Bezpieczne wdrożenie systemu DNS w organizacji

na podstawie NIST SP 800-81r3
Secure Domain Name System (DNS)
Deployment Guide

Czerwiec 2026

Spis treści

Najważniejsze wnioski

DNS powinien być traktowany jako aktywny punkt egzekwowania polityk bezpieczeństwa, a nie wyłącznie jako usługa rozpoznawania nazw.

01	**Protective DNS**	Blokowanie komunikacji z domenami phishing, malware i C2 jeszcze przed nawiązaniem połączenia.
02	**Centralizacja ruchu DNS**	Ruch DNS powinien przechodzić przez kontrolowany resolver korporacyjny lub autoryzowany punkt inspekcji.
03	**Widoczność i telemetria**	Logi DNS powinny zasilać SIEM/SOAR, DFIR oraz detekcję anomalii i eksfiltracji.
04	**DNSSEC i szyfrowanie**	DNSSEC chroni integralność danych DNS, a DoT/DoH/DoQ chronią kanał komunikacji po analizie ryzyka.
05	**Odporność architektury**	Separacja ról, hidden primary, secondary i kontrolowane transfery stref ograniczają ryzyka operacyjne.

Priorytety wdrożeniowe

Rekomendacje priorytetowe

Obszary o największym znaczeniu organizacyjnym i komunikacyjnym dla zarządu, audytu oraz zespołów bezpieczeństwa

Protective DNS Filtrowanie domen malware, phishing i C2 na etapie rozpoznawania nazwy	**Kontrolowany resolver** Wymuszenie ruchu DNS przez centralny punkt inspekcji
SIEM / SOAR Korelacja logów DNS z danymi endpoint, firewall i DHCP	**DNSSEC** Podpisywanie stref i walidacja odpowiedzi DNS
Encrypted DNS DoT/DoH/DoQ tam, gdzie nie ogranicza to kontroli bezpieczeństwa	**DNS exfiltration** Detekcja wysokiej entropii QNAME, nietypowych typów rekordów i wolumenów

REKOMENDACJA
Najpierw należy zapewnić centralny punkt kontroli i widoczności DNS. Bez tego detekcja anomalii, blokowanie publicznych resolverów oraz przeciwdziałanie eksfiltracji pozostają niepełne.

Macierz wpływu i trudności wdrożenia

Wpływ / trudność	Niska	Średnia	Wysoka
Wysoki	• Blokada publicznych DNS • RPZ / CERT Polska • Centralny resolver	• Logi DNS do SIEM • Detekcja eksfiltracji • Polityki DoH w przeglądarkach	• Hybrydowy protective DNS • Rozbudowana analityka DNS Security
Średni	• QNAME minimization • Audyt rekordów publicznych	• DNSSEC dla stref zewnętrznych • DNSTAP • Monitoring look-alike domains	• Pełna automatyzacja SOAR • Zaawansowana detekcja anomalii
Niższy	• Higiena TTL • Usunięcie zbędnych rekordów TXT/HINFO/LOC	• Rotacja kluczy TSIG • Procedury false positive	• HSM dla KSK w środowiskach o podwyższonym ryzyku

JAK CZYTAĆ MACIERZ
Priorytetem powinny być elementy z komórek „wysoki wpływ / niska lub średnia trudność". Elementy o wysokiej trudności warto planować jako projekty etapowe.

Referencyjna architektura DNS Security

Warstwa / komponent	Rola w architekturze	Kluczowe kontrole
1. Endpointy Windows / mobile / IoT	Generują zapytania DNS i powinny korzystać wyłącznie z autoryzowanej konfiguracji DNS.	MDM/GPO, blokada ręcznej zmiany resolverów, EDR/XDR, obsługa IoT przez lokalny forwarder
↓	Ruch DNS kierowany do kontrolowanego punktu	Blokada bezpośredniego UDP/TCP 53 do internetu oraz nieautoryzowanego DoT/DoQ/DoH
2. Resolver korporacyjny	Centralny punkt inspekcji, logowania i egzekwowania polityk	Walidacja DNSSEC, QNAME minimization, DNSTAP, retencja logów, integracja z SIEM
↓	Filtrowanie i decyzje bezpieczeństwa	RPZ, listy CERT Polska, threat intelligence, obsługa wyjątków i false positive
3. Protective DNS	Warstwa wykrywania i blokowania domen malware, phishing, C2 oraz domen wysokiego ryzyka	Blokady, alerty, scoring reputacyjny, analiza NRD/NOD, korelacja zdarzeń
↘ logi / zdarzenia	Przekazanie telemetrii do systemów bezpieczeństwa	SIEM/SOAR, playbooki reakcji, korelacja z DHCP, firewall i endpoint
4. Upstream resolver	Kontrolowane wyjście do resolvera nadrzędnego albo usługi chmurowej	DoT/DoH/DoQ tam, gdzie uzasadnione; lokalny fallback w modelu hybrydowym

Drzewo wyboru modelu protective DNS

Krok	Pytanie decyzyjne	Odpowiedź / warunek	Rekomendowany kierunek
1	Czy logi DNS i konfiguracja usługi mogą być przetwarzane poza organizacją?	Nie albo tylko w bardzo ograniczonym zakresie	Model on-premises lub hybrydowy z lokalnym punktem kontroli
2	Czy wymagana jest bardzo niska latencja i pełna kontrola lokalna?	Tak	Lokalne resolvery, RPZ, lokalna telemetria i własne procedury utrzymania
3	Czy organizacja potrzebuje dużej bazy threat intelligence i skalowalnej analityki?	Tak	Model cloud-based albo hybrydowy, z preferencją logów i konfiguracji w UE
4	Czy usługa chmurowa może być niedostępna bez utraty filtracji?	Nie	Model hybrydowy: cloud jako podstawowy kanał, lokalne RPZ jako fallback
5	Czy ryzyko profilowania zapytań DNS jest wysokie?	Tak	Ograniczyć zakres danych przekazywanych na zewnątrz, rozważyć on-premises lub silne warunki umowne.

