PT APPLICATION FIREWALL ПОВЫШАЕТ УРОВЕНЬ ЗАЩИЩЕННОСТИ ВУЗОВ

«Веб-порталы всегда находятся под пристальным вниманием злоумышленников, официальные сайты вузов не исключение. Изучая рынок ИБ-средств, мы обратили внимание на межсетевой экран уровня приложений PT Application Firewall, так как в нем реализованы самые современные технологии защиты веб-приложений. Использование PT Application Firewall позволило нам осуществлять непрерывный мониторинг безопасности портала УрФУ и оперативно реагировать на атаки. Мы благодарны экспертам компаний Positive Technologies и „Экстрим безопасность" за проявленную при совместных работах отзывчивость и высокий уровень профессионализма».

Артём Ушаков
Начальник управления информационной безопасности УрФУ

ПРОФИЛЬ ОРГАНИЗАЦИИ

- **Название:** Уральский федеральный университет имени первого Президента России Б. Н. Ельцина
- **Сфера деятельности:** образовательное учреждение
- **Задача:** защита официального сайта УрФУ от веб-атак
- **Решение:** межсетевой экран уровня приложений PT Application Firewall

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина — крупнейший федеральный университет России, в котором обучаются 35 000 студентов.

ЗАДАЧА

В последние годы веб-порталы образовательных учреждений все чаще становятся мишенью для киберпреступников. Злоумышленники атакуют сайты с целью хулиганства, фальсификации информации об успеваемости, политической пропаганды среди студентов. По данным аналитиков Verizon, только в 2015 году было зафиксировано 254 киберинцидента в сфере образования, среди пострадавших в том числе российские вузы.

Как показывает практика, веб-порталы вузов содержат большое количество уязвимостей, вызванных ошибками разработчиков. Согласно исследованию Positive Technologies, за счет эксплуатации уязвимостей веб-приложений злоумышленники могут получить доступ во внутреннюю сеть организации и к конфиденциальной информации пользователей в 47% случаях. Так, взлом вузовского веб-портала может повлечь за собой компрометацию персональных данных студентов и преподавателей, а также потерю контроля над важнейшими IT-ресурсами вуза.

Официальный портал УрФУ (urfu.ru) — основная информационная площадка вуза с личными кабинетами для сотрудников и студентов. Ежемесячная посещаемость портала от 10 000 до 15 000 человек. Максимальное количество посещений наблюдается в период единого государственного экзамена и приемной кампании и приходится на абитуриентов. Именно в это время наиболее актуальны обеспечение бесперебойной работы сайта и защита персональных данных сотрудников, студентов и абитуриентов.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

- Защита от всех распространенных уязвимостей по классификациям OWASP и WASC
- Выявление уязвимостей в исходном коде и автоматизированное создание виртуальных патчей (модуль P-Code)
- Проверка загружаемых в веб-приложение файлов несколькими антивирусными движками (модуль M-Scan)
- Быстрое самообучение
- Автоматическая блокировка атак нулевого дня
- Блокировка атак на пользователей приложения
- Защита от программ-роботов
- Корреляция событий и построение цепочек атак

РЕШЕНИЕ

В условиях растущих угроз, связанных с кибератаками на веб-приложение, УрФУ потребовался современный инструмент для мониторинга безопасности портала. Для решения поставленной задачи УрФУ остановился на межсетевом экране уровня приложений PT Application Firewall, предназначенном для выявления и блокирования современных атак на веб-порталы.

PT Application Firewall был отмечен аналитиками Gartner как визионерский продукт в рейтинге Magic Quadrant for Web Application Firewalls 2015–2016 гг.

Благодаря алгоритмам машинного обучения PT Application Firewall создает статистическую модель функционирования приложения и на ее основе выявляет аномальное поведение, что позволяет блокировать большинство атак нулевого дня, фишинг, флуд, спам. Кроме того, механизм выявления веб-фрода позволяет своевременно отслеживать нехарактерную активность пользователей и несанкционированную деятельность программ-роботов. Еще одно преимущество системы — интеллектуальная обработка и корреляция событий безопасности для выделения самых важных из них.

Развертывание PT Application Firewall производила компания-интегратор «Экстрим безопасность», которая уже много лет работает на рынке информационных технологий Екатеринбурга и Свердловской области, а также других городов Российской Федерации. Совместно с экспертами Positive Technologies были проведены все необходимые работы по настройке PT Application Firewall в режиме мониторинга.

РЕЗУЛЬТАТ

Межсетевой экран уровня приложений PT Application Firewall позволил своевременно обнаружить попытки таких атак на сайт УрФУ, как Shellshock, SQL Injection и XSS, а также попытки загрузки вредоносного кода и атаки, направленные на выполнение произвольного кода на стороне сервера.

При успешной реализации этих атак злоумышленники могли бы:

- изменять содержимое сайта УрФУ, например размещать порочащую информацию, корректировать или удалять результаты ЕГЭ, данные об успеваемости студентов и т. п.;
- проникать во внутренние информационные системы вуза;
- получать доступ к конфиденциальной информацией вуза, к персональным данным сотрудников, студентов, абитуриентов;
- атаковать пользователей приложения (сотрудников, студентов или абитуриентов), например похищать их учетные данные с помощью поддельной формы аутентификации или заражать рабочие станции вредоносным ПО;
- получать доступ к файлам на веб-сервере;
- нарушить работу веб-сервера.

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны РФ, ФСБ и ФСТЭК, продукция сертифицирована ФСТЭК и «Газпромом». 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.ru
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays