Bezpieczeństwo w sieci – rekomendacje, dobre praktyki i zdrowy rozsądek

Piotr Studziński-Raczyński
Samodzielny specjalista ds. DNS

System nazw domen (ang. *Domain Name System*, DNS) to hierarchiczny, rozproszony system nazewnictwa dla komputerów, usług lub dowolnych zasobów podłączonych do Internetu lub sieci prywatnej. System ten kojarzy różne informacje z nazwami domen przypisanymi do każdego z uczestniczących w nim podmiotów. Przede wszystkim tłumaczy on łatwe do zapamiętania nazwy domen na numeryczne adresy IP potrzebne do lokalizowania usług i urządzeń komputerowych na całym świecie. Zapewniając ogólnoświatową, rozproszoną usługę przekierowania, opartą na słowach kluczowych, DNS stanowi zasadniczy element funkcjonowania Internetu. Nazwa domeny (np. „twojadomena.pl") to ciąg znaków identyfikujący obszar administracyjnej autonomii, uprawnienia lub kontroli w Internecie. Nazwy domen są tworzone zgodnie z zasadami i procedurami DNS. Każda nazwa zarejestrowana w DNS jest nazwą domeny. Nazwy domen są używane w różnych kontekstach sieciowych oraz celach dotyczących nazewnictwa i adresowania właściwych dla danych aplikacji. Ogólnie rzecz ujmując, nazwa domeny reprezentuje zasób protokołu internetowego (IP), np.: komputer osobisty używany do uzyskiwania dostępu do Internetu, serwer, na którym znajduje się strona internetowa lub sama witryna internetowa, a nawet jakakolwiek inna usługa przekazywana przez Internet.

Gdy DNS został pierwotnie zaprojektowany w latach osiemdziesiątych dwudziestego wieku, jego głównym założeniem było zminimalizowanie centralnej administracji sieci i ułatwienie podłączania nowych komputerów do Internetu. Nie przywiązywano jednak wtedy zbyt dużej wagi do kwestii bezpieczeństwa. Braki w tej dziedzinie stworzyły miejsce na różnego rodzaju nadużycia i ataki, w których odpowiedzi na zapytania DNS są fałszowane. W ten sposób użytkownicy Internetu mogą zostać wprowadzeni w błąd, np. mogą zostać podstępnie nakłonieni do ujawnienia poufnych, wrażliwych informacji, takich jak hasła i numery kart kredytowych. Mimo że dołożono wszelkich starań, aby załatać luki w zabezpieczeniach oprogramowania wykorzystywanego do tworzenia zapytań do DNS, podstawowy problem leży w samym funkcjonowaniu DNS.

