УДК 004.056

Миколайчук В. В., ст. викладач
Державний університет «Житомирська політехніка»

DNSSEC ЯК ЗАСІБ ЗАХИСТУ ВІД DNS-СПУФІНГУ В ХМАРНІЙ ПЛАТФОРМІ AZURE

Система доменних імен (DNS) є фундаментальним компонентом мережевої інфраструктури, що забезпечує перетворення доменних імен у IP-адреси. Проте класичний протокол DNS не передбачав механізмів автентифікації відповідей, що робить його вразливим до атак. Однією з найнебезпечніших є атака DNS-спуфінгу (DNS cache poisoning), при якій зловмисник підміняє легітимні DNS-відповіді фальшивими, перенаправляючи користувачів на шкідливі ресурси. У 2008 році Ден Камінський продемонстрував критичну вразливість протоколу DNS, що дозволяла здійснювати масштабні атаки отруєння кешу DNS-серверів [1]. Ця вразливість стала каталізатором впровадження технології DNSSEC.

DNSSEC (Domain Name System Security Extensions) – набір розширень протоколу DNS, стандартизований у RFC 4033–4035, що забезпечує автентифікацію походження DNS-даних та перевірку їх цілісності за допомогою криптографічних підписів [2]. Механізм DNSSEC ґрунтується на ланцюгу довіри (chain of trust) від кореневої зони DNS до конкретного домену. Кожна зона підписує свої ресурсні записи приватним ключем, створюючи записи типу RRSIG. Відкритий ключ зони публікується у записі DNSKEY, а його хеш передається батьківській зоні як запис DS (Delegation Signer), формуючи ієрархічний ланцюг довіри. Для підтвердження відсутності записів використовуються записи NSEC або NSEC3, що унеможливлюють підробку негативних відповідей.

Все більше організацій розгортають інфраструктуру в хмарних платформах, зокрема Microsoft Azure, що пропонує сервіс Azure DNS для управління DNS-зонами. У лютому 2025 року Microsoft оголосив про загальну доступність (GA) підтримки DNSSEC для публічних зон Azure DNS [3]. Реалізація відповідає стандарту RFC 9824, що визначає вимоги до операційних практик впровадження DNSSEC [4]. Azure DNS автоматично генерує та керує криптографічними ключами зони (ZSK та KSK), виконує підписування ресурсних записів та забезпечує ротацію ключів. Для активації DNSSEC адміністратору достатньо увімкнути функцію для публічної зони та додати запис DS до реєстратора домену.

Впровадження DNSSEC в Azure DNS надає суттєві переваги: захист від DNS-спуфінгу та MITM-атак, оскільки кожна відповідь криптографічно підписана. Це критично для організацій, що мають відповідати стандартам PCI-DSS або ISO 27001. Водночас існують виклики: криптографічні підписи збільшують розмір DNS-відповідей, що може спричинити фрагментацію UDP-пакетів та потребує підтримки EDNS0. Ефективність DNSSEC залежить від повноти впровадження на всіх рівнях ланцюга довіри та підтримки валідації на стороні рекурсивного резолвера [5].

Отже, DNSSEC є необхідним механізмом забезпечення безпеки DNS-інфраструктури в хмарному середовищі Azure. Загальна доступність підтримки DNSSEC для публічних зон Azure DNS свідчить про зрілість технології та готовність платформи Microsoft до відповідності сучасним стандартам безпеки. Автоматизація управління ключами з боку Azure DNS суттєво знижує бар’єр впровадження, роблячи DNSSEC доступним для широкого кола організацій. Подальші дослідження можуть бути спрямовані на аналіз продуктивності DNS-запитів із увімкненим DNSSEC та порівняння реалізацій у різних хмарних провайдерах.

Список використаних джерел

1. Kaminsky D. It’s The End Of The Cache As We Know It [Електронний ресурс] – Режим доступу до ресурсу: https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf.

2. RFC 4033 – DNS Security Introduction and Requirements [Електронний ресурс] – Режим доступу до ресурсу: https://datatracker.ietf.org/doc/html/rfc4033.

3. DNSSEC for Azure DNS public zones is now generally available [Електронний ресурс] – Режим доступу до ресурсу: https://azure.microsoft.com/en-gb/updates?id=479465.

4. RFC 9824 – DNSSEC Automation [Електронний ресурс] – Режим доступу до ресурсу: https://datatracker.ietf.org/doc/html/rfc9824.

5. DNSSEC overview [Електронний ресурс] – Режим доступу до ресурсу: https://learn.microsoft.com/en-us/azure/dns/dnssec.