Warszawa, 4 września 2026 r.

Kamil Wójcik
I Wiceprezes FSNT-NOT
Federacja Stowarzyszeń Naukowo-Technicznych NOT
Naczelna Organizacja Techniczna

Pan Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Ministerstwo Cyfryzacji

LIST OTWARTY

Dotyczy: zwiększenia identyfikowalności klientów usług serwerowych i chmurowych oraz przejrzystości reagowania na nadużycia

Szanowny Panie Ministrze,

W ostatnich dniach infrastruktura Naczelnej Organizacji Technicznej została dotknięta poważnym incydentem cyberbezpieczeństwa. Kilka dni pracy nad jego analizą, ograniczaniem skutków i odtwarzaniem danych skłoniło mnie do zwrócenia uwagi na problem, który wykracza daleko poza jedno zdarzenie. **Najważniejszy wniosek jest prosty: cyberprzestępca nie musi dziś budować własnego zaplecza technicznego. Potrzebną mu moc obliczeniową, publiczne adresy IP i szybkie łącza może kupić na zwykłym, legalnym rynku usług cyfrowych.**

Opisałem ten problem w mediach społecznościowych. W ciągu dwóch dni publikację otworzyło ponad 700 tys. osób, liczba interakcji z treścią przekroczyła 70 tys., a ponad 7 tys. osób zareagowało na nią w różnej formie; niemal 98 proc. z nich wybrało reakcję „Lubię to”. Obiecałem odbiorcom, że zwrócę się w tej sprawie do Ministra Cyfryzacji. Dlatego kieruję do Pana Ministra niniejsze pismo. Statystyki publikacji pozostają do wglądu.

Ze względów bezpieczeństwa ograniczam zakres ujawnianych informacji o samym incydencie. Nie podaję nazw ani rodzaju zaatakowanych systemów, szczegółowej chronologii, metod działania sprawców ani informacji pozwalających odtworzyć architekturę środowiska. Pełny materiał techniczny, w tym dzienniki zdarzeń i zabezpieczone dowody, jest dostępny Panu Ministrowi i właściwym organom państwa do wglądu w odpowiednim, niepublicznym trybie.

Uważam jednak, że można i należy ujawnić jeden element, ponieważ dobrze pokazuje istotę problemu. W materiale dotyczącym zdarzenia występują między innymi adresy 89.116.171.113 i 89.117.94.35, należące do zakresów używanych przez Ethernet Servers i ogłaszanych przez AS46475 Limestone Networks; adres 37.19.196.20 z sieci DataCamp Limited, znanej handlowo również jako DataPacket; oraz adres 79.99.78.148 przypisany w publicznych rejestrach do ByteVirt LLC.[1][2][3]

Nie wyciągam z tych adresów wniosku o narodowości ani miejscu pobytu sprawców. Adres serwera nie jest adresem człowieka. Wniosek jest inny i, moim zdaniem, ważniejszy: **do**

prowadzenia działań przeciwko polskiej organizacji wykorzystano infrastrukturę dostępną na zwykłym, ogólnodostępnym rynku w państwach demokratycznych. Nie jest do tego potrzebny serwer zlokalizowany w Rosji czy Korei Północnej. Wystarczy usługa zakupiona u dostawcy działającego w naszej części świata.

To prowadzi do pytania o sposób, w jaki sprzedajemy dziś dostęp do infrastruktury cyfrowej. Dokumentacja dużych dostawców pokazuje, że elementami weryfikacji klienta są najczęściej dane kontaktowe, numer telefonu i ważna metoda płatności. AWS wymaga ważnej metody płatności i wykorzystuje numer telefonu do potwierdzania konta; Vultr i DigitalOcean wprost wskazują, że metoda płatności służy im również do weryfikacji użytkownika i ochrony przed oszustwami oraz automatycznymi nadużyciami. OVHcloud informuje natomiast, że dokument potwierdzający tożsamość lub adres nie jest pobierany systematycznie i może być wymagany między innymi przy wątpliwościach co do tożsamości albo ryzyku oszustwa.[4]

Nie kwestionuję potrzeby wygodnego i szybkiego uruchamiania usług. To jedna z podstaw rozwoju współczesnej gospodarki cyfrowej. Problem polega na tym, że **potwierdzenie, że karta płatnicza działa lub że ktoś odbiera wiadomości pod wskazanym numerem telefonu, nie jest równoznaczne z ustaleniem, komu rzeczywiście udostępniono infrastrukturę.** Jeżeli klient poda nieprawdziwe dane, a jedynym rzeczywiście skutecznym warunkiem uruchomienia zasobów pozostaje płatność, koszt anonimowości jest bardzo niski.

Nie mam złudzeń, że silniejsza weryfikacja tożsamości zatrzyma najbardziej zaawansowane grupy przestępcze. Bezpieczeństwo rzadko polega jednak na stworzeniu bariery absolutnej. Polega na zwiększaniu kosztu i ryzyka działania. Dla mniej zaawansowanych sprawców sama świadomość, że usługodawca zna ich rzeczywistą tożsamość, może działać odstraszająco. Dla grup wyspecjalizowanych oznacza konieczność pozyskania cudzej lub fałszywej tożsamości, odpowiednich środków płatniczych i tworzenia kolejnych warstw pośrednich. **Wyższy koszt, dłuższy czas i większe ryzyko po stronie sprawcy pogarszają opłacalność ataku.**

Problem staje się pilniejszy także ze względu na skalę zagrożeń. Ministerstwo Cyfryzacji podało, że w 2025 r. krajowe zespoły reagowania na incydenty otrzymały 682 245 zgłoszeń i obsłużyły 272 941 incydentów; liczba obsłużonych incydentów wzrosła o 144,4 proc. w porównaniu z rokiem wcześniejszym.[5] Brytyjskie Narodowe Centrum Cyberbezpieczeństwa (NCSC) ocenia jednocześnie, że rozwój sztucznej inteligencji niemal na pewno zwiększy skuteczność działań włamywaczy, częstotliwość i intensywność cyberzagrożeń, a do 2027 r. narzędzia wykorzystujące sztuczną inteligencję będą ułatwiały wykorzystywanie znanych podatności oraz skalowanie działań.[6]

Europol w ocenie zagrożeń cyberprzestępczością z 2026 r. wskazuje na tę samą tendencję: rozwój sztucznej inteligencji, automatyzacji i usług pośredniczących zwiększa zasięg oraz skuteczność cyberprzestępczości.[7] Jeżeli po jednej stronie pojawi się sprawca wspierany przez sztuczną inteligencję i dziesiątki lub setki krótko działających serwerów, a po drugiej stronie właściciel małej firmy ręcznie ustalający, do kogo należy każdy adres IP i na jaki adres kontaktowy wysłać zgłoszenie, obecny sposób reagowania stanie się niewydolny.

W tym miejscu pojawia się drugi problem: sposób reagowania dostawców na zgłoszenia nadużyć. Dostępne badania nie pozwalają uczciwie powiedzieć, że określony odsetek takich zgłoszeń „trafia do kosza", ale pokazują bardzo duże różnice w sposobie i szybkości reakcji. W badaniu obejmującym 480 zgłoszeń skierowanych do podmiotów odpowiedzialnych za obsługę nadużyć odpowiedzi nadeszły z 89 adresów; 78 było automatycznych, a 11 niewątpliwie pochodziło od

ludzi.[8] Spamhaus, badając kampanię Qbot, odnotował czasy reakcji od około pół godziny u najszybciej reagujących operatorów do ponad 20 dni u najwolniejszych.[9]

Publiczny projekt URLhaus nadal porównuje czasy reakcji sieci na zgłoszenia dotyczące złośliwych zasobów, a Netcraft podaje, że w jego własnym systemie mediana czasu usuwania stron wyłudzających dane wynosi 33 minuty, przy czym większość skutecznych działań podejmowana jest dzięki bezpośrednim kontaktom technicznym z dostawcami, a nie przez standardowe kolejki zgłoszeń.[10] Nie uznaję danych jednej firmy za reprezentatywne dla całego rynku. Pokazują one jednak, że szybka reakcja jest organizacyjnie możliwa, jeśli istnieją odpowiednie procedury, automatyzacja i odpowiedzialność po stronie dostawcy.

