КРОК

02.4.6

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РЕШЕНИЯ КРОК ДЛЯ ЗАЩИТЫ КОРПОРАТИВНЫХ РЕСУРСОВ ОТ DDOS-АТАК

DDoS-атака (Distributed Denial of Service) – имеет целью заблокировать или максимально затруднить легитимным пользователям доступ к предоставляемым системой ресурсам и сервисам. DDoS-атака может быть направлена на заполнение полосы пропускания, исчерпание ресурсов атакуемого сервиса, исчерпание ресурсов операционной системы и ресурсов приложения.

В результате простоя сервисов, вызванных DDoS-атаками, организации несут финансовые потери, а также теряют репутацию в глазах клиентов.

Возможные объекты DDoS-атак:

- интернет-магазины;
- системы электронных платежей;
- системы дистанционного банковского обслуживания;
- социальные медиасервисы;
- сервисы провайдеров услуг фиксированной и мобильной связи;
- сервисы хостинг-провайдеров;
- электронные торговые площадки;
- сайты органов государственной власти.

02.4.6

Примеры недавних DDoS-атак:

- В 2016 г. во время олимпийских игр в Рио была зарегистрирована DDoS-атака мощностью 579 гигабит в секунду;
- В 2016 г. на фоне политических событий в Турции компания RT (ранее Russia Today – «Россия сегодня») подверглась многоэтапной DDoS-атаке, длившейся более недели, и затронувшей серверы компании в ряде стран мира;
- В 2015 году каждый четвертый российский банк столкнулся с DDoS-атакой, в ряде случаев, мощностью до 40 Гбит\с. При этом часть злоумышленников требовали заплатить крупную сумму в криптовалюте (BTC) за прекращение атаки;
- В 2014 г. целью DDoS-атак стали Банк России, Сбербанк, Газпромбанк, Альфа-банк и «ВТБ 24». В результате доступ к их сайтам и интернет-сервисам был временно заблокирован, в ряде случаев оказались недоступны сети банкоматов.
- В 2014 году многочисленным атакам подверглись новостные и медиа-ресурсы, правительственные сайты РФ: официальные сайты Первого канала, «Российской газеты», Ленты.ру, журналов «Эксперт» и «Русский репортер», Kremlin.ru и многих других коммерческих и государственных учреждений. Помимо того, что эти ресурсы оказывались недоступны, в ряде случаев злоумышленники изменяли их контент, размещая компрометирующую информацию.

УСЛУГИ КРОК

Компания КРОК оказывает следующие услуги по обеспечению защиты корпоративных интернет-ресурсов от DDoS-атак.

- **Анализ защищенности корпоративных интернет-ресурсов и устойчивости их к DDoS-атакам**: интервьюирование специалистов заказчика, анализ документации, структур и конфигурации интернет-ресурсов, проведение инструментального анализа защищенности. Результатом работ являет отчет, включающий рекомендации по нейтрализации выявленных уязвимостей.
- **Разработка политики безопасности**, соответствующей требованиям заказчика к уровню доступности ресурсов, основанная на передовом международном опыте защиты интернет-ресурсов.
- **Разработка процедур, определяющих порядок реагирования на DDoS-атаки**. Документ устанавливает ответственность, полномочия, схемы взаимодействия подразделений компании заказчика, а также возможные технические методы и средства реагирования в сложившихся условиях.

ПРЕИМУЩЕСТВА КРОК

Широкая компетенция

КРОК работает на ИТ-рынке с 1992 года и сегодня входит в топ-10 крупнейших ИТ-компаний и топ-3 консалтинговых компаний России (РА «Эксперт», «Коммерсант-Деньги», РИА Рейтинг).

КРОК – № 1 среди поставщиков ИТ-услуг в стране, лидирует в сфере управления приложениями (PAC), ИТ-аутсорсинга, в сегментах BI- и ERP-решений, на рынке систем электронного документооборота (TAdviser), в области телекоммуникаций (РА «Эксперт») и видеоконференцсвязи (TAdviser), а также комплексных проектов построения инфраструктуры ЦОДов, зданий и сооружений (CNews).

В области информационной безопасности КРОК предлагает полный спектр услуг от аудита информационных систем и создания корпоративной политики ИБ до внедрения, интеграции и поддержки технических решений. Компания создает системы для управления идентификационными данными и доступом (IAM), строит ситуационные и аутентификационные центры, обеспечивает сетевую безопасность и фильтрацию web-трафика, защищает корпорации от утечек информации (DLP), мошенников (anti-fraud) вирусов и спама, помогает контролировать целостность программных сред и доступ к периферийным устройствам и приложениям.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

ПРЕИМУЩЕСТВА КРОК

Квалификация, подтвержденная международными сертификатами

Квалификация специалистов КРОК подтверждена международными сертификатами Lead Auditor (British Standards Institution) SANS GIAC, CISA (ISACA) и CISSP (ISC2), лицензиями ФСТЭК и ФСБ России, сертификатами ведущих производителей оборудования и программного обеспечения, включая Kaspersky Lab DDoS Prevention Certified Professional, Arbor Certified Pravail APS Specialist, Radware Certified Solution Expert, CheckPoint Certified Security Expert (CCSE), Cisco Certified Internetwork Expert (CCIE) и других.

