Лещенко Б. С., магістрант, гр. КБм-21-1,
Єфіменко А. А., к.т.н., доц.,
завідувач кафедри комп'ютерної інженерії та кібербезпеки
Вакалюк Т. А., д.пед.н., проф.,
професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

ПРОБЛЕМАТИКА ЗАХИСТУ СЕРВІСІВ DNS У СУЧАСНОМУ СВІТІ

Акронім DNS розшифровується як – «Domain Name System», що в перекладі з англійської мови – «Система доменних імен», також в деяких випадках DNS можна розшифрувати як – «Domain Name Servers».

DNS це ієрархічна, розподілена база даних, яка використовується для передачі інформації про доменні іменна. Розбіжності в скороченні демонструє труднощі з документацією DNS [1].

Метафора, якою найчастіше описують DNS, це дерево. DNS має корінь та різні

Домени верхнього рівня (Top Level Domains або TLDs) схожі на гілки, що відходять від кореня. Кожна гілка має менші гілки, які є доменами другого рівня (Second Level Domains або SLDs), а листки – це повні доменні імена (Fully Qualified Domain Name – FQDN), які іноді називають іменами хостів.

Система доменних імен існувала, ще до початку створення всесвітньої мережі Інтернет, ця система є фундаментальною та однією з найважливіших в роботі сучасних комп'ютерних мереж.

Кожен системний адміністратор, спеціаліст з інформаційної безпеки, спеціаліст з кібербезпеки та будь-яка людина, яка має справу з комп'ютерними мережами, повинні розумітися в принципах роботи DNS.

DNS є основною складовою повсякденного життя кожного в Інтернеті, але дуже мало людей розуміє, як це працює, або наскільки крихкою може бути основна інфраструктура. Навіть фахівці з безпеки, яким доручається захистити організацію, часто не мають повного уявлення про потенційні підводні камені в DNS [2].

Практично всі пристрої, які підключені до мережі, використовують DNS.

DNS постійно підлягає атакам з боку зловмисників. Сьогодні існує багато корпоративних рішень для захисту від таких атак, але їх вартість занадто велика для невеликих підприємств.

Також сьогодні все більше людей починають працювати з дому та з власних комп'ютерних систем, що вносить додаткову небезпеку з точки зору інформаційної безпеки.

Дуже часто звичайні користувачі та працівники підприємств не беруть до уваги ризики своєї кібербезпеки та ніяк не турбуються про безпеку своїх даних.

Використання стандартних авторизаційних даних для входу до адміністративної панелі маршрутизатору та застарілі версії операційних систем та програмного забезпечення – це речі, з якими постійно стикаються кібердослідники.

Система доменних імен є ще одним вектором, завдяки якому, приватність кінцевих користувачів може бути порушена. Недооцінка важливості безпеки протоколу DNS, навіть у 2021 році, може призвести до значних грошових втрат та , навіть, техногенних катастроф [3].

Збої в роботі доменної системи імен завдають шкоди, без перебільшення, всім сферам людської життєдіяльності починаючи сферою телекомунікацій і фінансовими сервісами і закінчуючи сферами освіти та охорони здоров'я.

Окрім високої частоти атак, телекомунікаційні провайдери також стикаються з більш втратними атаками – близько 8% організацій заявили, що вони сумарно постраждали від збитків у розмірі понад 5 мільйонів доларів внаслідок атак на DNS. [4].

Список використаних джерел

1. Liska A. DNS Security Defending the Domain Name System / A. Liska, S. Geoffrey. – Cambridge: Elsevier Inc, 2016. – 212 с. – (1).
2. Wireshark User Guide [Електронний ресурс] -https://www.wireshark.org/docs/wsug_html/
3. Donahue G. Network Warrior / Gary A. Donahue. – Sebastopol: O'Reilly Media, Inc, 2011. – 785 с. – (2).

Sidheeq S. Configure Cisco Router As DNS Servers In GNS3 – Step By Step [Електронний ресурс] / Saifudheen Sidheeq. – 2020. – Режим доступу до ресурсу: https://getlabsdone.com/configure-cisco-router-as-dns-server-in-gns3-step-by-step/.