Właśnie dlatego proponuję spotkanie poświęcone dwóm kwestiom. **Pierwsza to weryfikacja tożsamości klienta zależna od poziomu ryzyka.** Nie chodzi o kopiowanie dokumentu tożsamości przy każdej, nawet najtańszej usłudze. Chodzi o ustalenie wspólnego minimum, a następnie o silniejszą weryfikację tam, gdzie rośnie ryzyko szkody albo pojawiają się sygnały ostrzegawcze: szybkie uruchamianie wielu serwerów lub pozyskiwanie wielu publicznych adresów IP, wcześniejsze potwierdzone nadużycia, ponowne tworzenie kont po ich zamknięciu czy istotne niespójności w danych klienta. Dostawca powinien też mieć techniczną możliwość ustalenia, któremu zweryfikowanemu klientowi w danym czasie udostępniał konkretny publiczny adres IP.

Nie jest to pomysł bez precedensu. Brytyjskie wytyczne dla dostawców infrastruktury internetowej, przygotowane w związku ze zwalczaniem innych poważnych przestępstw w sieci, wprost zalecają stosowanie zasady „poznaj swojego klienta” przez dostawców usług chmurowych, tak aby bezprawne działania mogły zostać powiązane z identyfikowalnym użytkownikiem. Te same wytyczne wskazują na potrzebę przyjmowania zgłoszeń o nadużyciach, określania czasu reakcji i publikowania danych o podjętych działaniach.[11]

Druga kwestia to **obowiązek publikowania przez większych dostawców porównywalnych danych o tym, jak rzeczywiście reagują na zgłoszenia nadużyć.** Taki raport powinien zawierać między innymi liczbę zgłoszeń, liczbę spraw potwierdzonych i odrzuconych, medianę czasu pierwszej reakcji, medianę czasu potrzebnego do ograniczenia potwierdzonego zagrożenia, czas, w którym obsługiwanych jest 90 proc. spraw, liczbę zawieszonych usług oraz skalę ponownych nadużyć przez klientów, wobec których wcześniej podejmowano działania. Dane nie muszą ujawniać tożsamości klientów ani szczegółów prowadzonych postępowań. Mają pozwolić porównać, czy dostawca reaguje w godzinę, dobę czy kilkanaście dni.

Także tutaj europejskie prawo daje użyteczny punkt odniesienia. Akt o usługach cyfrowych (DSA) już nakłada na część dostawców usług pośrednich obowiązek okresowych sprawozdań, a w przypadku usług hostingu przewiduje między innymi podawanie liczby zgłoszeń i mediany czasu potrzebnego na podjęcie działania. Od lipca 2025 r. obowiązują ujednolicone zasady raportowania, dzięki którym dane mają być porównywalne. Przedmiot tych raportów jest inny niż przedmiot zgłoszeń dotyczących infrastruktury użytej do cyberataku, ale mechanizm regulacyjny jest gotowy: wspólne definicje, wspólny format i mierzalny czas reakcji.[12]

Taka przejrzystość, oprócz kryteriów ekonomicznych, dodałaby kolejne kryterium wyboru dostawcy. Dziś klient wybierający dostawcę zna cenę, parametry techniczne i deklarowaną dostępność usługi. Zwykle nie ma możliwości ocenić, czy ten sam dostawca potrafi skutecznie reagować, gdy jego infrastruktura jest wykorzystywana przeciwko innym. **Jeżeli czas i skuteczność reagowania stałyby się publicznie porównywalne, sprawne reagowanie na nadużycia zyskałoby wartość rynkową, a nieskuteczne – realny koszt reputacyjny.**