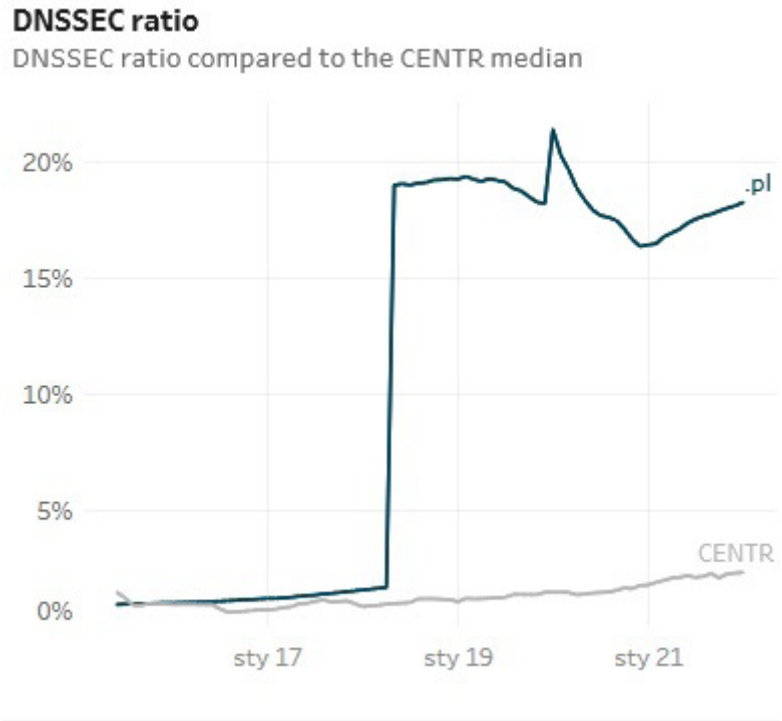
Inżynierowie z Internet Engineering Task Force (IETF), organizacji odpowiedzialnej za standardy protokołu DNS, od dawna zdawali sobie sprawę, że brak silniejszego uwierzytelniania w DNS stanowi problem. Prace nad rozwiązaniem tego problemu rozpoczęły się w latach dziewięćdziesiątych, a ich efektem było opracowanie rozszerzenia DNSSEC (Domain Name System Security Extensions). DNSSEC wzmacnia uwierzytelnianie w DNS za pomocą podpisów cyfrowych opartych na kryptografii klucza publicznego. W DNSSEC, to nie zapytania i odpowiedzi DNS są podpisywane kryptograficznie, podpisywane są dane DNS (przez właściciela tych danych). Każda strefa DNS posiada parę kluczy: publiczny i prywatny. Właściciel strefy używa klucza prywatnego do podpisywania danych DNS w strefie i generowania podpisów cyfrowych na tych danych. Jak sugeruje sama nazwa, klucz prywatny jest utrzymywany w tajemnicy przez właściciela strefy. Klucz publiczny strefy jest natomiast publikowany w samej strefie i może być pobierany przez każdego. Każdy resolver rekursywny, wyszukujący dane w strefie, pobiera również klucz publiczny strefy, który wykorzystuje do sprawdzenia autentyczności danych DNS. W ten sposób resolver potwierdza, że podpis cyfrowy pod pobranymi przez niego danymi DNS jest ważny. Jeśli tak rzeczywiście jest, dane DNS są prawidłowe i zostają zwrócone użytkownikowi. Jeśli podpis nie zostanie potwierdzony, resolver zakłada atak, odrzuca dane i zwraca użytkownikowi komunikat o błędzie.

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) stworzyła w 2008 roku wieloletni program tematyczny (MTP1),

którego ostatecznym celem była wspólna ocena i poprawa odporności publicznej łączności elektronicznej w UE. W ramach tego programu zbadano innowacyjne technologie, które potencjalnie mogą zwiększyć odporność takiej komunikacji. Rozszerzenia bezpieczeństwa DNS (tj. DNSSEC) zostały uznane za technologię, która zwiększa poziom wiarygodności i jakość DNS. Jest ona uzupełnieniem innych technologii, takich jak *Secure Sockets Layer*, które zabezpieczają dostarczanie treści poprzez zwiększenie bezpieczeństwa usług internetowych[1].

