waves ENTERPRISE

Анализ безопасности корпоративных данных и инфраструктуры на блокчейн-платформе

2020

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Enterprise Blockchain Security

Waves Enterprise вывела на рынок корпоративную блокчейн-платформу, обеспечивающую крупным компаниям, а также государственным и общественным организациям, исключительный уровень безопасности и конфиденциальности данных.

wavesenterprise.com

IT

- Главный офис: Москва, Россия
- Год основания: 2018
- «Лабораторией Касперского» выполнен анализ защищенности блокчейн-приложений

Waves Enterprise, гибридная блокчейн-платформа, сочетает эксклюзивную публичную и приватную сети и предоставляет возможность модульного шифрования. Платформа готова к сертификации государственными и другими регулирующими органами. При интеграции в существующую IT-инфраструктуру решение Waves Enterprise предоставит преимущества блокчейна корпоративным клиентам, а также общественным службам, государственным цифровым сервисам и умным городам.

Безопасные обработка и хранение конфиденциальной информации о людях, активах и операциях – важные функции любой крупной организации. Решения на базе блокчейна помогут упростить реализацию этих функций и добиться максимальной эффективности административных процессов. Это позволит минимизировать бюрократию и повысить прозрачность и надежность операций обработки данных, что выгодно всем пользователям.

Артем Калихов, директор по продукту Waves Enterprise, объясняет: «Когда речь идет о миллионах записей, главным приоритетом является безопасность. Данные как государственных, так и коммерческих организаций должны быть надежно защищены от несанкционированного доступа и изменения – игнорировать этот вопрос нельзя.

Мы предлагаем нашим клиентам сочетание технологии блокчейн и настраиваемых возможностей криптографии, где блокчейн отвечает за неизменность записей, а модуль шифрования обеспечивает необходимый уровень защиты важной и конфиденциальной информации. Наше решение содержит все необходимые компоненты, снабжено полным пакетом документации и готово к государственной сертификации, что позволит потенциальным клиентам избежать задержек с развертыванием».

Повышение надежности систем

В государственном и коммерческом секторах нарушение безопасности может негативно сказаться на больших объемах конфиденциальных данных и цифровых активов.

По своей природе технология блокчейн обеспечивает неизменность запротоколированных операций и обладает преимуществами с точки зрения конфиденциальности. Однако и блокчейн не застрахован от недочетов и ошибок в коде приложения и инфраструктуре.

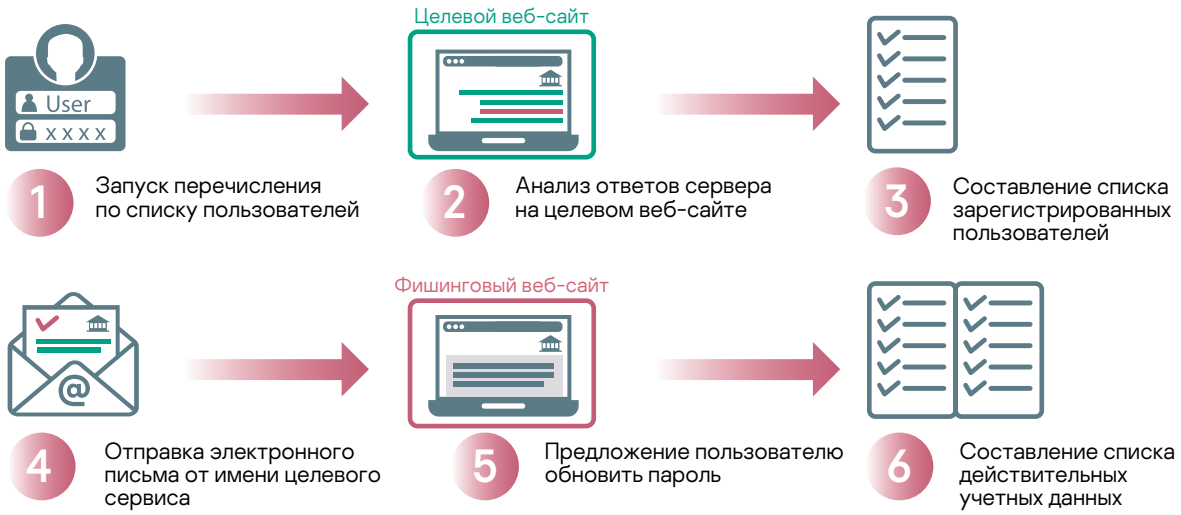
«Платформа Waves Enterprise и базирующиеся на ней децентрализованные приложения предназначаются для хранения и передачи конфиденциальных данных. Учитывая риски, которые может представлять использование этих приложений, с целью полноценной реализации заявленных возможностей нашего решения мы включили в жизненный цикл разработки контроль и повышение уровня безопасности приложений на платформе.