W ostatnich dniach Pan Minister publicznie zwracał uwagę na podobny konflikt bodźców w sporze z firmą Meta dotyczącym oszukańczych reklam. Według Reutersa wskazał Pan, że platforma przedkłada zysk nad bezpieczeństwo użytkowników; w tej samej sprawie CERT Polska miał wskazać 122 oszukańcze reklamy, z których usunięto 10.[13] Nie stawiam znaku równości między platformą reklamową a dostawcą serwerów. Widzę jednak ten sam problem ekonomiczny: dostawca uzyskuje przychód natychmiast, natomiast koszt nadużycia ponosi ktoś inny.

W przypadku cyberataku ta asymetria jest szczególnie dotkliwa. Napastnik może stracić tani serwer i po kilku minutach kupić następny. Ofiara płaci za analizę zdarzenia, przestój, odtwarzanie danych, pracę specjalistów, zabezpieczenie dowodów i przywracanie zaufania do systemów. **W praktyce zysk ze sprzedaży infrastruktury pozostaje prywatny, a znaczna część kosztu jej przestępczego wykorzystania zostaje przerzucona na ofiarę.**

NOT ma kompetencje techniczne, personel i kopie zapasowe, a mimo to usuwanie skutków poważnego incydentu wymagało ogromnego nakładu pracy. Znacznie trudniejsza będzie sytuacja kilkuosobowej firmy, szkoły, małego biura projektowego czy lokalnego przedsiębiorcy bez własnych specjalistów od cyberbezpieczeństwa. Wraz ze wzrostem automatyzacji to właśnie takie podmioty będą coraz częściej ponosiły koszt działalności, której skalę sprawca może zwiększać niemal bez ograniczeń.

Przyjęta w marcu tego roku Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej zakłada między innymi zwiększenie odporności kraju i skuteczniejsze zwalczanie cyberprzestępczości.[14] Uważam, że rozmowa o identyfikowalności użytkowników infrastruktury i o mierzalnych standardach reagowania dostawców na nadużycia naturalnie wpisuje się w ten kierunek.

Dlatego proponuję Panu Ministrowi spotkanie w siedzibie Naczelnej Organizacji Technicznej poświęcone temu problemowi. Uważam też, że dobrze, aby uczestniczyli w nim przedstawiciele Ministerstwa Cyfryzacji, NASK, CERT Polska i branży usług serwerowych i chmurowych, eksperci ds. cyberbezpieczeństwa oraz przedstawiciele małych i średnich przedsiębiorstw. Celem nie jest wskazanie jednego winnego, lecz wypracowanie zasad systemowych, które podniosą koszt nadużycia, poprawią identyfikowalność sprawców i sprawią, że jakość reakcji dostawców stanie się widoczna i porównywalna dla rynku.

Państwo coraz więcej wymaga w zakresie cyberbezpieczeństwa od podmiotów, które mogą zostać zaatakowane. Powinno zatem, korzystając ze swoich możliwości i kompetencji, podjąć działania oraz przyjąć adekwatne rozwiązania formalnoprawne, aby dostawcy usług cyfrowych z większą starannością weryfikowali osoby i podmioty korzystające z ich infrastruktury.

Uważam, że nadszedł czas, aby równie poważnie przyjrzeć się odpowiedzialności tych, którzy odpłatnie udostępniają infrastrukturę wykorzystywaną później do prowadzenia ataków.

Z wyrazami szacunku,

Kamil Wójcik
I Wiceprezes FSNT-NOT

Signed by / Podpisano przez:
Kamil Paweł Wójcik
Date / Data: 2026-09-04 13:22

Źródła i materiały publiczne

[1] Publiczne dane RIPE/BGP dla 89.116.171.0/24 i 89.117.94.0/24: Ethernet Servers Ltd; trasy ogłaszane przez AS46475 Limestone Networks, Inc. https://www.browserscan.net/ru/ip-range/AS46475/89.116.171.0/24 https://www.browserscan.net/es/ip-range/AS46475/89.117.94.0/24

