**Рекомендации по мерам для снижения риска кибератак**

**типа DNS Traffic Amplification.**

Амплификация DNS - это распределенная атака типа «отказ в обслуживании» ( [DDoS](https://www.imperva.com/learn/application-security/denial-of-service/) ), при которой злоумышленник использует уязвимости в серверах системы доменных имен (DNS), чтобы превратить изначально небольшие запросы в гораздо более крупные, усиливая атаки на серверы жертвы.

Усиление DNS - это тип отражающей атаки, которая манипулирует общедоступными системами доменных имен, заставляя их наводнять цель большим количеством пакетов UDP. Используя различные методы усиления, злоумышленники могут «раздувать» размер этих UDP-пакетов, делая атаку настолько мощной, что она может вывести из строя даже самую надежную интернет-инфраструктуру.

**Общие рекомендации для клиентов А1.**

1) Убедиться в необходимости работы своего сервиса DNS

DNS сервис может использоваться как:

* авторитативный, если в вашей инфраструктуре есть сервисы (вы их владелец), доступ к которым осуществляется для его пользователей по доменному имени и ваш авторитативный DNS отвечает адресом, по которому находится запрашиваемый сервис;
* рекурсивный, если пользователи вашей сети запрашивают адрес по имени чужого веб-ресурса (например, для пользователей офисной сети обработка запросов “где находится интернет ресурс”) и вы не можете использовать напрямую рекурсивный DNS провайдера А1 (например, у вас используется NAT и/или вам необходимы функции по специфической обработке DNS запросов таких, как ограничение доступа к некоторым ресурсам сети интернет для ваших пользователей и т.п.).

Если вам не требуется DNS сервис по вышеперечисленным причинам, крайне рекомендуем по возможности:

* остановить сервис DNS (на пограничном с оператором роутере, прокси и т.д.);
* удалить службу DNS-сервера из загрузочных скриптов системы;
* деинсталлировать DNS-сервер.

2) Если же роль DNS сервиса актуальна, то необходимо обеспечить максимальную защиту сервера от атак извне.

a) Ограничить доступ к DNS сервису, следуя принципам минимальной достаточности для выполнения сервисом DNS своей роли:

* если DNS-сервер исключительно авторитативный, то обработка рекурсивных запросов на нем не нужна. Он должен отвечать только на запросы по тем адресам, которые принадлежат вашим доменным именам и в случае, если соответствующая запись не найдена в своей зоне, не перенаправлять рекурсивные запросы к другим DNS сервисам;
* если DNS-сервер выполняет роль рекурсора для пользователей внутренней сети, доступ к его порту 53udp/tcp должен быть разрешен только для пользователей вашей внутренней сети. Крайне желательно средствами межсетевого экрана (VPN, наличия маршрутов/iptables/ipfw) ограничить полностью трафик в сторону вашего DNS по портам 53udp и 53tcp из сети интернет - он вам точно не нужен. Допускается настройка самого DNS, в котором следует определить ваши внутренние доверенные сети, запросы от которых будет обрабатывать ваш DNS;
* если ваш DNS выполняет сразу две роли - авторитатива и рекурсива, то крайне желательно разделить выполнение этих ролей двумя разными сервисами DNS, не совмещая эти роли в одном сервисе DNS и настроить каждый из них согласно настоящим рекомендациям. Если все же вы не можете разнести гибридные функции, то следует отдельно настроить средствами DNS правила обработки рекурсивных запросов только от внутренних сетей, а авторитативных от внутренней сети с использованием внутреннего адреса ресурса, от внешних сетей - с использованием публичного адреса ресурса с запретом рекурсии для таких запросов.

Общая рекомендация - по возможности осуществить переход на TCP протокол взаимодействия в рамках сервиса DNS.

b) Следует всегда использовать актуальные версии программного обеспечения DNS-серверов, своевременно устанавливать последние стабильные обновления и патчи на ОС, а также на используемые прикладные сервисы, устанавливать последние версии прошивок маршрутизаторов (при истечении сроков end-of-life поддержки производителем устройств маршрутизаторов следует заменять такие устройства на более новые, на которые производитель будет выпускать обновления еще в течении нескольких лет) с тем, чтобы злоумышленники не могли воспользоваться широко и давно известными уязвимостями устаревшей версии ПО (прошивки).

**Рекомендации для BIND**

 **Ограничение рекурсии**

Если DNS-сервер исключительно авторитативный, то обработка рекурсивных запросов на нем не нужна. Он должен отвечать только на запросы по своей зоне, не перенаправляя их.

Для этого в раздел *options* конфигурационного файла добавляются строки:

allow-recursion {"none";};

recursion no;

Если же сервер выполняет роль и авторитативного, и рекурсивного DNS, необходимо разрешить выполнять запросы только из доверенных подсетей, модифицируя конфигурационный файл следующим образом:

 acl "trusted\_ip" {
 192.168.0.0/16; //здесь ваши сети
 10.0.0.0/8; //здесь ваши сети
 localhost;
 };

 options {
<skipped>
 allow-recursion { trusted\_ip; };
 allow-query-cache { trusted\_ip; };
<skipped>
 };

**Дополнительно можно использовать параметры:**

 Разрешаем обычные запросы только из локальной сети.

 allow-query { localhost; trusted\_ip; };

 Перенаправляем запросы, которые не резолвит наш DNS, на DNS провайдера.

 Для примера 8.8.8.8 DNS серверы Google (крайне рекомендуем использовать DNS провайдера)

 forwarders { 8.8.8.8; }; //это пример крайнего случая!

 Скрываем версию BIND, вместо этого выводим указанную строку.

 version "DNS Server";

**Рекомендации для MikroTik Routers важно проверить настройки фаервола!**

Если необходимо отключить рекурсивные запросы для службы DNS необходимо выполнить команду:

/ip dns set allow-remote-requests=no

Если необходимо запретить доступ к DNS из сети Интернет можно добавить правило в firewall выполнив команду:

/ip firewall filter add action=drop chain=input dst-port=53 protocol=udp place-before=0 in-interface=указать wan порт обычно ether1

**Прочее**

В случае, когда под управлением администратора находится не сервер, а сетевое оборудование конечного пользователя (маршрутизаторы уровня доступа), необходимо убедиться в том, что функция DNS-relay не используется, либо не активирована на интерфейсе, доступном из Интернет. Также через внешний интерфейс не должна быть доступна функция управления устройством.