Poziomy dojrzałości wdrożenia DNS Security

Tabela pozwala potraktować rekomendacje jako roadmapę: od minimum kontroli do modelu dojrzałego.

Obszar	Minimum	Rozszerzony	Dojrzały
Kontrola ruchu	Centralny resolver; blokada DNS poza organizację	Kontrola DoH/DoT/DoQ; wymuszenie konfiguracji przez GPO/MDM	Polityki per segment, użytkownik i typ urządzenia
Filtrowanie	Lista CERT Polska i podstawowe RPZ	Wiele źródeł reputacyjnych, procedura false positive	Hybrydowy protective DNS, scoring i automatyzacja wyjątków
Widoczność	Logowanie blokad i zdarzeń bezpieczeństwa	DNSTAP, SIEM/SOAR, korelacja z DHCP/firewall/EDR	Detekcja anomalii, DNS tunneling i playbooki SOAR
Odporność	Primary + secondary, ACL dla transferów	Hidden primary, TSIG, monitoring AXFR/IXFR	DNSSEC, HSM dla kluczy wysokiego ryzyka, testy ciągłości działania

UŻYCIE PRAKTYCZNE
Tabela może zostać wykorzystana jako szybka checklista audytowa albo plan etapowania prac wdrożeniowych.

Bezpieczne wdrożenie systemu DNS w organizacji na podstawie:

NIST Special Publication 800-81 Revision 3 Secure Domain Name System (DNS) Deployment Guide

1. Wprowadzenie

Dokument ten stanowi streszczenie i adaptację rekomendacji zawartych w publikacji NIST SP 800-81r3 (*Secure Domain Name System Deployment Guide*, marzec 2026). Jego celem jest przedstawienie praktycznych wskazówek dotyczących bezpiecznego wdrożenia i utrzymania infrastruktury DNS w organizacjach, ze szczególnym uwzględnieniem specyfiki sektora finansowego.

Rola DNS w ostatnich latach wyraźnie się zmieniła. Przez długi czas traktowano go jako czystą usługę operacyjną, która tłumaczy nazwy domen na adresy IP i ma działać niezawodnie. Dziś coraz więcej organizacji wykorzystuje DNS jako aktywny element architektury bezpieczeństwa. Koncepcja tzw. protective DNS zakłada wzbogacenie infrastruktury DNS o funkcje wykrywania i blokowania zagrożeń jeszcze na etapie rozpoznawania nazwy, zanim dojdzie do nawiązania połączenia. Takie podejście wpisuje się zarówno w model zero trust, jak i defense-in-depth, i jest fundamentem rekomendacji przedstawionych w tym dokumencie.

NIST w najnowszej rewizji dokumentu wyraźnie podkreśla zmianę roli DNS – z czysto operacyjnej na aktywny element architektury bezpieczeństwa (protective DNS) – wpisujący się w modele zero trust i defense-in-depth. Pozostała część tego dokumentu przedstawia konkretne rekomendacje wynikające z tej publikacji.

2. DNS jako element strategii bezpieczeństwa

REKOMENDACJA
DNS powinien być traktowany jako warstwa egzekwowania polityk bezpieczeństwa, obejmująca całą organizację, a nie wyłącznie jako usługa infrastrukturalna.

DNS jest obecny w każdej sieci i obsługuje praktycznie każdy typ klienta – stacje robocze, serwery, urządzenia IoT, zasoby chmurowe. To sprawia, że ochrona zastosowana na poziomie DNS automatycznie obejmuje całą infrastrukturę, niezależnie od typu urządzenia. Zanim dojdzie do jakiegokolwiek połączenia sieciowego, najpierw musi zostać rozpoznana nazwa domeny i właśnie w tym momencie DNS może zablokować zagrożenie, zanim komunikacja w ogóle się rozpocznie.

Dlatego organizacje powinny traktować DNS jako punkt egzekwowania polityk bezpieczeństwa, a nie tylko jako usługę rozpoznawania nazw.

2.1. Protective DNS - co to daje

Protective DNS to usługa, która analizuje zarówno zapytania, jak i odpowiedzi DNS w czasie rzeczywistym, porównuje je z danymi pochodzącymi ze źródeł typu threat intelligence i podejmuje działania, np. blokuje rozpoznanie domeny powiązanej z phishingiem albo loguje podejrzane zapytanie. Działa to na zasadzie DNS firewalla lub Response Policy Zone (RPZ). Blokada następuje na etapie rozpoznawania nazwy, czyli zanim nawiązane zostanie jakiekolwiek połączenie TCP/IP z celem. W efekcie pozostałe elementy infrastruktury bezpieczeństwa, takie jak firewall czy IDS/IPS, zostają odciążone.

