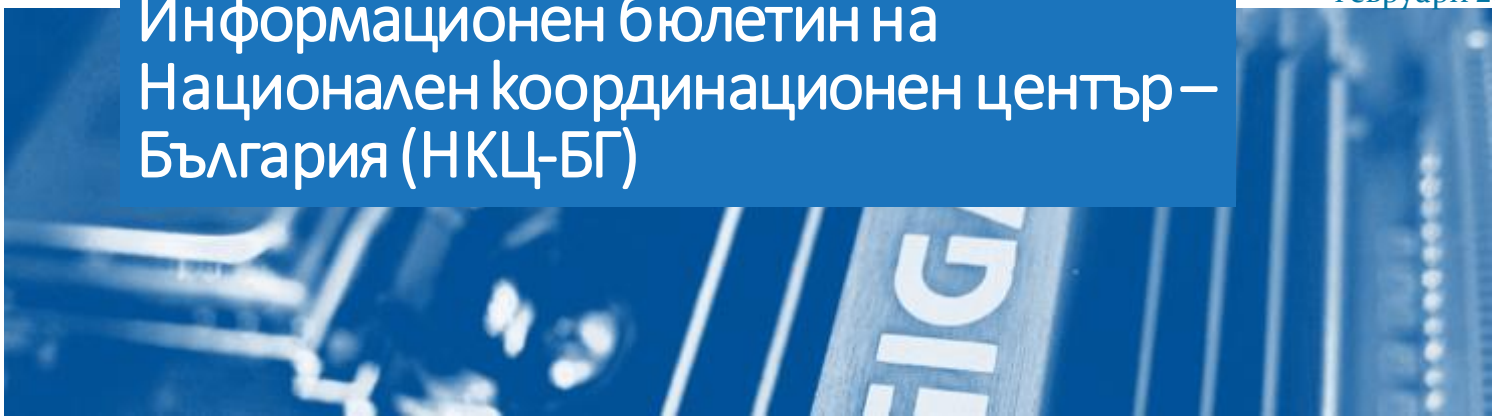
Министерство на електронното управление

Съфинансирано от Европейския съюз

Февруари 2025

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



CLOUDFLARE – КАКВИ ЗАЩИТИ ПРЕДЛАГА И КАК ТЕ ПАЗЯТ ТВОИТЕ САЙТОВЕ И ПРИЛОЖЕНИЯ

• В повечето случаи, когато говорим за сигурност в интернет, имаме предвид защити срещу хакери, злонамерен трафик, автоматични ботове и различни видове кибератаки. Cloudflare е компания, която предлага именно такива решения – базирани на облачна инфраструктура, които защитават уеб сайтове, приложения, мрежи и данни.

ЗАЩИТА ОТ DDOS АТАКИ

• Една от най-основните защити, които предоставя Cloudflare, е срещу DDoS атаки (Distributed Denial of Service) – опити да се претовари сайтът с огромно количество трафик, така че легитимните потребители да не могат да го използват. Cloudflare има автоматични механизми, които анализират и блокират зловреден трафик още преди да достигне до твоя сайт, често справяйки се с огромни обеми атаки за секунди.

Тази защита е жизнено важна, тъй като обемните атаки са в постоянен ръст – компанията отчита милиони опити за DDoS атаки годишно, които тя успешно неутрализира

ЗАЩО CLOUDFLARE Е ПРЕДПОЧИТАН ИЗБОР НА ДЪРЖАВНО НИВО В ЕС?

Cloudflare се използва на държавно ниво в Европейския съюз поради високото ниво на киберсигурност, устойчивост и съответствие с европейските регулации. Публичните институции все по-често са обект на кибератаки, особено DDoS атаки, които целят да направят държавни уебсайтове и електронни услуги недостъпни. Cloudflare разполага с глобална инфраструктура, способна да поема и неутрализира големи обеми злонамерен трафик, без прекъсване на услугите за гражданите.



WEB APPLICATION FIREWALL (WAF)

• Web Application Firewall е усъвършенстван защитен филтър, който анализира всички входящи HTTP/HTTPS заявки към сайта ти и блокира опасни такива – например:

- SQL Injection
- Cross-Site Scripting (XSS)
- други често срещани уязвимости

Тази защитна стена непрестанно се обновява и разчита на милиони данни от глобалната мрежа на Cloudflare, за да открива нови видове атаки.

УПРАВЛЕНИЕ НА БОТОВЕ (BOT MANAGEMENT)

• Не всички ботове са лоши (например Googlebot), но много автоматизирани скриптове причиняват щети – чрез сканиране на сайтове за уязвимости, източване на съдържание или опити за влизане чрез пробване на пароли.

