национальными сборными командами. БК «Лига Ставок» является генеральным партнером Российской Премьер-Лиги, официальным партнером Федерации хоккея России, генеральным партнером Федерации регби России, а также генеральным партнером Федерации бокса России.

Вызовы интенсивного развития

С момента своего основания БК «Лига Ставок» динамично развивалась и нуждалась в налаживании процессов, связанных с обеспечением кибербезопасности. Применяемые ранее решения были неоднородны, закупались у разных производителей, не предполагали возможностей управления из единого центра, а вся инфраструктура значительно отставала от уровня решений класса enterprise. При этом компания время от времени сталкивалась с атаками на приложения, DDoS и различными внутренними угрозами.

Специалисты БК «Лига Ставок» искали решение, которое соответствовало бы всем ключевым требованиям компании и обеспечило бы комплексную защиту филиальной сети и ИТ-среды. Важнейшими стали следующие характеристики:

- 1. Управление из единого центра.** Количество специалистов, способных развернуть решение для обеспечения кибербезопасности достаточно ограничено, в связи с чем важно было минимизировать сложность управления всей структурой.
- 2. Гибкость.** Компания постоянно развивается, сеть клубов и количество пользователей растет, а значит, было необходимо решение, которое способно быстро адаптироваться и расширяться, соответствуя актуальным и будущим вызовам.

Платформа Fortinet Security Fabric отвечала обозначенным требованиям, обеспечивая широкий обзор всей среды и позволяя легко управлять безопасностью системы и сетевыми операциями.

«Создание инфраструктуры безопасности на базе Fortinet Security Fabric позволило нам сформировать прочный фундамент развития ИТ-среды компании практически с нуля. Значительно повысилась управляемость, производительность и отказоустойчивость сети. Теперь мы способны эффективно обеспечивать безопасность и непрерывность бизнеса».

– Алексей Кислицын,
Директор департамента
информационной
безопасности

Общая информация

Клиент: БК «Лига Ставок»

Отрасль: Букмекерский бизнес

Страна: Россия

Повышение эффективности управления процессами

Одной из первых задач в рамках внедрения новой инфраструктуры безопасности стало создание однородной системы обеспечения безопасности рабочих станций (как в клубах, так и для сотрудников офиса), которые зачастую становятся первыми жертвами различных атак. Было принято решение развернуть FortiClient, средство защиты конечных точек следующего поколения, позволяющее собирать всю необходимую информацию о сети, распределенной по всей стране, отслеживать и предотвращать угрозы. Теперь данные об угрозах и состоянии конечных станций стекались в одно место, что позволило повысить эффективность управления всеми процессами – от патч-менеджмента до централизованного управления и технического обновления конечных точек.

Защиту внутренней среды компании обеспечивают межсетевые экраны FortiGate: первый отвечает за очистку входящего и исходящего трафика, второй – терминацию всех VPN-соединений, что позволяет эффективно организовать работу удаленных сотрудников и сегментировать доступ к различным ресурсам. Таким образом, удалось обеспечить сетевые потребности более 3500 человек – 2500 кассиров в клубах по всей стране и 300 сотрудников, которые работают удаленно, а также нужды 1000 ПК в клубах, которые используются для обслуживания клиентов и 500 – в головном офисе компании.

Анализировать информацию и управлять каждой частью такой обширной системы позволяют FortiManager и FortiAnalyzer, которые обеспечивают эффективное администрирование, прозрачность, а также позволяют получать информацию в режиме реального времени по всей платформе Fortinet Security Fabric.

Важным аспектом внутрикорпоративной безопасности также является почта сотрудников. Несмотря на постоянное обучение и разъяснение потенциальных рисков, всегда существует опасность заражения. За предотвращение возможных проблем в этом направлении отвечают решения FortiMail и FortiSandbox, защищающие корпоративную систему от вредоносного ПО и атак нулевого дня.

Сегодня в БК «Лига Ставок» эксплуатацией системы занимаются 8 человек: 2 сетевых инженера отвечают за конфигурацию программно-аппаратной составляющей системы, 4 специалиста занимаются непосредственно созданием и применением политик безопасности, еще 2 администратора – почтовыми шлюзами. После полноценного развертывания FortiWeb управление сервисом будет осуществляться отдельными специалистами, а по мере изменения масштабов бизнеса планируется увеличение штата технического персонала.

Процесс внедрения сопровождался рядом вызовов, связанных с отсутствием у технических специалистов компании достаточного опыта в области кибербезопасности. На момент начала сотрудничества команда только формировалась, и не все сотрудники были знакомы с решениями Fortinet. Тем не менее, эти трудности со временем удалось преодолеть: штат был сформирован под текущие нужды, а все пробелы в обучении ликвидированы.

Прочный фундамент: управляемость и масштабируемость

Развертывание Fortinet Security Fabric позволило БК «Лига Ставок» за несколько лет создать безопасную сетевую инфраструктуру, которая легко управляется и масштабируется согласно запросам бизнеса. Значительно выросла производительность, пропускная способность, управляемость, доступность и работоспособность сети. Еще на первых этапах внедрения специалисты компании провели качественный аудит возможных киберугроз и обозначили приоритеты развития инфраструктуры. Важнейшим результатом для бизнеса стало достижение высокого уровня отказоустойчивости системы. Таким образом, проект

Бизнес результаты

- Обеспечили отказоустойчивость клиентской и корпоративной части бизнеса
- Объединили всю инфраструктуру в единую сеть
- Улучшили защиту компании от таких угроз, как атаки на приложения, DDoS
- Снизили сложность инфраструктуры за счет однородности решений

Решение

- FortiGate
- FortiManager
- FortiAnalyzer
- FortiClient
- FortiWeb
- FortiMail
- FortiSandbox

по созданию эффективной системы информационной безопасности повлек за собой крупномасштабную модернизацию корпоративной сети, которая к моменту реализации проекта также отставала от темпов развития компании. Успех проекта обусловлен тесным взаимодействием департаментов ИТ и информационной безопасности, а также подходом, при котором обеспечение информационной безопасности является общей корпоративной задачей. Сотрудники выполняют рекомендации департамента ИБ, при этом, постоянно проходят обучение и тесты. Департамент ИТ эффективно эксплуатирует средства безопасности, а сотрудники ИБ, в свою очередь, разрабатывают политику, регламенты, а также планы по развитию, осуществляют выбор и интеграцию средств защиты, их внедрение, отладку и передачу в эксплуатацию.

При помощи решений FortiToken и FortiAuthenticator в ближайшее время планируется внедрить двухфакторную аутентификацию для сотрудников. Потребность в этом возникла в связи с планируемым запуском внутрикорпоративного портала, который будет работать через FortiWeb. Кроме того, БК «Лига Ставок» планирует запустить тестирование SD-WAN на базе флагманских клубов, а затем постепенное расширение технологии на всю инфраструктуру.