POSITIVE TECHNOLOGIES ЗАЩИТИЛА СЕРВИСЫ ТРАНСПОРТНОЙ ДИРЕКЦИИ ЧЕМПИОНАТА МИРА ПО ФУТБОЛУ

«Продукты Positive Technologies MaxPatrol SIEM и PT Application Firewall стали важной составляющей созданного нами контура информационной безопасности, отлично интегрировались с другими используемыми решениями и обеспечили качественное и непрерывное функционирование всех информационных систем. Работа на домашнем чемпионате мира совместно со специалистами Positive Technologies показала их высокий профессионализм и эффективность предлагаемых ими решений. За все время проекта злоумышленники не смогли провести ни одной успешной атаки на защищаемые информационные ресурсы»

Николай Якимов, генеральный директор «ЛАНИТ Северо-Запад»

ПРОФИЛЬ ОРГАНИЗАЦИИ

- **Название:** АНО «Транспортная дирекция чемпионата мира по футболу 2018 года в Российской Федерации»
- **Деятельность:** организация транспортных услуг при подготовке и проведении ЧМ по футболу 2018 года
- **Информационные сервисы:** официальный сайт транспортной дирекции, сайт для оформления бесплатных билетов, «Транспортный гид болельщика», информационный ресурс для временного персонала
- **Инфраструктура:** три центра обработки данных: два в Москве и один в Новосибирске

- **Задача:** комплексная защита веб-приложений и мониторинг безопасности инфраструктуры
- **Решение:** услуги PT ESC по мониторингу безопасности инфраструктуры и веб-приложений

С 14 июня по 15 июля 2018 года в России проходила финальная часть чемпионата мира по футболу. По распоряжению Правительства РФ была создана АНО «Транспортная дирекция — 2018». В ее задачи входили транспортное планирование и координация транспортного обслуживания при подготовке и проведении мундиаля.

ЗАДАЧА

Для транспортного обслуживания чемпионата по заказу дирекции IT-компания «ЛАНИТ Северо-Запад» разработала информационные сервисы для болельщиков, волонтеров и компаний-перевозчиков. Главной задачей транспортной дирекции на время подготовки и проведения чемпионата было обеспечить бесперебойную работу и защиту высоконагруженных сервисов в режиме реального времени в условиях ежедневных доработок и обновлений приложений со стороны разработчиков.

50 тыс.
пользователей
скачали приложение «Транспортный гид болельщика»

90%
всех билетов
было оформлено через сайт tickets.transport2018.com

16,3 тыс.
автобусов
зарегистрировано на специальном информационном ресурсе

400 тыс.
билетов
оформили болельщики с 12 июня по 16 июля

РЕШЕНИЕ

Для решения поставленных задач транспортная дирекция совместно с компанией «ЛАНИТ Северо-Запад» выбрала услуги по мониторингу безопасности инфраструктуры компании Positive Technologies. Ключевым фактором выбора стал предложенный специалистами Positive Technologies Expert Security Center (PT ESC) многоуровневый подход к обеспечению безопасности, который включал:

- выявление существующих рисков информационной безопасности ресурсов сетевого периметра и выработку мер по минимизации угроз;
- анализ веб-трафика, анализ событий и выявление инцидентов ИБ на уровне функционирования приложений, средств защиты, операционных систем и логики работы приложений;
- круглосуточный мониторинг информационной безопасности.

Сервисы безопасности PT ESC и прежде доказывали свою эффективность во время экспертного сопровождения общегосударственных проектов, таких как зимняя Олимпиада-2014 в Сочи, выборы Президента РФ и проведение ЕГЭ.

Работы проводились в период с февраля по сентябрь 2018 года. На первом этапе специалисты Positive Technologies по тестированию на проникновение провели анализ работы приложений в ручном режиме и с использованием анализатора защищенности исходного кода приложений PT Application Inspector, а также проверили корректность настройки сетевого оборудования. По итогам они предложили разработчикам и IT-специалистам рекомендации по устранению потенциально опасных ошибок и затем проверили выполнение всех рекомендаций.