Konkretne korzyści z wdrożenia:

- Blokowanie komunikacji z domenami powiązanymi z malware, phishingiem i infrastrukturą C2 w czasie rzeczywistym
- Filtrowanie ruchu do domen niezgodnych z polityką organizacji (np. kategorie treści, ograniczenia prawne, świeżo zarejestrowane domeny)
- Generowanie danych telemetrycznych – historyczne i bieżące logi zapytań DNS są istotne w przypadku konieczności wszczęcia procedur DFIR (Digital Forensics and Incident Response)
- Integracja z ekosystemem bezpieczeństwa – dane z DNS mogą być korelowane w systemach klasy SIEM/SOAR z innymi zdarzeniami

- Spełnienie wymogów regulacyjnych dotyczących blokowania dostępu do niedozwolonych zasobów

2.2. Wdrożenie protective DNS

Nie ma jednego słusznego modelu wdrożenia. Niektóre organizacje stawiają na własne serwery z RPZ, inne korzystają z chmurowych usług DNS z wbudowaną analizą zagrożeń. Każde podejście ma swoje zalety i ograniczenia:

On-premises (DNS firewalle, RPZ na lokalnych resolverach): niska latencja, pełna kontrola nad polityką, możliwość atrybucji zapytań do konkretnych klientów. W niektórych wdrożeniach, w zależności od przyjętych założeń, ograniczeniem może być mniejsza baza threat intelligence niż w usługach chmurowych, słabsze algorytmy detekcji w ruchu na żywo z uwagi na ograniczone zasoby CPU/RAM oraz koszty utrzymania po stronie podmiotu.

Cloud-based (przekierowanie zapytań do zewnętrznej usługi protective DNS): większe zasoby threat intelligence, baza zagrożeń aktualizowana jest w czasie rzeczywistym, lepsza skalowalność i analityka w czasie rzeczywistym oraz w pewnych sytuacjach większa poufność (właściciele odpytywanych domen nie widzą kto konkretnie o nie odpytuje). Minusy to wyższa latencja, zależność od dostawcy i potencjalna utrata poufności wynikająca z możliwości profilowania na podstawie generowanych zapytań DNS (zarówno w zakresie prowadzonej działalności, jak też elementów infrastruktury informatycznej), dodatkowe koszty subskrypcji. Z uwagi na kwestie przetwarzania danych poufnych wskazane jest korzystanie z usług chmurowych, w których konfiguracja usługi i logi zapytań DNS są zlokalizowane na terenie Unii Europejskiej.

Infrastruktura hybrydowa. Jeżeli szacowanie ryzyka w zakresie ewentualnego przetwarzania danych poufnych na to pozwala, najlepsze rezultaty daje połączenie obu modeli. W normalnych warunkach zapytania trafiają do usługi chmurowej z jej rozbudowaną bazą zagrożeń. Jeśli usługa chmurowa stanie się niedostępna, lokalne RPZ zapewniają podstawową ochronę zamiast fail-open bez żadnej filtracji.

W uzupełnieniu do rekomendacji NIST, w polskim kontekście minimalnym lokalnym krokiem w zakresie protective DNS jest subskrybowanie oraz wymuszanie blokowania domen z listy „złośliwych domen" publikowanej przez CERT Polska. Lista jest aktualizowana regularnie i zawiera domeny powiązane z phishingiem, malware i innymi zagrożeniami obserwowanymi w polskiej przestrzeni sieciowej. Samo wdrożenie tej listy jako źródła nie jest wystarczające i należy traktować je jedynie jako punkt wyjścia do budowy listy niebezpiecznych domen pochodzących z wielu źródeł. Zgodnie z zasadą defense-in-depth rekomendowane jest uzupełnienie filtrowania o co najmniej jedną dodatkową listę reputacyjną z niezależnego źródła. Różni dostawcy list korzystają z innych źródeł telemetrycznych, więc taki zbiór będzie bardziej komplementarny niż lista tylko od jednego dostawcy. Należy jednak pamiętać, że na listach RPZ mogą znaleźć się również legalne domeny dodane w wyniku pomyłki lub błędnej automatycznej interpretacji nazwy domenowej. Typowym przypadkiem są polskojęzyczne domeny uznawane przez automatyczne systemy za DGA (*Domain Generation Algorithm*). Wdrożenie list RPZ lub ich poszerzenie o kolejne źródła powinno być zawsze poprzedzone analizą ich zawartości, oceną jakości źródła, procedurą obsługi false positive oraz oszacowaniem ryzyka wynikającego z ich wykorzystywania.

Dodatkową warstwą ochrony może być kwarantanna nowo zarejestrowanych domen (tzw. *newly registered domains* lub *newly observed domains*). NIST wprost wskazuje monitorowanie nowych rejestracji w kontekście domen podobnych do domen organizacji (*look-alike domains*); filtrowanie wszystkich NRD/NOD należy traktować jako praktyczne rozszerzenie modelu protective DNS zależne od ryzyka, a nie jako bezwarunkową rekomendację dla każdego środowiska. Domeny zarejestrowane stosunkowo niedawno są częściej wykorzystywane w kampaniach phishingowych oraz do dystrybucji malware niż domeny posiadające już historię wykorzystywania. Na podstawie oszacowanego ryzyka oraz analizy zapytań DNS generowanych przez użytkowników można podjąć decyzję o monitorowaniu, alertowaniu albo blokowaniu takich domen. Rekomenduje się co najmniej alertowanie na zapytania do domen zarejestrowanych lub zaobserwowanych w ostatnich dniach. Blokowanie takich domen powinno być poprzedzone analizą ryzyka, testami wpływu na biznes oraz wdrożeniem mechanizmu wyjątków dla uzasadnionych przypadków biznesowych. Okres rejestracji objęty kwarantanną powinien być określony indywidualnie przed wdrożeniem, na podstawie oszacowanego ryzyka.

