



Wiceprezes Rady Ministrów Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.118.2026
Warszawa, 23 października 2026

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

nr 2026/67a/5

**dotycząca ochrony dostawców usług internetowych przed atakami typu DDoS¹ -
aktualizacja**

Niniejsza rekomendacja została wydana na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa² jako aktualizacja rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa nr 2026/67a/5 z dnia 29.06.2026 r. dotycząca ochrony ISP przed atakami typu DDoS³. Jej celem jest podniesienie poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa (KSC), w związku z zagrożeniem atakami na dostępność usług udostępnianych w sieci Internet.

Wprowadzenie

Atak typu DDoS to jedna z najczęściej spotykanych form cyberataków, której celem jest uniemożliwienie działania usług dostępnych w Internecie. W przypadku dostawców usług internetowych (ISP) ataki te polegają przede wszystkim na przeciążeniu infrastruktury sieciowej ogromną ilością ruchu pochodzącego z wielu rozproszonych źródeł. Działanie to jest skuteczne, ponieważ żaden system nie dysponuje nieograniczoną przepustowością łącza ani nieograniczonymi możliwościami przetwarzania pakietów. Każda sieć operatorska opiera się na określonej przepustowości łącza internetowego oraz wydajności urządzeń sieciowych. Gdy natężenie ruchu przekroczy te możliwości, dochodzi do wysycenia łącza lub wyczerpania zasobów urządzeń, co sprawia, że sieć przestaje prawidłowo obsługiwać ruch użytkowników. Najbardziej dotkliwe dla operatorów ISP rodzaje ataków DDoS to:

1. Ataki Wolumetryczne (Volumetric attacks) - ich celem jest zajęcie całej przepustowości łącza (np. UDP Flood).
2. Ataki na protokoły (Protocol attacks) - skupiają się na przeciążeniu zasobów urządzeń sieciowych (np. SYN ACK flood).

Rekomendacja

1. Analiza ryzyka i zarządzanie nim

- a) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;

¹ DDoS (Distributed Denial of Service) – rozproszony atak polegający na skoordynowanym generowaniu dużego ruchu sieciowego z wielu źródeł w celu wyczerpania zasobów systemu informatycznego i uniemożliwienia jego prawidłowego funkcjonowania.

² Dz. U. z 2026 r. poz. 20, z późn. zm. (dalej jako: ustawa o KSC).

³ <https://www.gov.pl/web/baza-wiedzy/rekomendacja-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-dotyczaca-ochrony-isp-przed-atakami-typu-ddos>

- b) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze;
 - podmiot prowadzący działalność gospodarczą, jakim jest ISP, powinien uwzględniać także inwestycje w cyberbezpieczeństwo, aby być w stanie ograniczać skutki materializujących się ryzyk wpływających na cyberbezpieczeństwo i ciągłość działania, a zatem na główne procesy jego działalności gospodarczej.
2. **Plany ciągłości działania i testy odporności infrastruktury:** przygotowanie planów ciągłości działania, obejmujących procedury postępowania na wypadek ataku DDoS. Procedury powinny być regularnie testowane i aktualizowane. Ponadto zaleca się regularne przeprowadzanie testów odporności infrastruktury w celu weryfikacji skuteczności wdrożonych mechanizmów ochronnych i mitygujących.
- a) Plan awaryjny powinien być przygotowany i przećwiczony. Plan powinien obejmować komunikację z klientami, z zespołami reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) i służbami oraz z dostawcami tranzytu. Kanały komunikacji muszą działać niezależnie od własnej sieci, np. SMS albo strona statusowa hostowana poza własnym AS⁴. Listę kontaktów warto trzymać także offline. Plan, który nie był testowany, w praktyce może nie zadziałać.
 - b) Łącze awaryjne z niezależną adresacją - łącze od innego dostawcy, z adresacją PA⁵ spoza atakowanych prefiksów i z przepustowością wystarczającą dla odbiorców krytycznych (urzędy, placówki medyczne, służby), których ruch w razie potrzeby przełącza się przez NAT. Procedurę przełączenia należy przygotować tak, żeby dało się ją wykonać w ciągu minut, a nie godzin.
 - c) Telefonia niezależna od Internetu. Lokalni ISP często dostarczają podmiotom publicznym również usługi VoIP. Wydzielone połączenie L2/L3 do operatora VoIP, które nie przechodzi przez publiczny Internet sprawia, że telefony działają nawet podczas dużego ataku wolumetrycznego.
 - d) Odpowiednia przepustowość do punktów wymiany ruchu i CDN⁶. Większość ruchu klientów pochodzi z sieci CDN. Dobre połączenie z punktami wymiany ruchu i bezpośredni peering pozwalają utrzymać kluczowe usługi także wtedy, gdy łącza tranzytowe są w pełni wysyczone. Punkt wymiany ruchu daje też dodatkową ścieżkę i często możliwość blackholingu.
 - e) IPv6 dla klientów. Obecnie ataki DDoS prowadzone są niemal wyłącznie po IPv4. Klienci z dual stackiem⁷ zachowują dostęp do części zasobów, w tym DNS i dużych serwisów, nawet jeśli ruch IPv4 trzeba będzie ograniczyć lub

