Безопасный веб для владельцев сайтов

Ваш сайт тормозит из-за атаки или из-за того что стал популярнее?

Может это и вовсе не DDoS, даже админы с опытом работы могут решить, что началась атака, если к ним пришли по ссылке из FB в 2 раза больше пользователей, чем обычно. И это наша работа отличать DDoS от нагрузки.

Подключайте систему защиты от DDoS с кешированием →

Сейчас каждый достаточно просто может создать свой сайт, но не так-то просто обеспечивать его безопасность и стабильность в условиях нарастания массива кибер-атак. Чтобы защитить свой вебсайт, вам нужно учитывать его технические настройки, программное обеспечение которое вы использовали при создания сайта, контент сайта, а также разного рода плагины и расширения, которые вы установили для расширения возможностей вашего сайта. Главное, что вам нужно иметь план на случай непредвиденных обстоятельств. Этот план должен включать:

- **Регулярное создание резервных копий файлов и баз данных, на случай если эти данные потеряются из-за технической проблемы или атаки;**
- **Знать условия пользования сервисом вашего хостинг-провайдера и степень его готовности защитить вас во время атаки;**
- **Знать условия пользования сервисом и опции безопасности вашего провайдера доменных имен (DNS-провайдера);**
- **Внедрение решений для смягчения атак, заблаговременно.**

Для владельцев сайтов, далеких от IT

Шаг 1. Свяжитесь с лицом, которое может помочь с вашим сайтом (вашим веб-мастером, людьми, которые помогли вам настроить ваш сайт) или на биржах фриланса наймите админа.

Шаг 2. Обратитесь в клиентский отдел к своему хостинг провайдеру, у которого вы приобрели домен (например, REG.ru, Beget, Timeweb) и измените «Время жизни» (TTL) на 1 час. Это может помочь вам намного быстрее перенаправить ваш сайт, когда он подвергнется атаке (по умолчанию 72 часа или три дня). Этот параметр часто можно найти в «дополнительных» свойствах вашего домена, иногда тип SOA в записях вашего DNS или служебных записях. Если вы поздно отреагировали и атака началась, иногда спасает решение временно сменить провайдера. Это позволит частично снизить влияние возможных новых атак, ведущихся в адрес вашего сайта. Подключить дополнительный IP вам поможет клиентская служба хостинга.

Шаг 3. Обратитесь к профильному оператору защиты от DDoS-атак.*

Шаг 4. Как только вы восстановите контроль, пересмотрите свои риски и потребности и сделайте выбор между безопасным хостинг-провайдером и/или продолжайте пользоваться услугами у специализированного сервиса защиты от DDoS-атак.

*Когда выбираете оператора защиты, важно учитывать, что у некоторых основная деятельность это облачный dns хостинг и CDN, и предлагаемая защита от DDoS по сути номинальная услуга.

Для осведомленных и уверенных

- Настроить кеширование (либо nginx fastcgi либо плагины типа Wordpress super-cache).
- Анализировать логи и писать правила, если нападающий бьёт в поиск, отключите поиск для всех.
- Следить, чтобы ресурсов сервера было достаточно - если у вас самый дешёвый хостинг или сервер на 1,5 ядра с 0 гигабайт оперативной памяти, то не то что самостоятельно защитится, а защитился вообще не получится - атаку обычно не получается выявить и заблокировать моментально.
- Блокировать ботов с помощью инструментов fail2ban, который создает правила для iptables. Анализируя журналы, fail2ban обнаруживает повторяющиеся неудачные попытки аутентификации и автоматически устанавливает правила брандмауэра для отбрасывания трафика, исходящего с IP-адреса злоумышленника. Также обратите внимание, что бан происходит после записи журнала. Медленному процессору могут потребоваться часы, чтобы догнать его до реального времени. Обязательно убедитесь, чтобы ресурсов системы на это хватало - парсить логи и банить/разбанивать тысячи ботов - очень ресурсоёмкая операция, и важно не забанить самих себя.
- Настройте мониторинг доступности сайта (от Яндекс.Метрики до Uptimerobot / Statuscake) при этом проверяйте или код ответа (должен быть 200), а ещё лучше текст на странице (если там нет такой-то фразы, то скорее всего вместо страницы выдаётся ошибка).
- Научитесь собирать метрики и читать их, чтобы понять хватает ли серверу ресурсов для ежедневной работы и какой запас есть.
- На каких-то платформах это уже встроено и есть по-умолчанию, где-то можно включить дополнительные опции https://www.digitalocean.com/products/monitoring/
- Где-то можно установить внешние сервисы newrelic / datadog

Помните, что если в сайт влетает сотня гигабит атакующего трафика, то отбиться от такого самостоятельно очень сложно, скорее всего ваш сервер просто отключит провайдер, чтобы другие пользователи "рядом" не страдали.

Поэтому часто все эти шаги эффективны не ВМЕСТО а ВМЕСТЕ с системой защиты от DDoS, при подключении которой есть шанс, что это всё может и не понадобиться, а значит можно не быть системным администратором или оплатить им меньше часов.

Подключить сейчас защиту от кибер неприятностей →

Поэтому часто все эти шаги эффективны не ВМЕСТО а ВМЕСТЕ с системой защиты от DDoS, при подключении которой есть шанс, что это всё может и не понадобиться, а значит можно не быть системным администратором или оплатить им меньше часов.

Самостоятельно построить защиту

Сборка собственного программно-аппаратного комплекса для защиты сайта имеет смысл только для очень крупных компаний, располагающих многомиллионными бюджетами. Кроме финансовых затрат и расхода времени на закупку и настройку оборудования и ПО, надо также содержать специалистов по безопасности и постоянно поддерживать их знания и навыки на должном уровне.

Даже высококлассный комплекс защиты будет неэффективным, если атака превышает по мощности емкость интернет-канала, через который комплекс подключен к интернету. По этой причине крупнейшие компании используют одновременно несколько защитных систем, включая защиту каналов у операторов связи.

Собственный защитный комплекс никогда себя не окупит — нападения не происходят постоянно, инфраструктура устаревает, а хакеры постоянно наращивают мощность атак.

Поэтому сейчас даже крупный бизнес передает защиту веб-ресурсов на аутсорсинг. Использование сервисов защиты по модели SaaS (программное обеспечение как сервис) позволяет быстро получить услугу без сложной технической интеграции, а расходы на апгрейд инфраструктуры и развитие средств защиты берет на себя провайдер защиты.

Как работает облачная защита

Безопасное «облако» ускоряет доставку контента сайта и отражает нелегитимный трафик, не пропуская его на сервер клиента. Это обеспечивает непрерывную и быструю работу находящихся под защитой сайтов.

Узнать больше на сайте deflect.ca →