2.3. Logowanie DNS

Logi DNS to jedno z cenniejszych źródeł danych dla zespołów bezpieczeństwa. Na podstawie zapytań DNS można odtworzyć ścieżkę komunikacji endpointu, zidentyfikować próby połączenia z infrastrukturą C2 albo wykryć eksfiltrację danych. Problem w tym, że logowanie całego ruchu DNS generuje duże wolumeny danych i może obciążyć serwery DNS. Zarówno system, jak i punkt w infrastrukturze, w którym logi zapytań DNS będą zbierane, mają ogromne znaczenie pod kątem wielkości logów, ich przydatności oraz możliwości dalszego wykorzystania do analizy lub automatycznych działań przez inne systemy zabezpieczające. Należy więc podejść do tego zadania w sposób przemyślany, uwzględniając analizę wymagań, projekt architektury i harmonogram wdrożenia.

Zapytania do domen sklasyfikowanych jako złośliwe lub nieautoryzowane muszą być logowane zawsze. Jest to minimalne założenie dla bezpieczeństwa usługi DNS.

Logi DNS powinny trafiać do SIEM i być korelowane z innymi źródłami, takimi jak: historia dzierżaw DHCP, logi endpointów oraz dane z firewalli.

Format DNSTAP jest rekomendowany jako efektywna metoda logowania zdarzeń pozwalająca na ograniczenie kosztów operacyjnych generowanych przez logowanie i przetwarzanie danych DNS w porównaniu do tradycyjnego podejścia query logging.

Aby zmniejszyć wolumen danych, można odfiltrować wpisy dotyczące znanych bezpiecznych domen przed wysyłką do SIEM. W praktyce oznacza to priorytetowe logowanie zdarzeń dotyczących rejestrów RPZ (*Response Policy Zones*) i innych zdarzeń bezpieczeństwa. Pełny log powinien być zachowany na wypadek późniejszej analizy incydentu. Okres rotacji i retencji logów powinien być określony na podstawie indywidualnych potrzeb środowiska, z uwzględnieniem regulacji prawnych, potrzeb DFIR, typowego czasu wykrycia incydentu, kosztów SIEM/storage, klasyfikacji danych oraz faktycznych możliwości technicznych.

3. Ochrona serwerów autorytatywnych

Serwery autorytatywne przechowują informacje strefowe organizacji, czyli mapowania nazw domen na adresy IP oraz inne rekordy. Kompromitacja takiego serwera pozwala atakującemu przekierować ruch organizacji na dowolną infrastrukturę. Zagrożenia dotyczą zarówno mechanizmów synchronizacji danych między serwerami, jak i samej treści stref.

3.1. Transfery stref

Transfery stref (AXFR/IXFR) to mechanizm replikacji danych DNS między serwerem primary a secondary. W normalnych warunkach to standardowa operacja zapewniająca redundancję oraz odporność usługi na niedostępność związaną np. z awarią. Problem pojawia się, gdy transfer nie jest odpowiednio zabezpieczony, atakujący może wywołać odmowę usługi (DoS) przez masowe żądania transferów albo zmodyfikować przesyłane dane w przypadku „przejęcia” relacji zaufania.

Aby tego uniknąć należy:

- skonfigurować ACL na serwerach primary, aby transfery były dozwolone wyłącznie od znanych adresów IP serwerów secondary;
- zabezpieczyć transfery za pomocą TSIG (*Transaction Signatures*), mechanizmu wzajemnego uwierzytelniania opartego na wspólnym kluczu (rekomenduje się również stosowanie silnych algorytmów HMAC (np. HMAC-SHA256, HMAC-SHA512) oraz wdrażanie bezpiecznych procedur zarządzania i rotacji kluczy);
- rozważyć wykorzystanie ZONEMD RR do weryfikacji integralności przesłanych danych strefowych;
- wyłączyć całkowicie transfery na serwerach secondary, chyba że są źródłem dla kolejnych secondary;
- wdrożyć mechanizmy ograniczania częstości żądań (*rate limiting*), szczegółowe logowanie i monitorowanie transferów oraz alertowanie o nietypowym ruchu – jeżeli jest to możliwe, a architektura środowiska zakłada, że nie wpłynie to na jego dostępność lub wydajność,;
- monitorować żądania typu AXFR pochodzące z niezaufanych źródeł w celu wykrywania zagrożeń.

3.2. Higiena DNS i integralność domen

Część incydentów związanych z DNS nie wynika tylko z zaawansowanych ataków. Odpowiedzialne mogą być również zaniedbania administracyjne, tj. dług technologiczny, brak zasobów lub brak kompetencji. Wygasła delegacja, zapomniany rekord CNAME albo brak monitoringu nowych rejestracji stwarzają podatności, które atakujący chętnie wykorzystują.

Najczęstsze problemy

Lame delegations: błędna delegacja strefy, w której rekordy NS wskazują na nieistniejący serwer

Aby temu przeciwdziałać należy regularnie weryfikować poprawność delegacji.

Dangling DNS records: rekord CNAME lub A wskazujący na nazwę lub adres IP, które nie są już kontrolowane przez organizację (np. zasoby w chmurze publicznej)

Może pozwolić atakującemu na zarejestrowanie takiej nazwy i przejęcie kontroli nad procesem rozpoznawania nazw. Aby temu przeciwdziałać, należy regularnie i automatycznie audytować i usuwać niepotrzebne rekordy DNS (ang. DNS scavenging)."

Look-alike domains: atakujący rejestrują domeny łudząco podobne do oficjalnych, wykorzystując techniki (typosquatting, homoglify)

Aby przeciwdziałać tego typu atakom, zaleca się monitorowanie nowych rejestracji domen podobnych do własnych oraz defensywną rejestrację wariantów, które mogłyby zostać wykorzystane przez atakujących.**Zone drift/thrash:** zbyt duże wartości Refresh w SOA powodują rozbieżności danych (drift), zbyt małe, nadmierne obciążenie (thrash). Zalecany zakres Refresh to 1200-864000 sekund.

