Zagrożenia i przypadki fałszowania czasu w publicznej usłudze NTP POOL

Tomasz Widomski Krzysztof Borgulski
ELPROMA Elektronika Sp. z o.o. 05-152 Czosnów, ul. Duńska 2a, Polska (EU)
www.elpromaelectronics.com e-mail: info@elpromaelectronics.com

BIOGRAFIA

Tomasz Widomski, Absolwent Informatyki Politechniki Warszawskiej (PW). Ukończył studia podyplomowe w Szkole Głównej Handlowej (SGH) i MBA Cyberbezpieczeństwo na Wojskowej Akademii Technicznej (WAT). Od 35 lat związany z firmą Elproma - krajowy producent serwerów czasu NTP/PTP odpornych na jamming/spoofing GPS. Akredytowany przez Ministerstwo Cyfryzacji KPRM, krajowy delegat do ITU w Genewie przy ONZ. Konsultant Europejskiej Agencji Przemysłu Kosmicznego (EUSPA). Ekspert ds. cyberbezpieczeństwa infrastruktur krytycznych w obszarze synchronizacji IT/OT. Zarządzał polskim zespołem w międzynarodowych projektach Horizon 2020 DEMETRA, White Rabbit CERN oraz krajowym projektem eCzasPL w Głównym Urzędzie Miar RP.

Krzysztof Borgulski, Specjalista ds. synchronizacji czasu i systemów IT/OT, związany z firmą Elproma od 2008 roku. Współautor rozwiązań wdrożonych w projektach europejskich, takich jak Horizon 2020 DEMETRA, projekt Safe-Time, gdzie odpowiadał za rozwój usług bezpiecznej synchronizacji czasu z wykorzystaniem GNSS, NTP i PTP. Kierował wdrożeniem systemu eCzasPL – państwowego źródła czasu urzędowego UTC(PL), realizowanego we współpracy z Głównym Urzędem Miar RP. Koordynował również projekty realizowane dla infrastruktury krytycznej w Polsce i za granicą, m.in. dla sektora energetycznego**,** instytucji UE oraz struktur NATO. Uczestnik porozumienia PWCyber przy Ministerstwie Cyfryzacji KPRM.

STRESZCZENIE

Dokument omawia zagrożenia bezpieczeństwa związane z fałszowaniem czasu z użyciem sieciowego protokołu synchronizacji Network Time Protocol (NTP) i źródłem czasu publicznej usługi NTPPOOL. Autorzy obszernie dokumentują przypadki manipulacji czasem przez serwery NTP oraz analizują podatności w architekturze usługi Projektu NTP POOL. Podkreślają znaczenie wielopoziomowych zabezpieczeń. Dokument zawiera przykłady incydentów związanych z fałszowaniem czasu oraz zalecenia postępowania.

WSTĘP

Network Time Protocol (NTP[1]) jest standardowym protokołem synchronizacji czasu w sieciach komputerowych. Każda dystrybucja systemu Linux wyposażona jest w protokół NTP, który posiada również pochodne implementacje takie jak NTPsec[1], Chrony[1], NTPd-rs[1] oraz uproszczoną wersję SNTP[1] wbudowaną w systemy operacyjne Windows i Mac.

Projekt NTP POOL[2] to globalna usługa udostępniania wzorcowego źródła czasu UTC dla synchronizacji opartej o NTP. Jest dostępna jako grupa publicznych serwerów czasu. Dzięki routingowi TCP/IP i mechanizmowi równoważenia obciążenia DNS, miliony urządzeń i sieci klienckich mogą korzystać nieodpłatnie z tysięcy rozproszonych serwerów czasu. W praktyce NTP POOL jest domyślnym źródłem czasu znacznie większej ilości urządzeń, ponieważ większość routerów IP i urządzeń sieciowych IoT opiera swój *firmware* na systemie Linux.

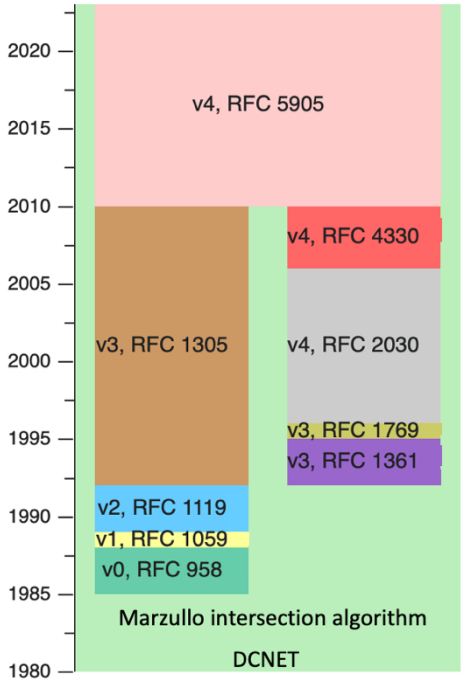
Poprawna synchronizacja jądra *kernel OS* systemów Linux i Windows ma obecnie krytyczne znaczenie dla stabilnej pracy całych systemów teleinformatycznych. Wpływa na porządek zdarzeń w dziennikach LOG, ważność cyfrowych certyfikatów, działanie uwierzytelniania (np. *Kerberos*), ważność kluczy szyfrujących oraz wielu innych mechanizmów bezpieczeństwa. Znacznie mniej znana, choć bardzo ważna, jest rola czasu w operacjach niskopoziomowych[3] *OS kernel*, gdzie znajduje się organizacja procesów i współbieżności.

Praca nawiązuje do rozdziału monografii [3] p.t. „*Atak na czas, opóźnienie i synchronizację IT/OT – skuteczna cyberbroń przyszłości*” Tomasza Widomskiego oraz do wcześniejszych publikacji [1][2]. Zawiera analizę bezpieczeństwa NTP POOL jaką w latach 2022 i 2025 dyskutowała Rada ds. Cyfryzacji (RdC) przy Ministerstwie Cyfryzacji KPRM. Rozdział dokumentuje znane incydenty ataków NTP praz NTPPOOL, podatności w architekturze usługi, rekomenduje metody ochrony oraz rozszerza zakres uzasadnienia dotychczasowej uchwały RdC[4]. MC KPRM z dnia 3 lutego 2023.

[1] https://en.wikipedia.org/wiki/Network_Time_Protocol.
[2] https://www.ntppool.org/en/.
[3] https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf (strona 28).
[4] https://mc.bip.gov.pl/fobjects/download/1173326/uchwala-nr-2-rdc-pdf.html.

BEZPIECZEŃSTWO WBUDOWANE W NTP

Standardowa konfiguracja NTP nie zapewnia kryptograficznego uwierzytelnienia źródeł czasu (serwerów), mimo że zaczynając od wersji 3 z 1993 r. protokół ten posiada wbudowany mechanizm jednoznacznego powiązania klientów z serwerami czasu przy użyciu kluczy symetrycznych, a od wersji 4 z 2010 r. chroni ona w infrastrukturze kucza publicznego PKI do dziś miernie działającą automatykę zarządzania wymianą tych kluczy (rysunek 1).

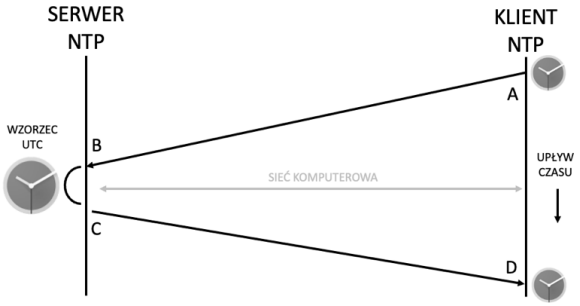


Rys. 1 Ewolucja RFC protokołu NTP
Źródło: Wikipedia[1]

W historycznym ujęciu, już od ponad 40 lat protokół NTP posiada więc wszelkie niezbędne mechanizmy chroniące go przed manipulacją czasem, ale są one miernie zrozumiałe i dlatego najczęściej niestosowane w praktyce. Problem nie omija również liderów IT takich jak firma Microsoft, która przez wiele lat opierała system Windows na usłudze Time32, której do dziś zdecydowanie bliżej jest do uproszczonej wersji SNTP[5]. Dobrą wiadomością jest to, że referencyjna pełna wersja NTP może być samodzielnie skompilowana ze źródłowego kodu w języku C i uruchomiana w dowolnym środowisku Windows. Wartym docenienia jest, że używając pełnej wersji NTP uzyskujemy automatycznie mechanizm wykrywania fałszywych źródeł *falsetickers* czasu UTC, pod warunkiem używania wielu serwerów NTP jednocześnie. Pełna wersja NTP ma wbudowany mechanizm DTS Intersection[6] oparty na algorytmie K. Marzullo[7]. Niestety pozostaje to miernie zrozumiałe dla większości administratorów IT, którzy zbyt powierzchownie traktują czas, ograniczając jego rolę wyłącznie do funkcji informacyjnej. Tym czasem desynchronizacja rozproszonej architektury teleinformatycznej może prowadzić do poważnych awarii. To niedoceniane ryzyko pozostawia szeroko otwarte tylne drzwi do licznych cyberataków[8] - również tych spoza synchronizacji.

PRZYPADKI MANIPULACJI CZASEM PRZEZ SERWERY NTP

Wymiana pakietów synchronizacyjnych NTP odbywa się w formie niezaszyfrowanej wiadomości tekstowej wysyłanej warstwą transportową UDP. Oznacza to, że atakujący *Man-in-the-Middle*[8] (MITM) może łatwo podsłuchiwać i modyfikować pakiety synchronizacyjne. W konsekwencji ma on możliwość **opóźniania** pakietu, **powtarzanie,** a nawet **podmianę** całej zawartości. Ostatecznie skutkuje to nieprawidłowym obliczeniem rozbieżności czasu między klientem a serwerem (*offset*), a w konsekwencji błędnym ustawieniem zegara klienta. Rozbieżność czasu klienta względem serwera NTP liczona jest w obiegu pakietu UDP po punktach ABCD (rysunek 2). Pomiar zaczyna się od klienta NTP w punkcie A i przebiega przez serwer czasu (punkty B i C) powracając do klienta w punkcie D. Jest to tzw. *round-trip NTP,* gdzie w każdym punkcie do transmisji dokładany jest lokalny znacznik czasu nadania lub odbioru w każdym z punktów. W oparciu o znaczniki czasu ABCD obliczane jest opóźnienie *delay* jakie wnosi sieć TCP/IP włączając routing. Następnie klient NTP sam oblicza *offset* własnego zegara i koryguje go samodzielnie. Opóźnienie *delay* wyrażone jest wzorem [(D-A) - (C-B)], a *offset* wyznacza się jako ½[(B-A) + (C-D)]. Zaburzenie wartości któregokolwiek ze znaczników ABCD skutecznie doprowadza do desynchronizacji[9].

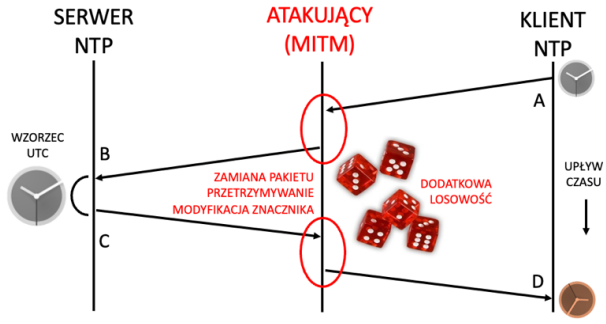


Rys. 2 Round-Trip NTP. W każdym punkcie ABCD pobierany jest l znacznik czasu wg. lokalnego zegara.
Źródło: własne

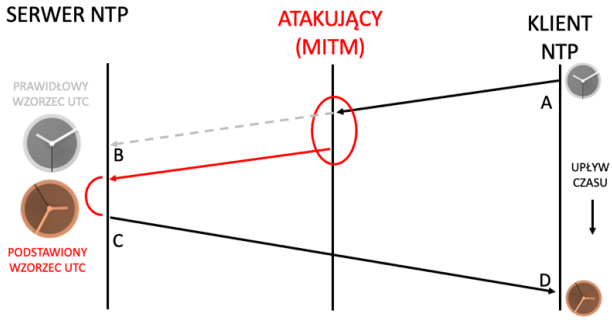
Ale nawet kryptograficzne uwierzytelnienie nie eliminuje w całości ryzyka ataku MITM, ponieważ *Man-in-the-Middle* może nie zmieniać zawartości pakietu NTP, a jedynie przetrzymywać go tworząc opóźnienie *delay* (rysunek 3). Przeciwdziałać temu nie może nawet kryptograficzne uwierzytelnienie NTP. Szczególnie niebezpieczne są losowe opóźnienia pakietów tworzące szum *jitter* fałszujący korekcję *offset* zegara klienta *i delay* sieci. Prowadzi to do niemierzalnej na poziomie pakietów NTP desynchronizacji, ale odczuwalnej przez systemy IT i OT.

[5] https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-sntp/8106cb73-ab3a-4542-8bc8-784dd32031cc.
[6] https://en.wikipedia.org/wiki/Intersection_algorithm.
[7] https://en.wikipedia.org/wiki/Marzullo%27s_algorithm.
[8] https://blog.apnic.net/2022/12/09/securing-ntp-against-mitm-attacks.
[9] https://www.usenix.org/system/files/sec23fall-prepub-520-kwon.pdf.

Z kolei brak kryptograficznego uwierzytelnienia komunikacji umożliwia atak typu sieciowy spoofing NTP, w którym napastnik może podmienić nawet całe serwery NTP z poziomu sieciowego urządzenia pośredniego (rysunek 4).



Rys. 3 Atak MITM z poziomu routera TCP/IP. Pakiety mogą być modyfikowane, podmieniane lub przetrzymywane. Opcjonalna losowości długości opóźnienia bardzo skutecznie zaburza identyfikację ataku. Źródło: własne



Rys. 4 Atak MITM na poziomie routera TCP/IP z przekierowaniem na fałszywy (podstawiony) serwer. Źródło: własne

Udokumentowano szereg scenariuszy ataków na protokół synchronizacji NTP. Warto wyróżnić kilka:

- **Atak**[9] **MITM na NTP**. Napastnik pośredniczący w komunikacji NTP może dowolnie zmienić znaczniki czasu ABCD[2] w odpowiedziach zanim dotrą one do synchronizowanego klienta NTP (rysunek 3, czerwony obszar to miejsce ataku). Atakujący może również „przetrzymać" pakiet NTP wprowadzając dodatkowe opóźnienia (rysunek 3, czerwony obszar jako miejsce przetrzymania pakietu). W ten sposób ofiara otrzymuje nieprawidłowy wzorzec czasu lub zostaje odsunięta od synchronizacji. Tego typu atak może zostać zrealizowany np. poprzez przejęcie kontroli nad routerem lub łączem na drodze do serwera czasu oraz w ramach **ataków**[10] **BGP hijacking** lub **DNS hijacking**, gdzie ruch z prawdziwego serwera NTP jest przekierowywany do serwera kontrolowanego przez atakującego (rysunek 4, patrz również dokument[10], akapit Atak #3).

- **Spoofing**[11] **z użyciem DNS**. Architektura NTP POOL opiera się na zapytaniach symbolicznych DNS (np. *pool.ntp.org*), które zwracają adresy IP serwerów czasu. Jeśli atakujący wykorzysta **podatności systemu DNS** (np. poprzez „zatruwanie" pamięci *cache*) i podsunie ofierze fałszywy rekord DNS, to klient NTP może zostać przekierowany do kontrolowanego przez napastnika serwera NTP udostępniającego błędny czas[11]. Badania pokazują, że jest to realny wektor ataku *off-path,* gdzie atakujący nie musi nawet znajdować się bezpośrednio między klientem a prawdziwym serwerem czasu NTP. Wystarczy manipulacja na poziomie DNS, aby *podmienić* serwer czasu na złośliwy. W roku 2020 zademonstrowano[11] praktyczny atak tego typu, ukierunkowany na klientów protokołu NTP korzystających z niezabezpieczonego DNS.

- **Atak przez fragmentację IP**. Inną techniką *off-path* zaprezentowaną w literaturze[10] jest wykorzystanie fragmentacji pakietów IPv4 do „wstrzyknięcia" własnych znaczników czasu. Eksperci Aanchal i Malhotra (NDSS 2016) pokazali, że można tak spreparować fragmenty pakietów UDP, aby klient NTP złożył z nich fałszywą odpowiedź zawierającą dowolnie przesunięty czas (dokument[10], akapit Atak #4). Choć atak taki wymaga spełnienia restrykcyjnych warunków (m.in. zmuszenia serwera NTP do fragmentacji odpowiedzi i zgrania czasowego tych fragmentów), stanowi to dowód na istnienie możliwości fałszowania czasu nawet przez napastnika, który nie ma bezpośredniego dostępu do ofiary.

- **Wykorzystanie błędów implementacji NTP**[10]. Istotną linią ataku jest także nadużycie mechanizmów kontrolnych samego protokołu *Network Time Protocol*. Na przykład, klient NTP zazwyczaj przerywa synchronizację, gdy przekroczony zostaje parametr *panic threshold* i wykryje się zbyt duże jednorazowe odchylenie czasu >1000s. Ma to zapobiec dużym spowodowanym błędem, które NTP domniemuje, że jest to spowodowane awarią sprzętu. Jednak badania wykazały możliwość obejścia zabezpieczenia *panic threshold*, poprzez wymuszenie restartu usługi (demona) *ntpd* lub jego odpowiedników[1] u ofiary. Osiąga się to stosując kombinację małych i dużych korekt czasu, tuż po ponownym uruchomieniu demona. **Atakiem "small-step-big-step"**, można skłonić klienta do zaakceptowania nawet znacząco dużej fałszywej zmiany czasu zegara klienta NTP, a następnie przywrócić zegar do pozornie normalnego biegu (dokument [10] - Atak #3). Taka sztuczka pozwala niezauważenie przedstawić datę w przyszłość, powodując wygaśnięcie określonych obiektów kryptograficznych (certyfikatów i tokenów), po czym cofnąć czas do prawidłowej wartości, utrudniając wykrycie manipulacji czasem.

[10] https://www.cs.bu.edu/~goldbe/papers/NTPattacks.html

[11] https://arxiv.org/pdf/2010.09338.

Obok wyżej wspomnianych zagrożeń istnieją też bardziej specjalistyczne sposoby wywoływania desynchronizacji w rozproszonych systemach IT/OT, które zostały opisane w literaturze [1][2][3].

Warto podkreślić, że w przeszłości zdarzały się również incydenty niezwiązane wprost z atakami, ale pokazujące odczuwalne skutki błędów czasu i daty. Na przykład, błędy oprogramowania i konfiguracji NTP powodowały, że niektóre serwery czasu podatne były na interpretację dodatkowej nowej **sekundy przestępnej**[3] **UTC** (ang. *leap second*)**,** czy tworzyły problemy z synchronizacją wynikającą z błędu w naziemnej telemetrii systemu satelitarnego GPS[12] (problem znany jako błąd satelity SVN #23). Choć często były to przypadki nieumyślne, skutkowały poważnymi zakłóceniami pracy całych systemów infrastrukturalnych, zaczynając od błędów w dziennikach LOG, aż po awarie IT dużej skali. Incydenty takie pouczają, że standardowe mechanizmy wykrywania nieprawidłowego czasu w protokole NTP nie zawsze są wystarczające, a zdeterminowany atakujący może celowym działaniem wywołać bardzo podobne objawy do tej awarii w PLK[13] z dnia 17 marca 2022.

