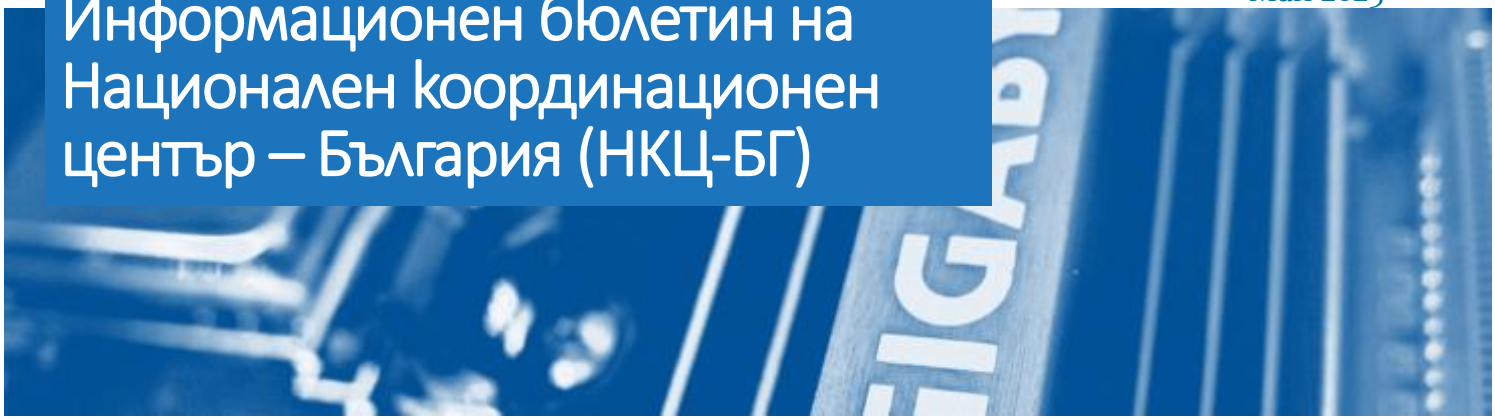
NCC-BG
NATIONAL COORDINATION CENTER
BULGARIA

Министерство на електронното управление

Съфинансирано от Европейския съюз

Информационен бюлетин на Национален координационен център – България (НКЦ-БГ)

Май 2025



ЗАЩИТАТА НА DNS – ПЪРВО НИВО НА ЗАЩИТА СРЕЩУ КИБЕРАТАКИ

Киберсигурността се фокусира върху защитните стени, антивирусния софтуер и откриването на крайни точки (endpoint detection). Въпреки че тези инструменти са от съществено значение, един критичен слой често се пренебрегва: системата за имена на домейни (DNS). Като отправна точка на почти всяко онлайн взаимодействие, DNS не е само фундаментална, а все по-често се превръща в цел на атакуващите. Когато не е защитена, се превръща в единична точка на отказ, която може да наруши услугите, да пренасочва потребители или да разкрие чувствителни данни. Защитата ѝ не е просто добра практика, а необходимост.

Системата за имена на домейни функционира като адресната книга на интернет. Тя преобразува лесни за запомняне имена на домейни (като example.com) в числови IP адреси (като 1.2.3.4), които компютрите използват, за да се идентифицират взаимно в мрежите. Всеки път, когато потребител посети уебсайт, отвори приложение или изпрати имейл, DNS заявка се задейства във фонов режим, за да свърже тази заявка с правилния сървър. Без DNS, потребителите трябва да запомнят сложни низове от числа за всяка онлайн дестинация. Въпреки че работи тихо и ефективно, DNS е от съществено значение за начина, по който навигираме в интернет.

НАЙ-ЧЕСТО СРЕЩАНИТЕ АТАКИ, БАЗИРАНИ НА DNS

DNS Spoofing – Препращане на потребители към фалшиви уебсайтове, които изглеждат истински.