W ramach higieny własnych stref DNS należy regularnie weryfikować, jakie informacje o organizacji są publicznie widoczne z zewnątrz. Znane są przypadki, w których rekordy DNS zawierały np. prywatne adresy IP z przestrzeni RFC 1918, czyli informacje, które nie powinny być publicznie dostępne. Tego rodzaju dane mogą posłużyć atakującemu do mapowania wewnętrznej infrastruktury bez konieczności uzyskania dostępu do sieci. Rekomenduje się przeprowadzenie audytu publicznych rekordów DNS organizacji oraz cykliczne powtarzanie tego procesu.

3.3. Dynamiczne aktualizacje

W wielu sieciach serwery DHCP automatycznie dodają rekordy DNS dla nowo przyłączonych hostów poprzez mechanizm dynamicznych aktualizacji (RFC 2136). Z punktu widzenia zarządzania infrastrukturą jest to rozwiązanie bardzo wygodne, należy jednak pamiętać, że niesie ono ze sobą pewne ryzyko. Jeśli aktualizacje mogą być przeprowadzane bez uwierzytelnienia, atakujący może dodać własne rekordy do strefy, usunąć istniejące albo zalać serwer masowymi żądaniami aktualizacji, co jest bardziej obciążające niż zwykłe zapytania.

W celu przeciwdziałania temu zagrożeniu, zaleca się:

- akceptowanie aktualizacji wyłącznie od uwierzytelnionych nadawców (TSIG lub ACL)
- używanie hidden primary przeznaczonych dla stref z dynamicznymi aktualizacjami.

3.4. Wartości TTL

TTL (*Time-to-Live*) określa jak długo rekord DNS ma być przechowywany w cache serwera rekurencyjnego. Zbyt krótki TTL generuje nadmierny ruch do serwerów autorytatywnych, a zbyt długi powoduje, że stare dane długo pozostają w cache po zmianie.

Rekomendowany zakres TTL to 1800 sekund (30 min) do 86400 sekund (24h) dla większości rekordów. TTL równy 0 nigdy nie powinien być używany. Wartość 0 powoduje problemy w niektórych implementacjach cache. Nawet wartość 5-30 sekund jest lepsza niż 0. Dla stref podpisanych DNSSEC, TTL musi być krótszy niż okres ważności podpisu RRSIG w przeciwnym razie klienci mogą trafić na wygasły podpis zanim rekord zostanie odświeżony.

4. DNSSEC – ochrona integralności danych DNS

Standardowy DNS nie ma żadnego mechanizmu weryfikacji, czy odpowiedź rzeczywiście pochodzi z właściwego serwera i czy nie została zmodyfikowana po drodze. DNSSEC rozwiązuje ten problem

poprzez dodanie podpisów cyfrowych do rekordów DNS. Resolver walidujący może sprawdzić podpis i odrzucić sfałszowaną odpowiedź.

Ważne jest rozróżnienie, że:

- DNSSEC chroni integralność danych (czy odpowiedź jest prawdziwa), ale nie zapewnia poufności (kto widzi zapytanie),
- poufność to zadanie dla DoT, DoH i DoQ, opisanych w rozdziale 5.

4.1. Algorytmy i parametry kluczy

Wybór algorytmu podpisu ma praktyczne konsekwencje, wpływa bowiem na rozmiar odpowiedzi DNS (a co za tym idzie, na wydajność) i na poziom bezpieczeństwa.

Akceptowalne algorytmy:

Algorytm	Kod DNSSEC	Dł. klucza (bity)	Dł. podpisu (bity)
RSA z SHA-256	8	2048+	~2050-4100
ECDSA P-256 z SHA-256	13	256	512
ECDSA P-384 z SHA-384	14	384	768
Ed25519	15	256	512
Ed448	16	456	912

Algorytmy ECDSA i Ed25519/Ed448 są preferowane ze względu na mniejsze rozmiary kluczy i podpisów, co przekłada się na mniejsze odpowiedzi DNS. Minimalna siła kryptograficzna 112 bitów obowiązuje do 2030 roku, po czym wzrasta do 128 bitów.

Czas życia kluczy podpisujących (ZSK/KSK) powinien wynosić 1-3 lata. Okres ważności podpisów DNSKEY RRSIG powinien być krótki (5-7 dni), aby ograniczyć okno eksploitacji w razie kompromitacji klucza. Tam, gdzie to praktyczne, zaleca się przechowywanie kluczy prywatnych (zwłaszcza KSK) w HSM.

4.2. NSEC vs NSEC3

W stosunku do wcześniejszych wersji dokumentu zmienia się podejście do NSEC/NSEC3, rekomendowane jest użycie NSEC zamiast NSEC3. NSEC3 miał utrudniać enumerację stref (zone walking), ostatecznie wpłynął na zmniejszenie liczby wektorów ataku do brute force, co przełożyło się na wzrost kosztu ataku, niestety nadal nieeliminując możliwości enumeracji stref. Jednocześnie generuje dodatkowe obciążenie obliczeniowe, ponieważ generowanie i weryfikacja NSEC3 wymaga obliczeń hashujących (z wielokrotnymi iteracjami w zależności od parametru), a przy wysokich współczynnikach iteracji koszt CPU rośnie. Jeśli lokalna polityka wymaga NSEC3, parametry powinny być ustawione zgodnie z RFC 9276, aby zminimalizować ryzyko niedostępności usługi spowodowane przeciążeniem serwera.

