ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ТЮМЕНСКОЙ ОБЛАСТИ КОНТРОЛИРУЕТ ЗАЩИЩЕННОСТЬ IT-ИНФРАСТРУКТУРЫ ПРАВИТЕЛЬСТВА С ПОМОЩЬЮ MAXPATROL 8

«Обеспечение высокого уровня безопасности государственных ресурсов и информационных систем является одной из ключевых задач Центра информационных технологий. Сотрудничество с Positive Technologies позволило нам объективно оценить текущую защищенность IT-инфраструктуры, выстроить стабильный процесс управления уязвимостями, а также обеспечить уровень безопасности, полностью соответствующий как мировым стандартам, так и требованиям российских регуляторов».

Александр Забокрицкий
Начальник отдела информационной безопасности ЦИТ Тюменской области

ПРОФИЛЬ КОМПАНИИ

- **Организация:** Центр информационных технологий Тюменской области
- **Отрасль:** государственный сектор, информационные технологии
- **Задача:** оценка защищенности инфраструктуры правительства Тюменской области и выстраивание процесса управления информационной безопасностью
- **Решение:** система контроля защищенности и соответствия стандартам MaxPatrol 8
- **Результат:** выстроен стабильный процесс управления информационной безопасностью и автоматизирован контроль соответствия требованиям регуляторов

ЗАДАЧА

Центр информационных технологий Тюменской области — подведомственное учреждение департамента информатизации Тюменской области. Основные направления деятельности ЦИТ — сопровождение государственных интернет-ресурсов и информационных систем, централизованное обслуживание оборудования и ПО на рабочих местах и администрирование сетей.

Для реализации данных процессов была создана распределенная IT-инфраструктура, обслуживающая множество департаментов. Поддержка такой инфраструктуры сопряжена с множеством разнородных проблем: растущим числом критически опасных уязвимостей в ИТ и несвоевременным их устранением; ошибками, допускаемыми техническими специалистами при настройке программных средств; отсутствием организованного контроля за соответствием компонентов систем необходимым требованиям. Все эти факторы представляли серьезную угрозу информационной безопасности сервисов ЦИТ и правительственных ресурсов.

В связи с этим перед ЦИТ встала задача по обеспечению надежного контроля защищенности используемых информационных систем. Для ее решения требовался инструмент, позволяющий своевременно обнаруживать уязвимости и предотвращать возможные атаки и их негативные последствия, а также способный минимизировать финансовые потери и репутационные риски обслуживаемых государственных структур в случае реализации угроз. Не менее важно было обеспечить соответствие уровня защищенности стандартам и требованиям регуляторов.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- **Тестирование на проникновение.** Проверки на сетевом уровне с минимальными привилегиями, анализ защищенности веб-приложений и СУБД
- **Системные проверки.** Проверки посредством удаленного доступа для контроля обновлений, анализа конфигураций и оценки стойкости паролей
- **Контроль соответствия стандартам.** Обработка результатов системных проверок с учетом требований регуляторов и отраслевых стандартов
- **Оценка эффективности процессов ИБ.** Проверка качества работы отделов ИТ и ИБ с помощью обширного набора технических и высокоуровневых метрик
- **Гибкая система отчетности.** Формирование информативных отчетов о состоянии защищенности IT-инфраструктуры на всех уровнях

РЕШЕНИЕ

В качестве решения Центр информационных технологий выбрал разработанную Positive Technologies систему контроля защищенности и соответствия стандартам MaxPatrol 8. На всех ключевых этапах контроля защищенности данная система эффективно решает следующие задачи:

- инвентаризация компонентов информационных систем и планирование контроля защищенности;
- поиск и устранение уязвимостей и ошибок конфигураций компонентов информационных систем, а также несоответствий фактических настроек установленным требованиям (внутренним политикам и стандартам);
- анализ результатов контроля защищенности, формирование информативных отчетов;
- оценка эффективности контроля защищенности и действий, связанных с устранением нарушений безопасности.

Для всестороннего анализа защищенности MaxPatrol 8 располагает мощными механизмами оценки уровня безопасности, такими как тестирование на проникновение (PenTest), системные проверки (Audit) и контроль соответствия стандартам (Compliance). Благодаря этим механизмам система воссоздает целостную картину процессов информационной безопасности, позволяет управлять ими централизованно без дополнительных ресурсных затрат на обслуживание отдельных компонентов систем и отслеживает соответствие уровня защищенности стандартам и требованиям регуляторов.

РЕЗУЛЬТАТ

Использование MaxPatrol 8 позволило Центру информационных технологий объективно оценить текущую защищенность информационных систем и взять под контроль безопасность IT-инфраструктуры как в целом, так и на уровне отдельных узлов и приложений. Благодаря автоматизации и централизации контроля защищенности существенно сократились трудозатраты сотрудников ЦИТ, связанные с обеспечением информационной безопасности, и было сведено к минимуму влияние человеческого фактора. С помощью MaxPatrol 8 был успешно выстроен единый циклический процесс управления уязвимостями, а также взяты под контроль выполнение требований регуляторов и соответствие отраслевым стандартам.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». 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.

POSITIVE TECHNOLOGIES

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