• Cloudflare използва поведенчески анализ, машинно обучение, изкуствен интелект и разширени правила, за да разделя доброжелаещи и недоброжелаещи ботове и да блокира автоматизираните атаки при нужда.

SSL/TLS КРИПТИРАНЕ И DNS ЗАЩИТА

• Cloudflare автоматично предлага SSL/TLS криптиране на трафика между потребителите и сайта ти. Това означава, че данните са защитени чрез HTTPS, без нужда от ръчна конфигурация. Освен това защитата на DNS (система, която „превежда“ името на сайта в IP адрес) предотвратява DNS-базирани атаки и манипулации.

ZERO TRUST И ЗАЩИТЕН ДОСТЪП

• В съвременните корпоративни мрежи не всички потребители работят локално – много отдалечени служители, устройства и приложения трябва да имат достъп до ресурси. Cloudflare Zero Trust моделът замества традиционните VPN с по-сигурни, базирани на идентичност и политика контроли, които гарантират, че само упълномощени потребители и устройства имат достъп.

Държавните администрации обработват големи количества чувствителни данни, включително лична, здравна и финансова информация. Cloudflare осигурява криптиране на трафика, защита на DNS и механизми за предотвратяване на изтичане на данни, което е ключово за защитата на гражданската информация и обществено доверие. Важен фактор е и съответствието с регулации като GDPR, което улеснява институциите при спазване на законовите изисквания и провеждане на одити по сигурност.

Високата наличност и устойчивост на услугите са от критично значение за електронното управление и публичната комуникация. Благодарение на разпределената си инфраструктура, Cloudflare гарантира непрекъсваем достъп дори при атаки или технически сривове. Допълнително, чрез Zero Trust модели и централизирано управление на достъпа, държавните организации могат по-добре да защитят вътрешните си системи и критична инфраструктура.

Cloudflare се използва на държавно ниво в ЕС, защото предлага надеждна защита срещу киберзаплахи, висока наличност на публичните

ФУНКЦИОНАЛНОСТИТЕ НА DNS4EU – ВЕЧЕ НАЛИЧНИ НАПЪЛНО БЕЗПЛАТНО



Основна цел на Европейската комисия е да осигури защитата на данните на потребителите в цифровото пространство на ЕС, като същевременно се придържа към най-високите стандарти за поверителност и сигурност.

Чрез мащабния проект **DNS4EU** беше изградена сигурна, съвместима с европейските изисквания за поверителност DNS система, която се интегрира с наличните DNS услуги. Министерството на електронното управление, представено чрез CERT България, е един от членовете на международния консорциум, участвали в реализацията на **DNS4EU**.

DNS4EU съчетава водещи функции от наличните DNS решения:

- **Поверителност на данните:** потребителските данни са напълно анонимизирани. Те не могат да бъдат използвани за реклама или други цели.
- **Разширена защита:** системата осигурява проактивна защита от заплахи чрез сътрудничество с националните екипи за реакция при инциденти с компютърната сигурност (НЕРИКС).
- **Възможности за филтриране:** потребителите могат да се възползват от вградена функция за защита на деца и блокиране на реклами.

DNS4EU предоставя услуги като безплатен публичен сървър за граждани и търговско решение за правителства и критична инфраструктура (DNS4GOV) Целта е да се засили европейската киберустойчивост в рамките на ЕС, спазване на GDPR и проактивно блокиране на злонамерени домейни.

услуги, защита на личните данни и съответствие с европейските изисквания за сигурност, което го прави стратегически инструмент за модерната държавна цифрова инфраструктура.



КАК РАБОТИ DNS4EU

Най-често хората и институциите използват DNS сървър, зададен от техния доставчик на услуга. DNS4EU предоставя множество възможности за създаване на сигурна DNS услуга, която не само изпълнява основни функции, но и филтрира злонамерен трафик. По този начин се осигурява ефективна защита на всяко устройство, използващо сървъра, без да е необходимо инсталиране или поддръжка на какъвто и да е софтуер. Ако някое устройство, свързано с DNS4EU, се опита да осъществи достъп до злонамерен домейн (например, за да активира злонамерен софтуер или да осъществи достъп до измамен уебсайт), той бива блокиран незабавно, предотвратявайки евентуални щети, причинени от заплахата.

Освен това, сървърът и всички процеси, необходими за неговото разработване и работа, се хостват 100% в ЕС, като по този начин се гарантира спазването на GDPR и на всички най-високи норми за поверителност, установени от ЕС.

Услугата се предлага безплатно на гражданите и институциите, за повече информация и ръководството за инсталиране можете да видите на официалният адрес на проекта: https://www.joindns4.eu/





Министерство на електронното управление

ул. „Ген. Гурко“ № 6

Гр. София 1000

Ел. поща: bnccc@egov.government.bg

Ел. адрес: https://ncc.egov.bg/