[2] Publiczne dane sieciowe dla 37.19.196.0/23: AS212238 DataCamp Limited; nazwy odwrotne w domenie datapacket.com. https://ipinfo.io/ips/37.19.196.0/24

[3] Publiczne dane RIPE dla 79.99.78.0/24: ByteVirt LLC. https://www.browserscan.net/ip-range/AS212336/79.99.78.0/24

[4] Praktyki weryfikacji kont u dostawców: AWS, Vultr, DigitalOcean i OVHcloud. https://docs.aws.amazon.com/accounts/latest/reference/getting-started.html https://docs.vultr.com/support/platform/billing/why-do-i-need-to-enter-a-payment-method https://docs.digitalocean.com/support/why-do-i-need-to-enter-a-payment-method/

https://www.ovhcloud.com/pl/terms-and-conditions/privacy-policy/

[5] Ministerstwo Cyfryzacji, „Krajobraz cyberprzestrzeni: sprawozdanie o stanie cyberbezpieczeństwa Polski za rok 2025", 16.04.2026. https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-sprawozdanie-o-stanie-cyberbezpieczenstwa-polski-za-rok-2025

[6] UK National Cyber Security Centre, „Impact of AI on cyber threat from now to 2027". https://www.ncsc.gov.uk/report/impact-ai-cyber-threat-now-2027

[7] Europol, „IOCTA 2026 - The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime", 28.04.2026. https://www.europol.europa.eu/publication-events/main-reports/iocta-2026-evolving-threat-landscape

[8] O. Çetin i in., „Understanding the role of sender reputation in abuse reporting and cleanup", Journal of Cybersecurity 2(1), 2016. https://academic.oup.com/cybersecurity/article/2/1/83/2629556

[9] Spamhaus, „Tracking Qbot" - porównanie czasu reakcji dostawców na zgłoszenia złośliwej zawartości. https://www.spamhaus.org/resource-hub/malware/tracking-qbot/

[10] URLhaus - publiczne zestawienia czasu reakcji; Netcraft - dane własne o czasie usuwania stron wyłudzających dane i bezpośrednich kanałach współpracy z dostawcami. https://urlhaus.abuse.ch/statistics/reactiontime/ https://www.netcraft.com/platform/threat-detection-and-takedown

[11] Rząd Wielkiej Brytanii, dobrowolne wytyczne dla dostawców infrastruktury internetowej dotyczące m.in. identyfikacji klienta, obsługi zgłoszeń i publikowania danych o działaniach. https://www.gov.uk/government/publications/voluntary-guidance-for-internet-infrastructure-providers/voluntary-guidance-for-internet-infrastructure-providers-on-tackling-online-child-sexual-exploitation-and-abuse-accessible-version

[12] Rozporządzenie (UE) 2022/2065 - akt o usługach cyfrowych (DSA), art. 15; Komisja Europejska - ujednolicone zasady sprawozdawczości obowiązujące od 1.07.2025. https://eur-lex.europa.eu/legal-content/EN-PL/TXT/?uri=CELEX%3A32022R2065 https://digital-strategy.ec.europa.eu/en/news/harmonised-transparency-reporting-rules-under-digital-services-act-now-effect

[13] Reuters, „Poland urges EU to fine Meta €250 million for scams and false ads", 27.08.2026. https://www.reuters.com/world/europe/poland-asks-eu-fine-meta-250-million-urges-action-against-scams-false-ads-2026-08-27/

[14] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej - uchwała nr 92 Rady Ministrów z 10.03.2026 r. https://eli.gov.pl/eli/MP/2026/309/ogl/pol https://www.gov.pl/web/cyfryzacja/nowa-strategia-cyberbezpieczenstwa-polska-wzmacnia-ochrone-przed-cyberatakami

Źródła internetowe zweryfikowano 31 sierpnia 2026 r. Szczegółowy materiał techniczny dotyczący incydentu NOT nie został załączony do pisma i pozostaje dostępny do wglądu w trybie niepublicznym.