5. Ochrona serwerów rekurencyjnych

REKOMENDACJA CSIRT KNF
Serwery rekurencyjne powinny stanowić kontrolowany punkt widoczności i inspekcji, ponieważ ich obejście istotnie obniża skuteczność ochrony.

Serwery rekurencyjne działają w imieniu klientów: odbierają zapytanie od stub resolvera (uproszczonej implementacji klienta DNS działającego na urządzeniu końcowym, operującego zgodnie z modelem klient-serwer i wysyłającego zapytania rekurencyjne do resolvera), a następnie same odpytują łańcuch

serwerów autorytatywnych, aż znajdą odpowiedź. To czyni je atrakcyjnym celem ataków, ponieważ zatrucie cache takiego serwera pozwala przekierować ruch wielu klientów jednocześnie. Poza tym tradycyjna komunikacja DNS odbywa się otwartym tekstem, co umożliwia pasywną obserwację oraz spoofing.

5.1. Szyfrowanie DNS (Encrypted DNS)

Tradycyjnie komunikacja DNS odbywa się otwartym tekstem na porcie UDP/53. W określonych przypadkach, np. jeżeli odpowiedź serwera jest zbyt duża lub jeżeli serwer preferuje protokół TCP, następuje przejście na komunikację za pośrednictwem TCP/53. Gdy wykorzystywany jest protokół DoT (DNS over TLS), ruch odbywa się na porcie TCP/853. Każdy, kto ma dostęp do sieci, może monitorować zapytania DNS i na tej podstawie profilować użytkowników, identyfikować odwiedzane serwisy albo podmieniać odpowiedzi (DNS spoofing). Szyfrowanie ruchu DNS minimalizuje te zagrożenia.

W architekturach opartych na zasadach zero trust DNS może pełnić rolę źródła danych dla decyzji bezpieczeństwa oraz punktu egzekwowania polityk. Model taki zakłada, że ruch do zasobów sieciowych jest powiązany z wcześniejszą, kontrolowaną rezolucją nazwy domenowej, a resolver DNS dostarcza informacji wykorzystywanych przez inne elementy infrastruktury bezpieczeństwa. Utrudnia to komunikację z infrastrukturą C2, zwłaszcza gdy malware próbuje ominąć standardowy proces rozpoznawania nazw albo korzysta z domen generowanych algorytmicznie. Ponieważ DNS staje się w takim modelu elementem sterowania polityką bezpieczeństwa, istotne jest zapewnienie integralności i poufności komunikacji DNS oraz utrzymanie centralnej widoczności zdarzeń.

Z uwagi na zalety szyfrowanej komunikacji DNS należy rozważyć jej wdrożenie zwłaszcza na odcinkach klient-resolver korporacyjny oraz resolver-upstream, tam gdzie jest to technicznie możliwe i nie koliduje z wymaganiami monitorowania, inspekcji oraz egzekwowania polityk bezpieczeństwa. NIST wskazuje, że amerykańskie agencje federalne FCEB są zobowiązane do stosowania szyfrowanego DNS w komunikacji z endpointami wszędzie tam, gdzie jest to technicznie wspierane; dla innych organizacji pozostaje to dobrą praktyką wdrażaną po analizie ryzyka.

Dostępne są trzy protokoły szyfrujące komunikację DNS:

1. DoT (DNS over TLS) – port TCP/853
2. DoH (DNS over HTTPS) – porty TCP/443 i UDP/443
3. DoQ (DNS over QUIC) – port UDP/853

Wszystkie trzy protokoły, przy właściwej konfiguracji, pozwalają na uwierzytelnienie serwera DNS przez klienta oraz zapewniają poufność i integralność transakcji DNS pomiędzy klientem a resolverem. Nie zastępują jednak DNSSEC: szyfrowanie DNS chroni kanał komunikacji, natomiast DNSSEC chroni integralność i autentyczność danych DNS w odpowiedziach. W celu podniesienia poziomu bezpieczeństwa systemu DNS należy, na podstawie wcześniejszego oszacowania ryzyka, rozważyć wdrożenie szyfrowania DNS tam, gdzie jest to technicznie możliwe i uzasadnione. W szacowaniu ryzyka należy uwzględnić, że szyfrowanie ruchu DNS ogranicza możliwość tradycyjnego monitorowania i inspekcji ruchu DNS na poziomie sieci, co ma istotne konsekwencje dla systemów klasy IDS/IPS oraz zapór NGFW. Szyfrowanie DNS poprawia prywatność i integralność kanału pomiędzy klientem, a resolverem, ale osłabia tradycyjną widoczność sieciową. Pełna ochrona wymaga więc połączenia kilku podejść, takich jak:

- blokowanie nieautoryzowanych resolverów i dopuszczanie tylko znanych adresów IP resolverów korporacyjnych,
- telemetria endpointowa, np. z systemów EDR/XDR,
- centralne logowanie i korelacja zdarzeń z resolverów, np. w SIEM/SOAR lub platformie DNS Security,
- stosowanie inspekcji TLS/QUIC tam, gdzie jest to możliwe i dozwolone, z uwzględnieniem skutków prawnych oraz wpływu na prywatność użytkowników.

Urządzenia IoT, które nie obsługują szyfrowania, powinny komunikować się przez lokalny forwarder DNS.