Чтобы обеспечить стабильность работы платформы Waves Enterprise, мы обратились к "Лаборатории Касперского", признанному эксперту в области кибербезопасности, для тщательного тестирования компонентов нашего решения, включая узлы сети, службу авторизации и код клиентской части. Как нам известно, "Лаборатория Касперского" обладает практическим опытом обеспечения безопасности для разных систем, в частности для распределенных реестров (DLT), и уже неоднократно проводила аудит безопасности блокчейн-платформ», – заявил Артем Калихов.

«Чтобы обеспечить стабильность работы платформы Waves Enterprise, мы обратились к "Лаборатории Касперского", признанному эксперту в области кибербезопасности, для тщательного тестирования компонентов нашего решения, включая узлы сети, службу авторизации и код клиентской части. Как нам известно, "Лаборатория Касперского" обладает практическим опытом обеспечения безопасности для разных систем, в частности для распределенных реестров (DLT), и уже неоднократно проводила аудит безопасности блокчейн-платформ».

Артем Калихов, директор по продукту Waves Enterprise

Как происходит атака перечислением



«Атака перечислением – полезный прием для выявления уязвимостей веб-приложения. Этот приём часто используют на страницах входа на сайт, регистрационных форм или сброса пароля. Злоумышленники ищут различия в ответах сервера в зависимости от вводимых учетных данных. Анализируя различные сценарии, они определяют, зарегистрирован ли в системе тот или иной электронный адрес, и составляют список действительных пользователей. Затем злоумышленники могут осуществлять фишинговые атаки, отправляя на эти электронные адреса письма якобы от имени скомпрометированного сервиса, содержащие запрос информации или предложение выполнить действия, в результате которых действительные учетные данные будут раскрыты неавторизованным лицам».

Павел Покровский, руководитель направления Blockchain Security «Лаборатории Касперского»

ПРОВЕРКА
Анализ кода «Лабораторией Касперского» – важный этап перед релизом версии 1.2 платформы Waves Enterprise в марте 2020 г.

ДЕМОНСТРАЦИЯ
Демонстрация «Лаборатории Касперского» включает различные сценарии с использованием найденных уязвимостей и иллюстрирует их влияние на платформу Waves Enterprise.

РЕСУРСЫ
«Лаборатория Касперского» предоставила Waves Enterprise полезные нагрузки и сценарии атак для интеграции в автоматизированные инструменты тестирования на этапе восстановления.

Выбор подходящего решения: белый, серый или черный ящик

«Мы начали **анализ защищенности приложений** с развертывания и конфигурирования тестовой системы. В нашем случае "Лаборатория Касперского" предложила использовать методы "черного ящика" и "серого ящика": тестирование на проникновение сначала в роли стороннего атакующего, а затем в роли легитимного пользователя», – рассказал Артем Калихов.

«Мы выбираем подходящее решение в зависимости от потребностей клиента. **Анализ защищенности приложений** подразумевает 3 основных варианта тестирования: **белый ящик,** когда осуществляется аудит исходного кода, **серый ящик,** когда проводится имитация атаки со стороны легитимного пользователя сервиса, и **черный ящик,** когда тестируется устойчивость к сторонним атакам. Эти варианты подразумевают разные время- и трудозатраты, и, соответственно, различается и их стоимость», – прокомментировал Павел Покровский, руководитель направления группы Blockchain Security в «Лаборатории Касперского».