Od czerwca 2012 roku Rejestr domeny krajowej .pl, prowadzony przez NASK, umożliwia abonentom domeny .pl zabezpieczanie swoich nazw protokołem DNSSEC. Od tego czasu liczba nazw domen zabezpieczonych DNSSEC stopniowo się zwiększa. Szczególnym momentem w historii DNSSEC w Rejestrze domeny .pl był rok 2018, kiedy nastąpił znaczny wzrost zainteresowania tą usługą wskutek kampanii promocyjnych i działań edukacyjnych Rejestru domeny .pl[2], jak również aktywnego zaangażowania ze strony rejestratorów uczestniczących w Programie Partnerskim NASK. Na wykresie (Rys. 1) przedstawiono wskaźnik rejestracji nazw w domenie .pl zabezpieczonych protokołem DNSSEC w zestawieniu ze średnią wartością wskazywaną przez rejestry ccTLD zrzeszone w CENTR (*Council of European National Top-Level Domain Registries*). W styczniu 2020 roku NASK znalazł się wśród czterech podmiotów nagrodzonych przez nazwa.pl sp. z o.o., jednego z rejestratorów nazw domeny .pl, za intensywne działania na rzecz poprawy jakości Internetu. NASK, pełniący między innymi funkcję Rejestru domeny .pl, został wyróżniony w kategorii „Bezpieczeństwo" w związku z rozwijaniem i promocją protokołu DNSSEC, zwiększającego bezpieczeństwo korzystania z DNS. Nie spoczywając na laurach w dążeniu do stałego udoskonalania usługi i podnoszenia poziomu bezpieczeństwa domeny .pl, już w marcu 2020 roku Rejestr domeny .pl wprowadził zmianę w sposobie obsługi protokołu DNSSEC, czego efektem było dziewięciokrotne skrócenie czasu podpisywania i walidacji stref w porównaniu do uprzednio wykorzystywanego rozwiązania.

Rys. 1 Wskaźnik rejestracji nazw w domenie .pl zabezpieczonych DNSSEC w zestawieniu ze średnią rejestrów zrzeszonych w CENTR



[1] Good Practices Guide for deploying DNSSEC, ENISA, marzec 2010
[2] Szczegóły dotyczące aktywności Rejestru w zakresie działań edukacyjnych oraz publikacji NASK z zakresu DNSSEC dostępne są pod adresem https://www.dns.pl/DNSSEC

Wraz z rozwojem DNSSEC, DNS może stać się podstawą dla innych protokołów, które wymagają bezpiecznego przechowywania danych. Powstały nowe protokoły, które opierają się na DNSSEC, a więc działają tylko w strefach, które są podpisane. Na przykład *DNS-based Authentication of Named Entities* (DANE) pozwala na publikowanie kluczy Transport Layer Security (TLS) w strefach dla takich zastosowań, jak transport poczty. DANE zapewnia sposób weryfikacji autentyczności kluczy publicznych, który nie opiera się na urzędach certyfikacji. Nowe metody dodawania prywatności do zapytań DNS będą mogły opierać się na DANE również w przyszłości. W 2018r. ICANN (*Internet Corporation for Assigned Names and Numbers)* po raz pierwszy zmienił kotwicę zaufania dla root'a DNS. Podczas tego procesu wyciągnięto wiele wniosków na temat DNSSEC. W konsekwencji, wielu operatorów resolverów stało się bardziej świadomych w zakresie DNSSEC i włączyło walidację, a zainteresowani mieli okazję zobaczyć, jak działa cały system DNSSEC. ICANN wyraża nadzieję, że DNSSEC będzie coraz częściej stosowany zarówno przez operatorów resolverów, jak i właścicieli stref. Oznaczałoby to, że większa liczba użytkowników na całym świecie mogłaby skorzystać z opartej na kryptografii usłudze DNSSEC, zapewniającej, że otrzymują oni autentyczne odpowiedzi DNS na swoje zapytania.