PODATNOŚCI W ARCHITEKTURZE NTP POOL

Architektura usługi NTP POOL, choć zaprojektowana z myślą o niezawodności i dostępności czasu posiada słabości, które potencjalnie może wykorzystać atakujący w celu fałszowania czasu i to na masową skalę:

- **Brak kryptograficznego uwierzytelnienia.** Projekt NTP Pool opiera się na zaufaniu do anonimowych serwerów czasu, udostępnionych dobrowolnie przez ochotników dzielących się publicznie posiadanym sprzętem. Ponieważ protokół NTP w podstawowej konfiguracji nie weryfikuje kryptograficznie źródła czasu UTC to synchronizowany klient zakłada, że odpowiedź pochodzi od prawdziwego serwera czasu. Jeśli atakujący zdoła włamać się i **skompromitować serwer** lub **dodać własny złośliwy** do NTP POOL, to taki serwer czasu będzie traktowany przez używających go klientów na równi z innymi. Badania z 2021 r. wykazały, że już przejęcie kontroli nad niewielką liczbą serwerów NTP POOL rozlokowanych w popularnych regionach wystarczy, aby zauważalnie przesunąć czas u wielu klientów NTP w skali całego kraju, a nawet kontynentu[14]. Innymi słowy, pojedynczy **agresor dysponujący w publicznej przestrzeni NTP POOL podstawionymi serwerami czasu jest w stanie przestawić czas o minuty, godziny i dni na ogromnej liczbie systemów informatycznych** korzystających z puli. To stanowi poważne ryzyko dla integralności wielu ważnych usług IT[13]. Co więcej, samo **dołączenie nowego serwera czasu do NTP POOL jest względnie proste**. Procedury weryfikacji serwerów publicznych NTP skupiają się głównie na kontroli stabilności i dokładności wystawianego publicznie wzorca czasu UTC, a nie na tożsamości właściciela. Nie identyfikują też pierwotnego źródła UTC ani powiązań serwera w hierarchii STRATUM[1]. To oznacza, że potencjalny napastnik może zgłosić do publicznej puli własne serwery czasu, działające początkowo prawidłowo, aby zdobyć zaufanie systemu nadzorującego, a następnie wykorzystać je w skoordynowany przez siebie sposób do cyber-ataku. Atak taki określa się terminem „zatruwanie" NTP POOL. Jedynym znanym skutecznym **antidotum odtruwania NTP POOL jest statystyczne przeciwstawienie wielokrotnie większej populacji „zdrowych" (niezatrutych) serwerów** czasu kontrolowanych przez wyznaczone do tego celu struktury narodowej metrologii (NMI).

- **Zależność od infrastruktury DNS**. Jak wspomniano, klienci korzystają z puli poprzez subdomeny *pool.ntp.org*, pod które są podstawiane nazwy symboliczne konkretnych publicznych serwerów czasu, te zaś są zamieniane na adresy IP fizycznych serwerów NTP. To właśnie pośrednia warstwa obsługi nazw domen, stanowi dodatkowy wektor ataku, ponieważ **zatruwając DNS** lub przejmując kontrolę nad serwerem, atakujący może przekierować dużą liczbę klientów NTP na dowolnie podstawione przez siebie serwery NTP (rysunek 4). Ale nawet bez włamywanie się na same serwery czasu, manipulacja wpisami DNS pozwala skutecznie wprowadzić do puli adresy należące do agresora[13]. Dopóki klient nie stosuje zabezpieczeń DNSSEC (a większość nie weryfikuje podpisów DNS) i nie używa innych mechanizmów uwierzytelniania, nie odróżni on prawidłowego adresu serwera od fałszywego. W ten sposób **architektura oparta na DNS staje się podatna na ataki spoza ścieżki (off-path)** i wystarczy atak na system nazw, aby oszukać wielu klientów jednocześnie.

- **Ignorowanie zależności między serwerami (STRATUM)**. Mechanizm doboru serwerów czasu w NTP POOL zakłada, że każdy z nich dostarcza niezależny od siebie wzorzec czasu UTC. Ujmując to samo inaczej, poszczególne serwery publiczne nie powinny być ze sobą wzajemnie powiązane powielając (jeden od drugiego) wzorzec czasu UTC. W rzeczywistości serwery NTP tworzą hierarchię[1] *STRATUM 0-15*, gdzie wiele serwerów puli operuje w niższej warstwie i synchronizuje się z serwerami warstwy wyższej. Badacze NTP POOL zauważyli, że algorytm puli nie uwzględnia takich zależności wzajemnych powią-

[12] https://aaltodoc.aalto.fi/handle/123456789/19833.

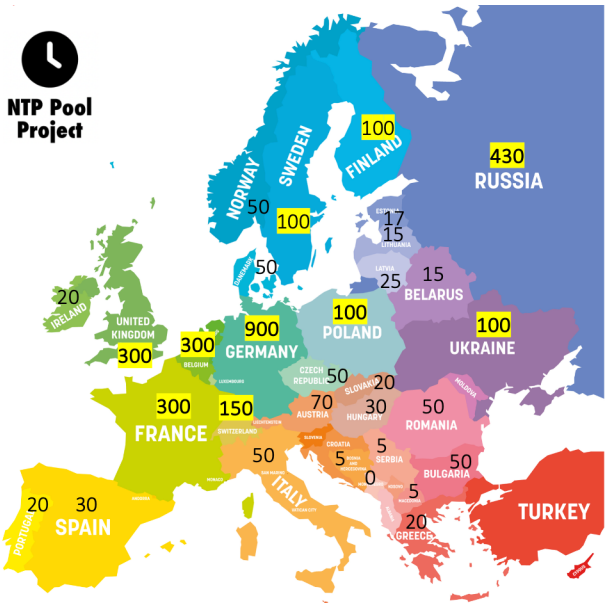
[13] https://www.rynek-kolejowy.pl/wiadomosci/pkp-plk-podsumowuje-wielka-awarie-13-tys-pociagow-opoznionych-kwestia-odszkodowan-otwarta-107221.html.

[14] https://www.ndss-symposium.org/wp-content/uploads/ndss2021_1A-2_24302_paper.pdf.

zań. To oznacza, że jeżeli atakujący przejmie kontrolę nad pewnym kluczowym serwerem *Stratum1*, z którego korzysta wiele innych serwerów *Stratum2* w puli, to może on poprzez manipulację na *Stratum1* pośrednio wpłynąć na zmianę czasu na wielu kolejnych serwerach *Stratum2* itp. W efekcie **sabotaż na poziomie Stratum1 może kaskadowo wprowadzić nieprawidłowości w całej puli regionalnej zawierającej serwery Stratum2, Stratum3 itp.** zwłaszcza, gdy doświadczony atakujący potrafi swobodnie zmodyfikować w NTP wpis numeru warstwy *STRATUM,* stale je utrzymując na poziomie Stratum1 mimo dziedziczności wzorca. Architektura puli nie posiada mechanizmu wykrywania takich *zależności tranzytowych*, co stanowi ważną podatność infrastruktury NTP POOL.

- **Ograniczenia ze strony systemu monitorowania NTP POOL.** Projekt utrzymuje specjalne serwery monitorujące, które regularnie sprawdzają zarejestrowane publiczne serwery czasu pod kątem poprawności czasu i dostępności usługi NTP. Jeśli publiczny serwer NTP zwraca czas znacznie odbiegający od wzorca UTC, jego wskaźnik *sscore* wiarygodności spada i ostatecznie zostaje on usunięty z puli, stając się niedostępnym do czasu poprawy własnego wyniku. Jednak najnowsze analizy SEC'23 wykazały, że ten **system badania „zdrowia" NTP POOL również można oszukać**[15]. Przykładowo, **atakujący może sztucznie wprowadzać opóźnienia sieciowe** *delay* między monitorem a wybranymi przez siebie serwerami puli. Może też wpłynąć na zegar samego serwera monitorującego NTP po to, aby spowodować błędne oceny *score*. W rezultacie można celowo „wypchnąć" z publicznej puli serwery prawidłowe i pozostawić te błędnie wskazujące czas.
  W skrajnym przypadku atakujący, dysponując wieloma złośliwymi serwerami w NTP POOL oraz dodatkowo wspierając się fałszywymi monitorami puli, może doprowadzić do usunięcia większości „uczciwych" serwerów, pozostawiając użytkowników zdanych na serwery kontrolowane w puli przez agresora. Choć scenariusz taki wydaje się mało prawdopodobny, to technicznie jest możliwy do wykonania. W marcu 2023 zapowiedziano[16] aktualizacje systemu monitorowania NTP POOL włączając użycie wielu rozproszonych węzłów oceniających *score* poszczególnych serwerów NTP wchodzących w skład puli.

Podsumowując, otwarta architektura i skalowalność stanowią wielką zaletę Projektu NTP Pool, który pozostaje jednocześnie źródłem podatności. Brak stosowania kryptograficznego uwierzytelniania pakietów NTP, poleganie na infrastrukturze zewnętrznej DNS oraz opieranie się na zaufaniu do anonimowych dostawców sprzętowych serwerów NTP tworzy powierzchnię ataku, którą doświadczony technicznie przeciwnik z pewnością spróbuje wykorzystać. Duża popularność projektu NTP POOL przy jednoczesnej niskiej świadomości ryzyka jej używania sprzyja atakującemu. Zagrożone są w szczególności kraje o niewielkiej lokalnej liczbie serwerów mniejszej od 300szt. (rysunek 5).



Rys. 5 Zaokrąglony rozkład populacji publicznych serwerów czasu w projekcie NTP POOL.
Źródło: https://www.ntppool.org/zone/europe

KONSEKWENCJE FAŁSZOWANIA CZASU

Manipulacja czasem urządzeń sieciowych może mieć poważne konsekwencje dla poprawnego[17] działania całych sieciowych systemów informatycznych IT[18] i przemysłowych OT, ma więc bezpośredni wpływ na cyberbezpieczeństwo. Wzmacnianie powszechnej świadomości ryzyka oraz rozwiązań stanowią ważną misję społeczną[19]. Oto najważniejsze obszary zagrożeń związane z desynchronizacją i protokołem NTP:

- **Logowanie i audyt zdarzeń.** Nieprawidłowy czas podważa zaufanie do chronologii zdarzeń systemowych zapisanych w dzienniku LOG. Utrudnia to analizę incydentów bezpieczeństwa. W środowiskach rozproszonych desynchronizacja powoduje, że zdarzenia na różnych rozsynchronizowanych czasowo maszynach nie są poprawnie kojarzone na jednej wspólnej osi czasu, co zaburza logikę przyczynowo skutkową analizy

[15] https://www.usenix.org/system/files/sec23fall-prepub-520-kwon.pdf.
[16] https://www.ntppool.org/en/.
[17] https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/.
[18] https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/.
[19] https://blog.cloudflare.com/good-news-vulnerable-ntp-servers-closing-down/.

błędów oraz prowadzi do paradoksów, w których skutek wyprzedza własną przyczynę. Fałszywe znaczniki czasu mogą ukryć aktywność atakującego. Np. logi z przyszłą datą mogą nie być przeszukiwane przez narzędzia monitorujące. Możliwa jest również sytuacja przeciwna, w której nieprawidłowe **znaczniki czasu mogą wywoływać fałszywe alarmy lub przeciwnie powodować ich brak,** gdy data zdarzenia nieprawidłowo wskaże przeszłość.

- **Kryptografia i protokoły bezpieczeństwa.** Wiele protokołów kryptograficznych opiera się na zaufanym czasie[20] w celu oceny ważności certyfikatów, tokenów i podpisów cyfrowych. Np. certyfikaty X.509 używane w TLS/SSL mają określone daty ważności „od/do". Jeśli lokalny zegar zostanie cofnięty, system może uznać już wygasły certyfikat SSL za wciąż ważny, co umożliwia atak typu REPLAY lub wykorzystanie dawno unieważnionych poświadczeń[19]. Z kolei przesunięcie czasu do przodu może sprawić, że ważny certyfikat zostanie odrzucony jako jeszcze nieobowiązujący, co wywoła błędy w połączeniach szyfrowanych i może zmusić aplikacje do obniżenia standardów bezpieczeństwa. W szczególności protokół **Kerberos** jest bardzo czuły na desynchronizację czasu. Jego uwierzytelnienie ma krótki okres ważności. W większości przypadków granicę stanowi 5 minut. Zbyt duża różnica czasu między klientem a serwerem uwierzytelniającym uniemożliwia logowanie[21] w sieciach zarządzanych przez Active Directory. Podobnie jest z **DNSSEC**, którego mechanizmy bezpieczeństwa podlegają ograniczonej ważności czasowej podpisów. Gdy zegar systemowy przesunięty jest poza okres ważności podpisu, spowoduje to uznanie odpowiedzi DNS za nieważną. Fałszerstwo czasu może zatem skutkować masowym łamaniem mechanizmów uwierzytelniania i autoryzacji, nawet jeśli same algorytmy kryptograficzne pozostają nienaruszone i są bardzo silne.

- **Certyfikaty SSL/TLS i infrastruktura PKI.** Jak wspomnieliśmy, poprawny czas jest kluczowy do weryfikacji certyfikatów cyfrowych. Atakujący manipulując zegarem ofiary może niezauważenie doprowadzić do sytuacji, w której pewien skompromitowany lub odwołany już certyfikat pozostanie nadal ważny. Spowoduje to, że niebezpieczne połączenie HTTPS nie zaalarmuje o problemie, ponieważ z perspektywy systemu certyfikat pozostaje nadal ważny. Innym skutkiem desynchronizacji może być dezaktywacja aktualizacji systemu rewokacji CRL/OCSP, jeśli komputer myśli, że jest dużo wcześniej lub później niż bieżący czas i data. Może wtenczas nieprawidłowo sprawdzać listy unieważnionych certyfikatów zaufania, takich jak RPKI wykorzystywanych do zabezpieczania tras BGP. Niewłaściwa ocena ważności certyfikatów na skutek złego czasu podważa cały mechanizm ochrony sieci[22].

- **Aplikacje zależne od czasu.** Poza bezpieczeństwem systemowym, fałszywy czas zaburza działanie zwykłych aplikacji. Przykładowo systemy **buforowania oraz CDN** korzystają z czasowych znaczników ważności TTL. Jeśli czas nagle przeskoczy do przodu, bufor *cache* może uznać świeże dane za przeterminowane[19]. W systemach finansowych niezsynchronizowane zegary mogą spowodować błędne sekwencje porządku zleceń transakcji (np. transakcje finansowe z przyszłości mogą zostać odrzucone). Wreszcie, zadania zaplanowane (np. *Cron Scheduler*) mogą nie wykonać się lub wykonać o złej porze, jeśli systemowy czas ulegnie nagłej skokowej zmianie. Podobne problemy związane są z zarządzaniem współbieżnością na niskim poziomie organizacji procesów w jądrze *kernel* systemu operacyjnego[23].

- **Krypto-waluty, Smart Contracts, Blockchain,** oczekują względnie spójnego zgodnego czasu użytkowników. Jeżeli węzeł ma zegar różniący się o kilkanaście minut, inne węzły łańcucha mogą go odrzucić. Rozsynchronizowanie można również wykorzystać do oszustwa. Manipulując znacznikami czasu w granicach dozwolonego odchylenia można wpływać na wydobycie sekwencji bloków z łańcucha *blockchain*.

Podsumowując, spójność czasu ma fundamentalne znaczenie bezpieczeństwa systemów informatycznych, aplikacji, a obecnie również nowych wschodzących cyfrowych systemów monetarnych. Fałszowanie czasu przez złośliwe serwery NTP zagraża chronologii zdarzeń w LOG. Manipulując czasem można unieważniać certyfikaty i blokować dostęp do systemów lub usług (TLS, Kerberos, DNSSEC). Tym samym desynchronizacja może zaburzyć podstawowe procesy biznesowe wywołując straty finansowe.

[20] https://blog.cloudflare.com/secure-time/.
[21] https://blog.apnic.net/2022/12/09/securing-ntp-against-mitm-attacks/.
[22] https://www.cs.bu.edu/~goldbe/papers/NTPattacks.html
[23] https://www.itu.int/en/itunews/Documents/2023/2023-02/2023_ITUNews02-en.pdf.

W dużej skali (np. cały region korzystający z zmanipulowanej puli NTP) skutki mogą być katastrofalne – od zmasowanych błędów i odrzucaniu certyfikatów, przez brak dostępu do szyfrowanych kanałów informacyjnych, aż po luki w nadzorze całych systemów bezpieczeństwa i chaos prowadzący do kryzysu.

ZNANE BADANIA NAUKOWE I INCYDENTY

Zagrożenia związane z fałszowaniem czasu od kilku lat znajdują się w centrum uwagi społeczności akademickiej i naukowej branży IT. Poniżej wybrane przykłady:

- **Badanie Boston University (Malhotra et al. 2016),** to jedna z przełomowych prac analizujących bezpieczeństwo NTP, która pokazała jak groźne są ataki na niezabezpieczony protokół. Autorzy przedstawili między innymi atak **Kiss-of-Death spoofing (CVE-2015-7704)** pozwalający dowolnemu napastnikowi zablokować synchronizację czasu u klienta poprzez wykorzystanie mechanizmu KoD. Zademonstrowali oni atak na przesunięcie czasu **time-shifting** zarówno z pozycji on-path (MITM/BGP, patrz opis *Timeshifting by Reboot*) jak i off-path poprzez fragmentację pakietów. Wykazali również wpływ takich ataków na inne protokoły. Pokazali, że zmanipulowany czas może unieruchomić DNSSEC, osłabić bezpieczeństwo SSL/TLS oraz wprowadzić podatności w infrastrukturze klucza publicznego (np. RPKI). Badanie nagłośniło potrzebę zmian w protokole NTP i dało początek prac standaryzacyjnych NTS (Network Time Security).

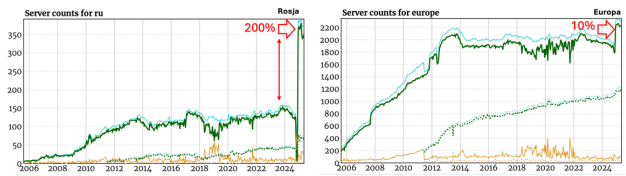
- **Projekt Chronos (IETF, 2017-2020).** To odpowiedź środowiska akademickiego, IETF[24], IRTF[25] mechanizm o nazwie **Chronos**. W podejściu Chronos klient NTP nie polega na garstce serwerów NTP, lecz odpytuje jednocześnie kilkadziesiąt serwerów NTP publicznej puli stosując bizantyjski algorytm filtrowania[26] odchyleń. Założenie Chronos opiera się na tezie, że nawet jeśli kilka serwerów NTP jest złośliwych lub skompromitowanych, to dopóki większość odpowiada poprawnie, klient sam wyliczy właściwy wzorcowy czas UTC i użyje go. Twórcy Chronos wykazali, że atak MITM musiałby mieć wpływ na globalną skalę UTC, aby skutecznie desynchronizować. Badacze udowodnili w procesie symulacji ataku, że aby wywołać przesunięcie czasu o 100 ms w Chronos, wymagałoby to od atakującego aż 20 lat ciągłego wysiłku, aby zmanipulować dużą liczbę źródeł UTC jednocześnie[25]. Chronos został przedstawiony do IETF jako tzw. Internet-draft. Stanowi ciekawy kierunek badań do poprawy bezpieczeństwa NTP po stronie klienta. Niemniej jednak, dalsze prace Jeitner/Shulman wskazują, że Chronos również ma pewny słaby punkt. Jest nim poleganie na DNS przy losowaniu listy serwerów NTP. Jeśli atakujący skompromituje DNS, to może on nawet tak zaawansowany mechanizm ochrony przekierować do własnych serwerów NTP (wracamy tu ponownie do problemu zatruwania[25]). To utwierdza w przekonaniu, że potrzebne są wielopoziomowe zabezpieczenia.

- **Badanie Hebrew University (Perry et al. 2021).** Praca *"A Devil of a Time: How Vulnerable is NTP to Malicious Timeservers?"*[27] skupiła się na ryzykach związanych bezpośrednio z projektem NTP POOL. Autorzy przeprowadzili pomiary i eksperymenty, które potwierdziły, że nawet przy istnieniu mechanizmów uwierzytelniania (takich jak NTS) klient NTP nadal może paść ofiarą złośliwego serwera czasu. Wykazano, że przejęcie kontroli nad kilkoma serwerami w puli lub zatruwając regionalnie NTP POOL (przypominamy, że zatruwanie to dołączenie nowych złośliwych serwerów kontrolowanych przez atakującego) pozwala na duże przesunięcia czasu wybiórczo u wielu klientów NTP. Jest to możliwe szczególnie z uwagi na nieświadomość zależności STRATUM w algorytmie przydziału serwerów NTP w POOL. Zasugerowano modyfikacje działania tak aby uwzględniała topologię sieci synchronizacji, w tym hierarchię STRATUM 0-15 przy wyborze serwerów NTP dla klienta, oraz włączenie podejścia Chronos w formie procesu nadzoru *watchdog*, który wykrywa podejrzane rozbieżności czasu serwerów NTP operujących w POOL.

- **Analiza ETH Zürich (Kwon et al. 2023).** Najnowsze badania objęły kompleksowy przegląd bezpieczeństwa ekosystemu NTP POOL, w szczególności skupiając się na wewnętrznym systemie monitorowania. Wykazano kilka scenariuszy, gdzie atakujący może manipulować monitorami POOL tak, aby wyeliminować konkurencyjne, prawidłowe serwery i zwiększyć udział własnych złośliwych. To jest de facto atak na infrastrukturę zarządzającą puli. Praca potwierdziła, że poprzednia architektura z pojedynczym węzłem monitorującym była podatna na wspomniany *adaptive delay attack* – manipulacje zegarem monitora przez atakującego. Zwrócenie uwagi na te problemy zaowocowało dyskusją w społeczności projektu NTP POOL, co skutkuje obecnie wdrażaniem środków zaradczych w formie wielu rozproszonych monitorów w puli.
- **Incydenty bezpieczeństwa związane z NTP.** Choć brak jest oficjalnych doniesień o celowych globalnych atakach fałszujących czas w NTP POOL (co prawdopodobnie wynika ze względu na trudność wykrycia wymagającą eksperckiej wiedzy), to pewne wydarzenia wskazują na powagę zagrożenia. Już w 2012 r. zanotowano

[24] https://www.ietf.org/blog/ntp-update/.
[25] https://www.ietf.org/live/previous/live105/ietf105-irtf-open/.
[26] https://arxiv.org/pdf/2010.09338.
[27] https://www.ndss-symposium.org/wp-content/uploads/ndss2021_1A-2_24302_paper.pdf.

pierwsze incydenty, w których błędna konfiguracja serwera NTP spowodowała rozesłanie nieprawidłowego wzorca czasu o dekady wstecz, wpływając na infrastrukturę IT w różnych organizacjach. Przypadek ten często nazywany jest „*NTP era bug*". W 2019 r. tzw. błąd *GPS Week Number Roll-Over* spowodował, że część serwerów Stratum-1 zaczęła dostarczać niepoprawną datę, co zaburzyło synchronizację niektórych sieci. Serwery te szybko wykluczono[28] z puli dzięki mechanizmom monitorującym. Z kolei jesienią 2024 r. miał miejsce w Rosji incydent z udziałem urządzeń IoT firmy Yandex. Nigdy nie został potwierdzony jako cyber atak i opisano go jako przeciążenie NTP POOL spowodowane błędem firmware urządzeń do streamingu wysokiej jakości dźwięku i obrazu (AVB). Niezależnie od natury incydentu pokazał on, że masowe odpytywanie NTP POOL przez wadliwy firmware sprzętu sieciowego IoT może skutkować destabilizacją usługi czasu w skali całego kraju[29]. Takie zdarzenie zawsze zwraca uwagę międzynarodowych ekspertów. Firma Yandex natychmiast wdrożyła poprawkę firmwaru, co podkreśla powagę z jaką Rosjanie traktują usługę NTP POOL, ważną dla gospodarki pracującej w trybie wojennym. Dodatkowo jako rekompensatę, Yandex wdrożył do POOL w grudniu 2024 blisko 300 nowych[30] serwerów NTP, co stanowi 200% wzrost w stosunku do czerwca 2024. Firma zrobiła to w ekstremalnie krótkim czasie kilku tygodni, tworząc bezprecedensowe posunięcie zapobiegające przyszłemu ryzyku celowego „zatrucia" rosyjskiej strefy NTP POOL. Tak duży wzrost liczby serwerów w Rosji widać w europejskiej puli (rysunek 6).



Rys. 6 Incydent „Yandex" widoczny w charakterystyce POOL Rosji (na lewo) i Europy (na prawo). Źródło:
https://www.ntppool.org/zone/ru
https://www.ntppool.org/zone/europe

Opisane incydenty ilustrują jak krytyczna jest niezawodność i prawidłowość działania NTPPOOL.

ZALECANE METODY OCHRONY

W odpowiedzi na opisane zagrożenia, eksperci zalecają wielopoziomowe podejście zabezpieczania funkcjonalności synchronizacji czasu. Poniżej przedstawiono kluczowe metody ochrony przed fałszowaniem czasu z użyciem protokołu NTP:

- **NTS (Network Time Security).** To zaproponowane przez IETF rozszerzenie protokołu NTP, które dodaje warstwę kryptograficzną opartą o TLS/DTLS wspieraną mechanizmem cookie. Służy do uwierzytelniania serwera NTP i zapewnienia integralność danych zawierających znaczniki czasu *round-trip*[2]. Pozwala klientowi upewnić się, że odpowiedź z serwera NTP faktycznie pochodzi z oczekiwanego urządzenia i nie została zmieniona podczas transportu. W praktyce działa to tak, że klient NTP najpierw nawiązuje sesję TLS z serwerem czasu (faza negocjacji NTS-KE) i wymienia klucze kryptograficzne oraz otrzymuje unikatowy token (cookie). Podczas synchronizacji, późniejsze standardowe zapytania NTP zawierają kryptograficzne uwierzytelnienie (AEAD) oparte na przekazanym tokenie. Nawet jeśli atakujący przechwyci pakiety, nie będzie w stanie ich zmodyfikować, bo nie zna klucza symetrycznego używanego w transmisji. W 2020 r. opublikowano RFC 8915 dla NTS i obecnie istnieją implementacje serwerów NTP i klientów wspierających ten protokół zarządzania kluczami. Usługi synchronizacji w chmurze np. *time.cloudflare.com* już udostępniają obsługę NTS. Zdecydowanie zaleca się korzystanie z NTS wszędzie tam, gdzie to możliwe, ponieważ eliminuje to klasę wyżej opisanych ataków MITM/spoofing. Stosując NTS napastnik nie może podszyć się pod serwer posiadający ważny certyfikat ani zmodyfikować zaszyfrowanych pakietów NTP. Chroni również przed złośliwymi serwerami, ale wyłącznie spoza POOL. Obecnie trwają prace przygotowujące polski system eCzasPL Głównego Urzędu Miar RP do wdrożenia NTS. Wdrożenie NTS wymaga aktualizacji zarówno po stronie serwera czasu, jak i klienta NTP. Jest obecnie najskuteczniejszym sposobem zabezpieczenia.

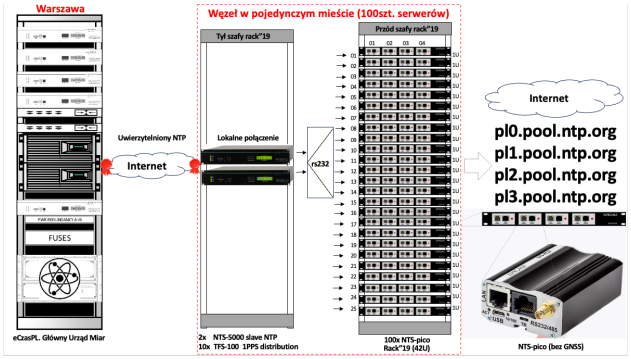
- **Bezpieczna konfiguracja klienta NTP.** Niezależnie od używania NTS, warto tak skonfigurować NTP (plik *ntp.conf* dla demonów ntpd i chronyd), aby zminimalizować skutki ewentualnego zewnętrznego ataku na czas. Dobrą praktyką są:
  - **Wykorzystanie wielu serwerów czasu NTP jednocześnie.** Zamiast polegać na pojedynczym serwerze NTP POOL, zaleca się użycie co najmniej 3–5 serwerów NTP z różnych domen i regionów routingu TCP/IP. Standardowy algorytm NTP wyposażony jest w funkcję Intersection[31] i algorytm DTS[32], który potrafi

[28] https://community.ntppool.org/t/gps-rollover-may-malfunction-on-or-after-april-6/1172.
[29] https://en.wikipedia.org/wiki/NTP_server_misuse_and_abuse.
[30] https://www.ntppool.org/zone/ru.
[31] https://en.wikipedia.org/wiki/Intersection_algorithm.
[32] https://en.wikipedia.org/wiki/Marzullo%27s_algorithm.

zidentyfikować i odrzucić źródła FALSETICKERS z odchyleniami czasu, jeśli większość pozostałych źródeł UTC podaje zgodny czas. Większa ilość i różnorodność używanych serwerów NTP utrudnia pojedynczemu atakującemu przejęcie kontroli w celu ataku desynchronizacji. Mechanizm *Chronos* idzie jeszcze dalej, proponując używanie kilkudziesięciu serwerów NTP jednocześnie. Choć takie ilości mogą z pozoru wydawać się przesadą, to kluczowe jest unikanie sytuacji, w której to pojedynczy serwer dyktuje czas. Gdy taki serwer wskazuje błędny czas to niestety jesteśmy na niego skazani.

– **NTP Panic Threshold i ograniczenie wielkości skoku czasu**. Upewnij się, że Twój klient NTP nie dokonuje nagłych dużych korekt czasu bez nadzoru. W protokole NTP istnieje parametr *panic threshold* ustawiony domyślnie na 1000 s, powyżej którego demon *ntpd* przerwie pracę. Zaleca się utrzymanie tej polityki, a jednorazową inicjującą synchronizację należy wykonywać manualnie lub przy starcie systemu. W *Chrony* domyślnie duże odchylenia czasu są korygowane stopniowo techniką *slew* zamiast jednorazowego skoku. Takie mechanizmy utrudniają atakującemu szybkie przesunięcie zegara o dużą wartość i w niezauważony sposób. Administrator powinien monitorować NTP w logach, ponieważ częste resetowanie demona *ntpd i chrony* lub otrzymywanie pakietów Kiss-of-Death (KoD) powinno wzbudzić podejrzenia ataku.

– **Filtrowanie i restrykcje sieciowe.** Ogranicz komunikację NTP tylko do znanych ci serwerów czasu, np. firewallem. Należy korzystać z NTP z uwierzytelnieniem symetrycznym. Warto blokować na routerach ruch NTP spoza oczekiwanych adresów IP oraz utrzymywać własne serwery NTP Stratum-1. **DNSSEC i kontrola DNS.** Jeśli korzystasz z domen klasy *pool.ntp.org*, rozważ włączenie „walidacji" DNSSEC na tzw. resolverze lokalnym. Chociaż większość stref puli NTP nie jest jeszcze podpisana DNSSEC, to coraz więcej dostawców takich jak *time.cloudflare.com* oferuje już podpisane rekordy. Dobrą praktyką jest używanie ustawionych „na sztywno" adresów IP serwerów czasu NIST, w Polsce GUM RP[33] (rysunek 7).



Rys. 7 Proponowana struktura „odtruwania" krajowej strefy NTP POOL. Rozproszona architektura 8 miast węzłowych dołączonych do systemu eCzasPL[33] Źródło: Elproma (www.elpromaelectronics.com)

- **Aktualizacja NTP.** Zaleca się aktualizowanie demonów NTP do najnowszych wersji, które adresują znane podatności jak np. CVE z 2015 roku. powinni śledzić komunikaty i zapoznać się z dokumentem *Best Current Practices* (RFC 8633)[34].
- **Redundancja i monitoring czasu.** W krytycznych zastosowaniach warto implementować niezależne metody weryfikacji czasu. Przykładowo, system może okresowo sprawdzać czas poprzez **protokół roughtime** (propozycja Google – usługa podająca czas z podpisem Ed25519) lub porównywać lokalny czas z sygnaturami HTTPS. Dobrą praktyką jest też monitorowanie spójności czasu i szybkie wykrycie anomalii.

Na koniec, należy podkreślić, że zabezpieczenie usługi synchronizacji czasu staje się coraz ważniejsze w ogólnej strategii narodowego bezpieczeństwa. Organizacje powinny traktować serwery NTP/PTP analogicznie do innych elementów krytycznej infrastruktury i uwzględniać to w modelach zagrożeń i testach. Należy testować odporność na desynchronizację i wdrażać nowe mechanizmy ochronne.

Autorzy dziękują panu **Krzysztofowi Sileckiemu** z NASK oraz panom **Maciejowi Gruszczyńskiemu i Albinowi Czubli** z Głównego Urzędu Miar RP.

LITERATURA

[1] B. Szafrański, praca zbiorowa „*Cyberbezpieczeństwo redefinicja zagrożeń",* Rozdział XII, W. Paluszyński „*Niedocenione zagrożenie – źródło i dystrybucja czasu*", str.177-214, Wojskowa Akademia Techniczna (2023).

[2] B. Szafrański, praca zbiorowa „*Cyberbezpieczeństwo vs. Sztuczna Inteligencja"* Rozdział XV, T. Widomski „Desynchronizacja IT/OT infrastruktury krytycznej – - jak monitorować" str. 253-290, WAT (2024).

[3] B. Szafrański, praca zbiorowa „*Cyberbezpieczeństwo vs. Współpraca informacyjna"*, T. Widomski „Atak na czas, opóźnienie i synchronizację IT/OT – Skuteczna cyber-broń przyszłości", WAT (2025).

[33] https://www.gum.gov.pl/pl/projekty-eu/e-czaspl

[34] https://datatracker.ietf.org/doc/rfc8633