По информационной безопасности компания КРОК входит в состав Сообщества пользователей стандартов ЦБ РФ по обеспечению информационной безопасности организаций банковской системы РФ (Сообщество ABISS). КРОК также является участником партнерской программы BSI «Ассоциированная программа консультантов BSI», подтверждающей высокий статус специалистов компании по внедрению систем менеджмента по направлениям «Информационная безопасность» (ISO 27001), «Непрерывность бизнеса» (ISO 22301), «Управление ИТ-сервисами» (ISO 20000-1).

ОСНОВНЫЕ ПАРТНЕРЫ

Arbor Networks – Официальный партнер.
Check Point. КРОК – Авторизованный партнер уровня Skilled Partner (3 stars).
Qrator Labs – Продуктивный партнер.
Radware – партнер.
Лаборатория Касперского – Платиновый партнер.
МФИ Софт – Официальный партнер.

- **Проектирование, внедрение и техническая поддержка систем защиты корпоративных интернет-ресурсов**:
  - Многоуровневые решения, ориентированные на сервис-провайдеров и крупные промышленные предприятия. Принцип работы заключается в сборе и анализе трафика с телекоммуникационного оборудования заказчика с последующей передачей команды на обработку трафика платформе, осуществляющей непосредственно очистку трафика от паразитных пакетов.
  - Системы обнаружения и предотвращения атак с возможностями автоматической защиты. В отличие от классических систем, которые полагаются только на статические сигнатуры, данные решения обеспечивает уникальный метод на основе поведенческого анализа и автоматически генерирует сигнатуры в реальном времени, чтобы предотвращать атаки, не основанные на уязвимостях приложений.
  - При невозможности создания собственных систем защиты от DDoS-атак, компания КРОК предоставляет услуги по распределенной фильтрации трафика, позволяющие выдержать DDoS-атаки практически любой мощности, в том числе направленные на исчерпание полосы пропускания.
- **Размещение корпоративных интернет-ресурсов заказчиков в защищенном виртуальном дата-центре КРОК**. Обеспечивается два уровня защиты от DDoS-атак:
  - базовые меры включают межсетевое экранирование и системы предотвращения вторжений для фильтрации паразитного трафика на уровне узла доступа в Интернет, а также оптимизацию настроек ресурсов, кластеризацию оборудования и использование резервных производительных каналов связи, регулярный мониторинг работы ресурсов и своевременное обнаружение атак;
  - индивидуальные меры информационной безопасности определяются в соответствии с потребностями заказчика и включают в себя дополнительные услуги по защите от DDoS-атак.

ПРОЕКТНЫЙ ОПЫТ

Сеть магазинов бытовой техники и электроники «Эльдорадо»

Защита интернет-магазина от хакерских и DDoS-атак

Специалисты КРОК совместно с Qrator Labs обеспечили круглосуточную защиту интернет-магазина «Эльдорадо», которая в автоматическом режиме отражает все хакерские и DDoS-атаки. Это позволяет ритейлеру не терять ни единого покупателя даже в самые «горячие» сезоны. В 2015 году проект получил премию «ИТ-Лидер».

Основные преимущества:

- предварительный анализ позволил выявить и оперативно устранить критические уязвимости в ПО интернет-магазина;
- система в автоматическом режиме противостоит DDoS-атакам и отражает хакерские активности, многие из которых планируются с учетом технических особенностей интернет-платформы заказчика;
- за первые полтора года нейтрализовано 5 крупных DDoS-атак (до 15 тысяч ботов, максимальная полоса атаки – 2,3 Гбит/с), блокировано свыше 320 тысяч хакерских активностей.

ПРЕИМУЩЕСТВА КРОК

Виртуальный дата-центр КРОК

КРОК – первая российская ИТ-компания, предлагающая облачные сервисы на базе собственной разработки – «Облачной платформы КРОК». КРОК имеет большой опыт проектов по виртуализации вычислительных комплексов, созданию систем распределенных вычислений. Все облачные сервисы компании КРОК реализуются на базе собственного центра обработки данных.

ЦОД КРОК удовлетворяет требованиям к инженерным системам не ниже Tier III.

- ЦОД обладает надежной, зарезервированной системой энергообеспечения с собственной распределительной подстанцией и генераторной установкой, современной системой кондиционирования с жестким контролем параметров климатического режима, многоуровневой системой безопасности.
- Физическая безопасность обеспечивается жестким контролем доступа в здание, в помещение ЦОДа и к оборудованию.
- Информационная безопасность обеспечивается межсетевым экранированием сегментов, шифрованием каналов передачи данных, анализом событий информационной безопасности.
- Мониторинг жизнеобеспечивающих систем ЦОДа ведется в режиме 24x7.

КРОК

111033, Москва, ул. Волочаевская, д.5, к.1,
T: (495) 974 2274 I Ф: (495) 974 2277
E-mail: infosec@croc.ru
slideshare.net/croc-library
cloud.croc.ru
croc.ru