Wśród poważniejszych zagrożeń bezpieczeństwa w sieci są te, mające podłoże socjotechniczne. Często to właśnie tego rodzaju działania umożliwiają sprawcom skuteczne osiągnięcie zamierzonego celu, również w branży domen internetowych. Znany użytkownikom portali pośredniczących w lokalnej sprzedaży towarów i usług schemat działania oszustów, polegający na zaczepieniu ofiary w sprawie wystawionego przedmiotu, za pośrednictwem zewnętrznego narzędzia - popularnego komunikatora[3] – znalazł również zastosowanie na rynku domenowym. O ile na rynku sprzedaży towarów i usług celem użycia komunikatora internetowego przez sprawcę jest przesłanie linka do strony imitującej portal, gdzie znajduje się fałszywy panel płatności do „uiszczenia zapłaty", o tyle w przypadku domen internetowych taki komunikator może być użyty jako narzędzie do uwierzytelnienia się przez osobę podszywającą się pod abonenta domeny. Taki los, według redakcji *KrebsonSecurity*, spotkał abonenta domeny „e-hawk.net", w przypadku której 23 grudnia 2019 r. sprawcom udało się oszukać pracownika działu obsługi klienta rejestratora i skłonić go do przeniesienia domeny do innego rejestratora za pomocą dość prozaicznego, wydawałoby się, podstępu socjotechnicznego - i to bez uruchomienia jakiejkolwiek weryfikacji rzeczywistego abonenta domeny. Otóż, sprawcy, kontaktując się z rejestratorem za pośrednictwem mobilnej aplikacji komunikatora, zadeklarowali, że są obecnie prawowitymi „właścicielami" domeny i udostępnili krótki filmik, na którym przedstawiony jest panel klienta rejestratora oraz kończąca się błędem próba potwierdzenia zainicjowanego już transferu wspomnianej nazwy domeny. Pracownik obsługi klienta rejestratora, chcąc sprawdzić czy system rzeczywiście nie działa poprawnie, zatwierdził transfer, co doprowadziło do przeniesienia domeny do resellera tego rejestratora. Trzy dni po tym zajściu, domena została przetransferowana do nowego rejestratora. Warto w tym miejscu zauważyć, że domena „e-hawk.net" była zabezpieczona usługą Registrar Lock, zapewniającą ochronę domeny na poziomie rejestratora.

Analizując działanie sprawców, widać, że pierwotny zabieg przeniesienia domeny do resellera tego rejestratora był celowy – taki transfer nie powoduje bowiem zmiany ID rejestratora z poziomu rejestru domen, a co za tym idzie, nie jest związany z procedurą przenoszenia obsługi domeny realizowaną przez rejestr. Dzięki temu „cichemu" zabiegowi sprawcy zyskali dodatkowy czas na dalsze działania bez zwracania na siebie uwagi faktycznego abonenta. I właśnie ten dodatkowy czas, kiedy działania oszustów pozostawały niezauważone, umożliwił im usunięcie blokady Registrar Lock i transfer domeny do zewnętrznego rejestratora. Nie wchodząc w dalsze szczegóły tego przypadku tzw. porwania domeny (ang. *domain hijacking*), widać, że zjawisko jest w dalszym ciągu aktualne, a stosowane techniki socjotechniczne przybierają coraz nowsze formy, obserwowane również w innych dziedzinach życia w przestrzeni cyfrowej. W opisanym powyżej

[3] Źródło: CERT Polska

przypadku, od strony proceduralnej na pewno zawinił czynnik ludzki, rejestrator nie powinien działać na podstawie informacji pochodzących z nieautoryzowanego adresu e-mail lub innego narzędzia niepowiązanego z obsługą danej nazwy domeny. To, na co warto zwrócić szczególną uwagę w zakresie systemów bezpieczeństwa w kontekście przedstawionego scenariusza, to dostępność narzędzi umożliwiających *zabezpieczenie domeny na najwyższym poziomie*[4]. Takim narzędziem jest usługa .pl Registry Lock, świadczona przez Rejestr Domeny .pl. Taki środek ostrożności, tj. zabezpieczenie domeny usługą Registry Lock, nie został jednak podjęty przez abonenta domeny „e-hawk.net". Jej zastosowanie mogłoby skutecznie zneutralizować wszelkie próby manipulacji wobec pracownika rejestratora, a w konsekwencji uniemożliwić transfer domeny i zmianę jej delegacji. W przypadku aktywnej usługi Registry Lock, rejestrator nie może bowiem samodzielnie przenieść obsługi domeny, usunąć domeny, ani np. zmienić jej delegacji[5]. Takie działanie wymaga realizacji złożonej, wieloetapowej procedury autoryzacyjnej, co stanowi silną barierę dla potencjalnych „porywaczy" domen, pozostawiając niewiele miejsca na tzw. słabe ogniwo.