Продукты Positive Technologies:

- межсетевой экран уровня веб-приложений PT Application Firewall,
- анализатор защищенности исходного кода приложений PT Application Inspector,
- система выявления инцидентов ИБ MaxPatrol SIEM

Positive Technologies Expert Security Center (PT ESC) — экспертное подразделение Positive Technologies. За 15 лет тестов на проникновение, анализа защищенности, расследования инцидентов и мониторинга безопасности эксперты наработали лучшие приемы и методы в области практической безопасности.

Были выявлены:

38 641
критически опасная атака, направленная на веб-приложения (среди них SQL Injection, OS Commanding, Shellshock)

22 453
критически опасных события от систем мониторинга инфраструктуры (выполнение подозрительных команд ОС, попытки неавторизованного доступа, попытки доступа по портам)

Следующим этапом стало создание контура безопасности. Информационные системы размещались в трех центрах обработки данных — двух в Москве и одном в Новосибирске. Компоненты средств защиты информации были установлены и настроены во всех ЦОД. Ядром контура стала система выявления инцидентов в режиме реального времени MaxPatrol SIEM: она получала информацию от межсетевого экрана уровня веб-приложений PT Application Firewall, операционных систем, СУБД, серверов и другого ПО, используемого в рамках защищаемой инфраструктуры.

«В начале 2018 года мы прогнозировали волну атак на веб-приложения, имеющие отношение к ЧМ-2018. Под угрозой были данные пользователей, работоспособность информационных сервисов. Это могло привести к репутационным и денежным потерям, а также существенно осложнить проведение мероприятия с точки зрения перемещения болельщиков. Поэтому нашей первостепенной задачей было выявить слабые места веб-приложений и всей инфраструктуры и разработать компенсирующие меры, — рассказывает руководитель PT ESC Алексей Новиков. — Ситуацию усложняло то, что приложения постоянно дорабатывались, еще одним вектором угроз могли стать ошибки разработчиков, которые могли бы привести к серьезным уязвимостям. Поэтому дополнительно мы отслеживали деятельность разработчиков, контролировали каналы, через которые они попадали в инфраструктуру, и мониторили вносимые ими изменения».

Для поддержки созданного контура ИБ с мая 2018 года специалисты подразделения PT Expert Security Center компании Positive Technologies осуществляли мониторинг защищенности всей инфраструктуры в режиме 24/7. Во время работ использовалась постоянно пополняемая экспертная база знаний, описывающая способы обнаружения новых угроз, наработки и методы, направленные на предотвращение инцидентов ИБ на веб-приложениях.

РЕЗУЛЬТАТЫ

При анализе защищенности эксперты Positive Technologies выявили:

- с помощью анализатора исходного кода — 38 уязвимостей, из них 3 критически опасных;
- в ходе тестирования на проникновение — 59 уязвимостей, из них 9 критически опасных;
- в рамках усиленного контроля сетевого периметра — 129 уязвимостей, из них 15 критически опасных;
- в процессе мониторинга — 3 уязвимости.

Результатом подготовительных работ, в ходе которых специалисты транспортной дирекции и разработчики системы устранили большинство уязвимостей и выполнили рекомендации PT ESC, стало соответствие информационных сервисов требованиям ИБ на момент их публичного выпуска. Последующий контроль безопасности обновляемых приложений, круглосуточный мониторинг безопасности, а также оперативное выполнение специалистами транспортной дирекции всех рекомендаций PT ESC позволили значительно повысить уровень защищенности инфраструктуры и не допустить возникновения критически опасных инцидентов, связанных с обнаруженными уязвимостями, хранением паролей в открытом виде, компрометацией информационных систем, кражей данных пользователей или заражением вредоносным ПО пользователей и инфраструктуры.

Автоматические средства защиты блокировали потенциальные угрозы. PT Application Firewall в автоматическом режиме заблокировал более полумиллиона угроз за весь период работы, а правила корреляции MaxPatrol SIEM сработали в общей сложности несколько десятков тысяч раз. Кроме того, 67 раз была проведена ручная блокировка IP-адресов, с которых осуществлялись попытки нелегитимных действий.

В ходе мониторинга эксперты Positive Technologies расследовали 21 комплексный инцидент и совместно со специалистами транспортной дирекции оперативно применили компенсирующие воздействия. За все время проекта злоумышленники не смогли провести ни одной успешной атаки на защищаемую систему.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.

POSITIVE TECHNOLOGIES

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays