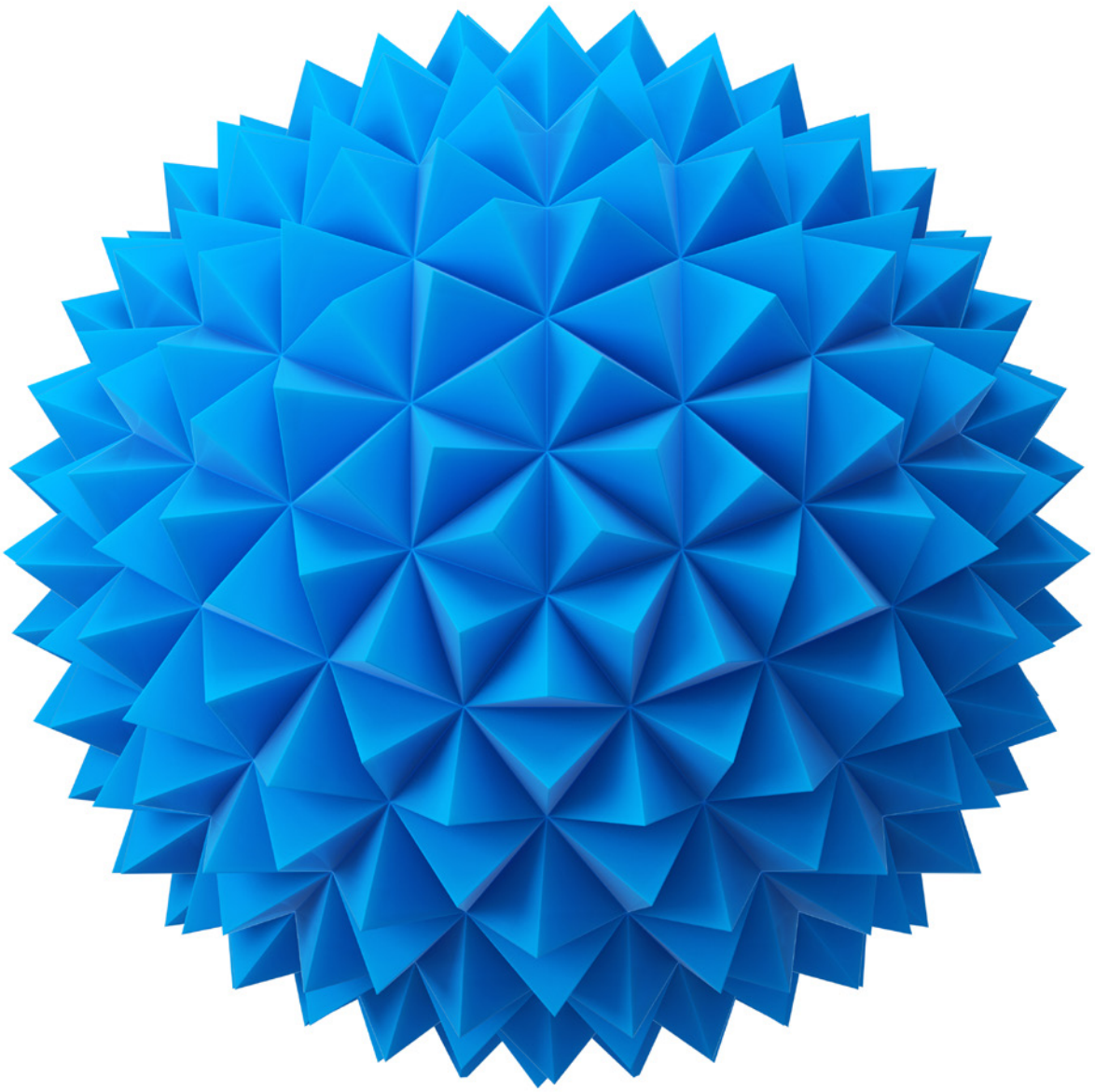
Deloitte.



DDoS-тестирование и моделирование атак

Что это?

DDoS-атака (Distributed Denial of Service) – это разновидность злонамеренной деятельности, которая является одной из самых распространенных и опасных сетевых атак, имеющих целью довести компьютерную систему до состояния, когда она не сможет обслуживать законных пользователей или правильно выполнять возложенные на нее функции. Успех атак этого типа основан на ограничении пропускной способности, которая является одной из характеристик любого сетевого ресурса, например, инфраструктуры, поддерживающей веб-сайт компании.

Во время DDoS-атаки на веб-ресурс направляется большое количество фальшивых запросов с целью исчерпать вычислительные возможности обработки данных и нарушить его нормальное функционирование. Таким образом, в результате атаки нарушается или полностью блокируется обслуживание простого пользователя. А это грозит простоями сервиса, репутационными рисками, потерей посетителей/клиентов и, в конце концов, убытками.

Зачем это нужно?

DDoS-атаки в первую очередь направлены на дестабилизацию бизнеса компании. Наилучший способ минимизировать ущерб от DDoS-атак – это иметь четкий план действий.

Разработанная компанией «Делойт» Практика тестирования эффективности вашей защиты от DDoS-атак и моделирования реальных современных DDos-атак позволит максимально снизить уязвимость ваших сервисов, решить ряд проблем и ликвидировать или свести к минимуму последствия, с которыми сталкивается компания в случае DDoS-атаки, а именно:

- **риск репутационных потерь,** когда огласка информации о возможном взломе или компрометации информационной системы может привести к снижению имиджа компании на рынке;
- **риск оттока клиентов** в случае недоступности сервиса и повышения обеспокоенности защищенностью систем;
- **влияние на финансовые показатели,** когда нарушение работы сервиса может приводить к прямым и косвенным финансовым потерям компании.

Как осуществляется (этапы)?

Практика проведения DDoS-тестирования и моделирования атак содержит определенные этапы, основными заданиями которых являются:

- Оценка эффективности имеющихся средств защиты и взаимодействия подразделений заказчика по выявлению и блокированию DDoS-атак
- Аналитика и рекомендации по повышению защищенности от DDoS-атак

На первом этапе

проведения работ происходит получение информации от Заказчика, которая содержит:

- анкетирование;
- определение типов атак;
- определение условия тестирования;
- определение объектов тестирования;
- дополнительную информацию об элементах инфраструктуры;
- согласование критериев успешности DDoS-атаки.

Второй этап

заключается в формировании и согласовании методики тестирования:

- условия тестирования;
- предельные нагрузки;
- список тестируемых узлов;
- список атак для каждого узла;
- параметры проведения каждой атаки;
- настройка систем защиты;
- настройка средств регистрации событий и мониторинга.

Подготовка к проведению работ:

- проверка работоспособности инструментов для проведения атак и систем мониторинга;
- проверка доступности узлов и серверов;
- проверка синхронизации всех узлов по времени.

Третий этап

является непосредственным проведением тестирования с моделированием реальных DDoS-атак, которые контролируются специалистами «Делойт», происходит фиксация и обработка результатов.

По результатам тестирования формируется отчет, который содержит аналитические оценки устойчивости прикладных систем и сетевой инфраструктуры к DDoS-атакам, оценки взаимодействия подразделений в условиях атаки, результаты DDoS-атаки, выводы и рекомендации по повышению защищенности от DDoS-атак.

Результат (что получит заказчик)?

Практика DDoS-тестирования компании «Делойт» направлена на повышение защищенности и устойчивости ваших сервисов, которая содержит:

- определение текущих предельных значений нагрузки на внешние веб-сервисы;
- проверку устойчивости внешних веб-сервисов к распределенным атакам, направленным на отказ в обслуживании;
- проверку устойчивости внешних ресурсов ИС к распределенным атакам, направленным на отказ в обслуживании;
- оценки эффективности имеющихся средств защиты против DDoS-атак;
- оценку эффективности взаимодействия подразделений заказчика по выявлению и блокированию DDoS-атак;
- повышение осведомленности сотрудников заказчика по взаимодействию при DDoS-атаках и противодействию этому типу угроз;
- рекомендации по повышению защищенности информационных систем (ИС) от DDoS-атак.

Благодаря комплексному объединению людей, методологии и технологий мы можем обеспечить быструю и эффективную способность реагировать на возможные DDoS-атаки, чтобы исключить или минимизировать ущерб от них. Четкое понимание ключевых рисков и потребностей компании делает практику «Делойт» уникальным инструментом, внедрив который, компания получит ряд конкурентных преимуществ:

- уменьшение рисков недоступности сервисов и потери данных;
- сокращение затрат на восстановление после DDoS-атак;
- проактивное, а не реактивное реагирование на DDoS-атаки;
- интеллектуальное расследование, которое позволяет понять природу DDoS-атак благодаря современным и передовым инструментам;
- управление в условиях кризисных ситуаций.

Почему «Делойт»?

Мы обладаем знаниями наилучших практик (Cobit), стандартов информационной безопасности и практическим опытом производства (ISO/IEC 27001, ISO/IEC 27002, NIST).

Также наша команда обладает рядом техник для сбора и анализа данных по многим операционным системам и ИТ-архитектурам, используя сочетание широко принятых инструментов и собственного разработанного ПО.

Команда имеет возможность эффективно собирать данные из множества сред, в том числе Windows, Mac OS X, Linux и мобильных платформ, таких как Android и iOS.

Мы используем общепринятые инструменты и методы для сбора и изучения данных по этим операционным системам.

Эти инструменты содержат как коммерческие (EnCase, Forensic Toolkit (FTK), HB Gary, Paraben, Mandiant, Bit9, NetWitness, Internet Evidence Finder, Hardware Write Block/Disk Duplicator), так и бесплатные решения (SANS Investigative Forensic Toolkit (SIFT), SANS Network Investigative Forensic Toolkit (SNIFT), Sleuthkit, Log2timeline, Autopsy, Registry Ripper, Sysinternals, Network Miner).

Команда «Делойт» – это сертифицированные специалисты в области информационной безопасности (CISM), кибербезопасности (CSX) и защиты от DDoS-атак как частичного направления.

deloitte.by

О «Делойт»

Наименование «Делойт» относится к одному либо любому количеству юридических лиц, включая их аффилированные лица, совместно входящих в «Делойт Туш Томацу Лимитед», частную компанию с ответственностью участников в гарантированных ими пределах, зарегистрированную в соответствии с законодательством Великобритании (далее — ДТТЛ). Каждое такое юридическое лицо является самостоятельным и независимым юридическим лицом. ДТТЛ (также именуемая «международная сеть «Делойт») не предоставляет услуги клиентам напрямую. Подробная информация о юридической структуре ДТТЛ и входящих в нее юридических лиц представлена на сайте www.deloitte.com/about.

«Делойт» предоставляет услуги в области аудита, консалтинга, финансового консультирования, управления рисками, налогообложения и иные услуги государственным и частным компаниям, работающим в различных отраслях экономики. «Делойт» — международная сеть компаний, в число клиентов которой входят около четырехсот из пятисот крупнейших компаний мира по версии журнала Fortune. «Делойт» имеет многолетний опыт практической работы при обслуживании клиентов в любых сферах деятельности более чем в 150 странах мира и использует свои обширные отраслевые знания и опыт оказания высококачественных услуг для решения самых сложных бизнес-задач клиентов. Более 244 тысяч специалистов «Делойта» по всему миру привержены идеям достижения результатов, которыми мы можем гордиться. Для получения более подробной информации заходите на нашу страницу в Facebook, LinkedIn или Twitter.

Настоящее сообщение содержит информацию только общего характера. При этом ни компания «Делойт Туш Томацу Лимитед», ни входящие в нее юридические лица, ни их аффилированные лица (далее — «сеть «Делойт») не представляют посредством данного сообщения каких-либо консультаций или услуг профессионального характера. Прежде чем принять какое-либо решение или предпринять какие-либо действия, которые могут отразиться на вашем финансовом положении или состоянии дел, проконсультируйтесь с квалифицированным специалистом. Ни одно из юридических лиц, входящих в сеть «Делойт», не несет ответственности за какие-либо убытки, понесенные любым лицом, использующим настоящее сообщение.

© 2017 Иностранное унитарное предприятие «Делойт и Туш». Все права защищены.