5.2. Ograniczenie dostępu do publicznych usług DNS

Nawet najlepsza konfiguracja firmowych resolverów nic nie da, jeśli użytkownicy (albo aplikacje) omijają je na rzecz publicznych usług DNS typu 8.8.8.8 czy 1.1.1.1. Wiele przeglądarek domyślnie włącza DoH do własnych resolverów, co skutecznie omija całą lokalną infrastrukturę bezpieczeństwa.

Dobrym podejściem architektonicznym jest wymuszenie obsługi ruchu DNS przez centralny resolver korporacyjny lub inny kontrolowany punkt pośredniczący oraz blokowanie bezpośredniego dostępu do zewnętrznych resolverów. Poniższe środki techniczne odpowiadają rekomendacjom NIST dotyczącym ograniczenia korzystania z publicznych usług DNS i adresują specyficzne wektory obejścia, w szczególności DoH wbudowany w przeglądarki i aplikacje.

Aby temu zapobiec należy:

a) blokować wychodzący ruch DNS (UDP/TCP 53) z sieci wewnętrznej do internetu, z wyjątkiem autoryzowanych serwerów wewnętrznych;
b) blokować nieautoryzowany ruch DoT (TCP 853) i DoQ (UDP 853) przez reguły firewall;
c) blokować nieautoryzowany DoH przez RPZ (blokada domen znanych serwerów DoH) i reguły firewall;
d) konfigurować przeglądarki i aplikacje, aby nie omijały lokalnych resolverów na rzecz wbudowanych DoH;
e) stosować MDM/EMM lub GPO do wymuszania konfiguracji DNS na urządzeniach mobilnych.

5.3. QNAME Minimization

Domyślnie serwer rekurencyjny wysyła pełną nazwę zapytania (QNAME) do każdego serwera w łańcuchu rozpoznawania, czyli np. serwer root i serwer TLD dowiadują się, że klient chce się połączyć z konkretnym adresem, mimo że potrzebują tylko wiedzieć, dokąd skierować kolejne zapytanie.

QNAME Minimization rozwiązuje problem przesyłania nadmiarowych danych w taki sposób, że serwer rekurencyjny ujawnia tylko tę część nazwy, która jest niezbędna do uzyskania następnego kroku delegacji. Koszt ewentualnych dodatkowych zapytań jest minimalny i maleje w miarę cache'owania zapytań. Warto więc rozważyć włączenie opisywanej funkcji na serwerach rekurencyjnych.

5.4. Wykrywanie eksfiltracji danych przez DNS

DNS może być używany jako kanał do eksfiltracji danych z organizacji. Wykorzystując proste techniki kodowania lub bardziej zaawansowane metody maskowania, atakujący może umieszczać dane w zapytaniach DNS dotyczących subdomen w kontrolowanej przez siebie domenie (np. base64-dane.evil.com). Technika ta pozwala na przesłanie zarówno pojedynczych ciągów znaków, jak i całych plików, np. .docx lub PDF.

Ponieważ ruch DNS jest zwykle przepuszczany przez firewalle, jeżeli nie są wykorzystywane rozwiązania typu explicit proxy, tego typu eksfiltracja bywa trudna do wykrycia standardowymi narzędziami. W celu zabezpieczenia się przed tego rodzaju atakami konieczne jest wdrażanie wyspecjalizowanych rozwiązań zabezpieczających ruch DNS na poziomie resolvera.

Skuteczność detekcji DNS exfiltration zależy od tego, czy organizacja ma wgląd w ruch DNS. Jeśli stacje robocze mogą odpytywać dowolne zewnętrzne resolvery bezpośrednio, analizie podlega tylko fragment ruchu. Dlatego warunkiem wstępnym detekcji jest wymuszenie całego ruchu DNS przez resolver korporacyjny, np. poprzez explicit proxy DNS i zablokowanie wychodzącego UDP/TCP 53 do adresów innych niż autoryzowany resolver.

Przy takim modelu resolver staje się jedynym punktem, w którym analiza jest możliwa i gdzie można zastosować konkretne kontrole ograniczające eksfiltrację, np.:

a) limit długości QNAME (np. odrzucanie zapytań z etykietą przekraczającą 50 znaków), który bezpośrednio ogranicza możliwość przesyłania base64-encoded payloadów,
b) rate limiting zapytań per host, który ogranicza przepustowość kanału eksfiltracji,
c) blokada zapytań do domen zarejestrowanych niedawno lub niewidzianych wcześniej w sieci,
d) blokada typów rekordów rzadko używanych w normalnym ruchu (TXT, NULL, ANY), które są preferowanymi nośnikami danych w tunelowaniu DNS

– bez centralnego punktu inspekcji mechanizmy te są nieegzekwowalne, IDS/IPS i EDR mogą uzupełniać detekcję, ale nie zastąpią kontroli na poziomie resolvera.

W procesie wykrywania DNS exfiltration warto zwrócić uwagę na:

a) nietypowo dużą liczbę zapytań z jednego hosta,
b) nietypowe wzorce zapytań,
c) wysoką entropię w QNAME (długie, losowo wyglądające nazwy),
d) zapytania do znanych złośliwych domen.

Narzędzia działające na podstawie detekcji sygnatur wykryją popularne narzędzia do tunelowania (iodine, dnscat2), ale warto też wykorzystywać mechanizmy detekcji pozwalające na wykrywanie anomalii w ruchu DNS, z uwagi na możliwość wykorzystywania niestandardowych narzędzi do wykonania tego rodzaju ataku.

6. Architektura i odporność infrastruktury DNS

REKOMENDACJA CSIRT KNF
Architektura DNS powinna zakładać separację ról, wysoką dostępność oraz minimalizację informacji ujawnianych przez publiczne strefy.