Od momentu wdrożenia usługi .pl Registry Lock w marcu 2019 roku, prowadzone są aktywne działania w zakresie jej promocji wśród użytkowników Internetu oraz samych abonentów nazw w domenie .pl. Prowadzone są one zarówno w postaci przekazu elektronicznego[6], jak również w ramach udziału NASK w wydarzeniach międzynarodowych, takich jak, np. Konferencja Secure[7] czy Forum Ekonomiczne[8]. Spektakularne przypadki ukazujące scenariusze porwania domeny były tematem przewodnim wielu prezentacji i prelekcji wygłoszonych podczas konferencji branżowych, m.in. Ecommerce Standard[9] w 2019 roku, jak również na łamach portali internetowych[10] traktujących o szeroko pojętym bezpieczeństwie w sieci. Również w zakresie prac analityczno-rozwojowych Rejestr domeny .pl ma swój udział w kształtowaniu koncepcji modelowania i standaryzowania możliwych implementacji usługi Registry Lock w rejestrach ccTLD zrzeszonych w CENTR – „*Models of registry lock for top-level domain registries*".[11]

Od umieszczenia w ofercie usługi .pl Registry Lock, oprócz wspomnianych działań edukacyjnych, Rejestr domeny .pl, starając się umożliwić rejestratorom dotarcie do jak najszerszej liczby odbiorców, stosuje w Programie Partnerskim NASK specjalną politykę cenową. W ramach aktualnie prowadzonej kampanii promocyjnej, obserwowany jest znaczny wzrost zainteresowania usługą .pl Registry Lock, który w okresie od października 2021 r. do marca 2022 r. zaowocował podwojeniem liczby nazw domen zabezpieczonych usługą .pl Registry Lock.

W lutym 2019 roku, John Crain, główny specjalista ds. bezpieczeństwa, stabilności i odporności w ICANN, powiedział, że wiele z najlepszych praktyk, które mogą utrudnić atakującym przejęcie domen lub infrastruktury DNS, jest znanych już od ponad dekady. „Wiele z nich sprowadza się do higieny danych" - powiedział Crain. „Duże organizacje, a także małe i średnie przedsiębiorstwa nie zwracają uwagi na podstawowe praktyki z zakresu bezpieczeństwa, takie jak np. wieloskładnikowe uwierzytelnianie. W dzisiejszych czasach, jeśli prowadzona przez organizację polityka bezpieczeństwa nie jest wystarczająco optymalna, taka organizacja naraża się na atak, który może skutkować przejęciem zasobów lub nawet kontroli nad jej działalnością. Taka jest dzisiejsza rzeczywistość. Widzimy, że w Internecie działają dużo bardziej wyrafinowani gracze i jeśli nie będziemy stosować podstawowych rozwiązań i praktyk z zakresu bezpieczeństwa, to istnieje dość duże prawdopodobieństwo, że nas zaatakują".

[4] https://www.dns.pl/sites/default/files/2019-04/pliki/pl_REGISTRY_LOCK_ulotka.pdf
[5] Zakres ochrony zależy od zaimplementowanego przez dany rejestr modelu usługi Registry Lock
[6] https://www.dns.pl/newsy/jak_zapobiec_porwaniu_domeny, https://www.dns.pl/newsy/niezabezpieczone_domeny_zagrozenie
[7] https://www.dns.pl/newsy/secure2019
[8] https://www.dns.pl/newsy/forum_cyberbezpieczenstwa_2019
[9] https://www.dns.pl/newsy/Ecommerce_Standard_2019
[10] https://www.forbes.pl/biznes/sadzisz-ze-masz-dobrze-zabezpieczona-domene-internetowa-prawdopodobnie-jestes-w/x3e3m6f
[11] https://centr.org/library/library/download/9799/6192/41.html