DNS Hijacking – Промяна на DNS записи или настройки, за да се пренасочва трафикът през злонамерени сървъри.

DNS Tunneling – Скриване на откраднати данни в DNS трафика, за да се „промъкнат“ през защитните стени.

DDoS атаки върху DNS сървъри – Претоварване на DNS инфраструктурата, правейки уебсайтове и приложения недостъпни.



DNS: ОСНОВНА ЦЕЛ НА КИБЕРАТАКИТЕ

DNS може да изглежда като просто още един фонов процес – транслиране на имена на домейни, така че потребителите да могат да сърфират в интернет, без да въвеждат IP адреси. Но под това се крие критична система, която е цел на кибератаки. Това е така, защото DNS участва в почти всяко кликване, връзка и заявка, направени онлайн. Проблемът е, че DNS не е създаден с мисъл за сигурността. По-голямата част от DNS трафика е некриптиран, неудостоверен и до голяма степен невидим за традиционните инструменти за сигурност. Това го прави идеален канал за атакуващите да стартират скрити, силно въздействащи атаки – от тихи пренасочвания до пълномащабни прекъсвания на услугите.

ВАЖНИ ПОДОБРЕНИЯ В ЗАЩИТАТА НА DNS

DNSSEC (Разширения за сигурност на системата за имена на домейни) добавя криптографски подписи към DNS записите, гарантирайки, че отговорите, които потребителите получават, са автентични и непроменени. Без него, нападателите могат да подправят легитимно изглеждащи домейни и да пренасочват потребители към злонамерени дестинации с лекота. С активиран DNSSEC този риск е драстично намален.

Тъй като заплахите стават все по-сложни, криптирането на DNS заявки вече е критичен слой на защита. Някои доставчици на DNS хостинг поддържат DNS през HTTPS (DoH) и DNS през TLS (DoT), които помагат за предотвратяване на атаки от типа „man-in-the middle“ чрез криптиране на DNS заявки между клиента и резолвера. Това е особено важно в среди като обществен Wi-Fi, където некриптиран трафик може да бъде прихванат или подправен.

И тъй като DNS не е само за уебсайтове, а играе и ключова роля в доставката на имейли, съществуват и услуги за помагане защитата и на този процес. Потребителите могат лесно да създават и управляват SPF, DKIM и DMARC записи – основни DNS конфигурации, които помагат за предотвратяване на фишинг и спуфинг, като посочват кои пощенски сървъри са оторизирани да изпращат имейли от името на домейн. Някои доставчици на DNS хостинг предоставят възможността за улеснено задаване на по-сложни настройки, позволявайки на организациите да укрепят репутацията на домейна си и да подобрят доставяемостта на имейлите.

Киберзаплахите стават все по-напреднали, разчитането единствено на вътрешни защити вече не е достатъчно. DNS, като първа стъпка в почти всяко онлайн взаимодействие, играе критична роля в спирането на заплахите, преди да достигнат до мрежата. Когато е правилно защитен, DNS става нещо повече от инфраструктура – той се превръща в защита на първа линия. Приоритизирането на сигурността на DNS е от съществено значение за изграждането на устойчива дигитална основа.



СИГУРНОСТТА НА DNS Е ФУНДАМЕНТАЛНА, А НЕ ВЪПРОС НА ИЗБОР

Тъй като дигиталната инфраструктура става все по-сложна, DNS вече не е просто фонова услуга – той е критична контролна точка във всяко онлайн взаимодействие. DNS осигурява всичко от зареждане на уебсайтове и обработка на транзакции до изпращане на имейли и достъп до облачни ресурси. Обхватът му е огромен, както и потенциалното му въздействие, ако остане необезпечен. Когато е правилно защитен и наблюдаван, DNS става нещо повече от просто резолвер. Той действа като слой за ранно откриване, разкривайки подозрителни модели, злонамерени заявки и признаци на компрометиране, преди заплахите да ескалират.









Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/