Bezpieczeństwo DNS zależy nie tylko od konfiguracji samej usługi, ale także od utwardzenia systemu operacyjnego, segmentacji sieci, kontroli dostępu, monitorowania oraz procesu aktualizacji. Kompromitacja któregokolwiek z tych elementów może doprowadzić do przejęcia całej usługi DNS. Dlatego architektura systemu DNS oraz sposób wdrożenia mają znaczenie dla jego bezpieczeństwa.

6.1. Separacja ról

Serwer DNS może pełnić dwie różne role: autorytatywną (serwuje dane strefowe) i rekurencyjną (rozpoznaje nazwy w imieniu klientów). Każda z tych ról ma inny profil zagrożeń i wymaga innej polityki bezpieczeństwa. Łączenie ich na jednym serwerze dostępnym z internetu zwiększa powierzchnię ataku.

- Serwer dostępny z Internetu powinien pełnić wyłącznie jedną rolę albo autorytatywną, albo rekurencyjną. Łączenie ról jest dopuszczalne tylko dla serwerów wyłącznie wewnętrznych.
- Infrastruktura DNS powinna być przeznaczona dla danej organizacji; nie powinno się uruchamiać innych usług na tych samych maszynach, z wyjątkiem powiązanych usług, takich jak DHCP.

Oprogramowanie serwera DNS powinno być usunięte z hostów, które nie pełnią roli name serwerów

6.2. Wysoka dostępność

Awaria DNS oznacza niedostępność całej sieci: aplikacje, poczta, VPN i systemy wewnętrzne przestają działać. Dlatego infrastruktura DNS musi być projektowana z myślą o ciągłości działania.

- Każda strefa musi mieć serwer primary i co najmniej jeden secondary.
- Serwery autorytatywne powinny być rozproszone geograficznie i sieciowo (różne segmenty, różne lokalizacje fizyczne).
- Stosować koncepcję hidden primary – serwer z rolą primary nie powinien być widoczny w rekordzie NS; widoczne powinny być tylko serwery z rolą secondary. Taka konstrukcja chroni serwer primary przed bezpośrednimi atakami.
- Hidden primary powinien akceptować transfery stref wyłącznie od autoryzowanego zbioru serwerów secondary (kontrolowane listą ACL) i odrzucać wszystkie inne żądania.

6.3. Minimalizacja wycieku informacji

DNS z założenia jest protokołem publicznym, każdy może odpytać serwer autorytatywny o rekordy danej strefy. Nie wszystkie wycieki da się wyeliminować, ale można ograniczyć ilość informacji przydatnych atakującemu do rekonesansu.

Na strefach zewnętrznych należy unikać publikowania rekordów typu RP (*responsible person*), HINFO (informacje o systemie operacyjnym hosta), LOC (lokalizacja) oraz niepotrzebnych rekordów TXT.

Atakujący mogą je wykorzystać do mapowania infrastruktury. Rekordy TXT niezbędne do działania mechanizmów uwierzytelniania e-mail (SPF, DKIM, DMARC) powinny pozostać, ale każdy inny przypadek wymaga indywidualnej oceny.

7. Podsumowanie rekomendacji

Obszar	Rekomendacja
Protective DNS	Wdrożyć protective DNS w modelu dopasowanym do ryzyka (on-premises, cloud lub hybrydowym). Integrować z SIEM/SOAR.
Szyfrowanie DNS	Rozważyć DoT/DoH/DoQ na odcinkach, gdzie nie ograniczy to wymaganej widoczności i egzekwowania polityk. Blokować nieautoryzowany ruch DNS.
DNSSEC	Podpisywać strefy zewnętrzne. Włączyć walidację DNSSEC na resolverach. Preferować ECDSA/Ed25519/Ed448 zamiast RSA tam, gdzie jest to wspierane.
Transfery stref	Ograniczyć ACL. Zabezpieczyć TSIG. Stosować ZONEMD.
Separacja ról	Nie łączyć ról autorytatywnej i rekurencyjnej na serwerach dostępnych z internetu.
Wysoka dostępność	Hidden primary + rozproszone secondary Minimum dwa serwery w różnych segmentach sieci
Higiena DNS	Audytować delegacje, CNAME, rekordy informacyjne. Monitorować look-alike domeny.
Logowanie	Logować zdarzenia DNS, w szczególności blokady protective DNS. Preferować DNSTAP i integrować logi z SIEM.
Eksfiltracja DNS	Wymusić centralny punkt inspekcji DNS. Monitorować entropię QNAME, wolumen zapytań i nietypowe typy rekordów.
TTL	Zakres 1800-86400 sek Nigdy TTL=0. Dla DNSSEC: TTL < okres ważności RRSIG

Pełna treść dokumentu źródłowego jest dostępna pod adresem:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81r3.pdf

Dokument został opracowany we współpracy z ekspertami cyberbezpieczeństwa z sektora publicznego oraz prywatnego.

Dziękujemy za współpracę.
Zespół CSIRT KNF

Znaczenie kolorów TLP dla odbiorców wiadomości

TLP: RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.
TLP: AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów i consituency) z osobami, które muszą poznać wiadomości oraz jedynie w zakresie niezbędnym do podjęcia odpowiednich działań. Dodatkowe ograniczenia mogą zostać wyspecyfikowane przez nadawcę w dowolnym zakresie i muszą być przestrzegane. Jednym ze standardowych ograniczeń jest oznaczenie TLP:AMBER+STRICT, które pozwala dzielić się informacjami wyłącznie w obrębie organizacji.
TLP: GREEN	Odbiorcy mogą dzielić się informacjami ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP: CLEAR	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).

Zespół