«Мы высоко оценили тот факт, что "Лаборатория Касперского" четко определила рамки анализа и предложила набор услуг, идеальный по соотношению "цена-качество". Это способствовало созданию исключительно профессиональной атмосферы», – резюмировал директор по продукту Waves Enterprise.

Результат анализа

Артем Калихов осветил некоторые аспекты проведенной проверки: «Анализ выявил несколько уязвимостей, которые негативно сказались бы на надежности платформы и на безопасности базирующихся на ней приложений. Эксперты "Лаборатории Касперского" провели демонстрацию, показав нам в подробностях каждую уязвимость и ее влияние на систему. Критические уязвимости были обнаружены в инфраструктуре платформы, операционных системах, используемых в образах Docker, а также в сторонних библиотеках. Если бы эти недочеты не были устранены, это могло бы повлечь за собой DoS-атаки, а также несанкционированное раскрытие данных».

«Атака перечислением – полезный прием для выявления уязвимостей веб-приложения. Этот приём часто используют на страницах входа на сайт, регистрационных форм или сброса пароля. Злоумышленники ищут различия в ответах сервера в зависимости от вводимых учетных данных. Анализируя различные сценарии, они определяют, зарегистрирован ли в системе тот или иной электронный адрес, и составляют список действительных пользователей. Затем злоумышленники могут осуществлять фишинговые атаки, отправляя на эти электронные адреса письма якобы от имени скомпрометированного сервиса, содержащие запрос информации или предложение выполнить действия, в результате которых действительные учетные данные будут раскрыты неавторизованным лицам, – рассказывает Павел Покровский. – Исследуя функцию "Забыли пароль?", мы выявили ее уязвимость к атаке перечислением, которая позволила бы атакующим определять действительные имена пользователей Waves Enterprise через веб-приложение».

«Если говорить вкратце, для устранения этой проблемы требуется, чтобы сервер отправлял ответы без подробной информации. Но проектировщики интерфейса стараются сделать приложение максимально простым и понятным для пользователя, и иногда соображения удобства у них превалируют над основами безопасности. Соблюдать баланс между удобством использования и безопасностью действительно необходимо, но в случае служб авторизации безопасность всегда должна стоять на первом месте. Именно поэтому мы прибегли к помощи независимых экспертов по безопасности для оценки того, **как наше приложение может сопротивляться атакам злоумышленников,** чтобы необходимый баланс был соблюден буквально в каждой строке кода», – пояснил Артем Калихов.

Безопасный жизненный цикл разработки: вклад экспертов

«Уязвимости могут возникать на каждом этапе процесса разработки. В Waves Enterprise мы внедрили безопасный жизненный цикл разработки, чтобы полностью оправдать ожидания наших клиентов в плане надежности платформы. Сотрудничество с "Лабораторией Касперского", ведущим экспертом в сфере кибербезопасности, является частью нашей стратегии предоставления безопасных блокчейн-решений для коммерческого и государственного сектора».

Важным итогом нашего сотрудничества с "Лабораторией Касперского" является вклад экспертов компании в наш безопасный жизненный цикл разработки. Они поделились с нами целым набором инструментов, включающим полезные нагрузки и тестовые сценарии атак, которые мы смогли встроить в наши собственные автоматизированные инструменты тестирования.

Мы очень высоко оценили гибкость и качество поддержки, оказанной нам экспертами "Лаборатории Касперского". По их рекомендациям мы быстро устранили все обнаруженные уязвимости. Повторный **анализ подтвердил достаточный уровень безопасности нашей платформы,** так что теперь мы уверены в том, что не создаем рисков для наших клиентов. Анализ и рекомендации "Лаборатории Касперского" дополнительно подтверждают безопасность платформы Waves Enterprise и помогают укрепить уверенность в нашей сети», – подытожил Артем Калихов.