⁴ AS (Autonomous System / System Autonomiczny) -spójna sieć IP zarządzana przez jedną organizację, posiadająca własną, unikalną tożsamość w globalnym routingu BGP.

⁵ Adresacja PA- Pula adresów IP przydzielona operatorowi przez wyższego dostawcę tranzytowego (upstream), będąca częścią jego większego bloku adresowego.

⁶ CDN (Content Delivery Network - Rozproszona sieć serwerów służąca do szybkiego dostarczania treści do użytkowników.

⁷ Dual Stack - Równoległe uruchomienie i obsługa stosu protokołów IPv4 oraz IPv6.

wyłączyć. IPv6 wymaga przy tym takiej samej staranności jak IPv4 (filtracja źródeł, RA Guard⁸), inaczej stanie się dodatkowym wektorem ataku.

3. **Konfiguracja telemetrii:** wdrożenie próbkowania ruchu obejmującego warstwę L2-L4 modelu ISO/OSI na routerach brzegowych oraz na przełącznikach. Zbierane dane telemetryczne powinny pozwolić na detekcję ataków DoS/DDoS ze szczególnym uwzględnieniem adresacji źródłowej i docelowej, natężenia ruchu wyrażonego w pps (pakietach na sekundę), fps (flowach na sekundę), bps (bitach na sekundę), a także flag w pakietach TCP oraz - o ile to możliwe - również adresów MAC.
4. **Mitygacja ataków i filtrowanie ruchu:** wdrożenie mechanizmów pozwalających na ograniczanie (rate-limiting) lub całkowite odrzucanie (discard) ruchu o charakterystyce zgodnej z obserwowanym atakiem. Ze względu na zróżnicowanie możliwości technologicznych operatorów, dobór konkretnych rozwiązań oraz skala automatyzacji powinny być dostosowane do specyfiki danej sieci. Rozwiązanie to może polegać np. na automatycznej mitygacji z wykorzystaniem BGP Flowspec⁹. W przypadku braku możliwości jej zastosowania, rekomenduje się implementację bezstanowych filtrów firewall oraz konfigurację sprzętowych ograniczników pasma (policerów) na interfejsach WAN.
5. **Weryfikacja adresów źródłowych (BCP 38¹⁰):** wdrożenie uRPF¹¹ na wszystkich interfejsach warstwy L3. W przypadku ograniczeń sprzętowych należy stosować statyczne, bezwarunkowe listy ACL dopuszczające ruch wyłącznie z adresów IP przypisanych do danego portu/VLAN-u subskrybenta (realizacja wymogów BCP 38 / RFC 2827) na portach dostępowych.
6. **Filtracja adresów Bogon¹²:** Na portach dostępowych należy wdrożyć prefix-listy odrzucające pakiety z źródłowymi lub docelowymi adresami Bogon (przestrzenie prywatne RFC 1918, adresy lokalne, multicast oraz nieprzydzielone przez IANA).
7. **Ochrona usług DNS i zapobieganie atakom DRDoS:** zwiększenie odporności własnych usług DNS na ataki wolumetryczne poprzez wdrożenie architektury anycast. Ponadto, aby zapobiec wykorzystywaniu własnej infrastruktury jako wzmacniacza w atakach typu DRDoS (Distributed Reflection Denial of Service), zalecane jest blokowanie na brzegu sieci przychodzącego ruchu klienckiego protokołów i usług powszechnie wykorzystywanych do amplifikacji ruchu (np. NTP, SNMP, SSDL).

⁸ RA Guard (Router Advertisement Guard) – mechanizm bezpieczeństwa stosowany na przełącznikach sieciowych w sieciach IPv6. Kontroluje on komunikaty Router Advertisement (RA) i blokuje je na portach, do których nie powinny być podłączone routery.

⁹ BGP FlowSpec (Border Gateway Protocol Flow Specification) – rozszerzenie protokołu BGP umożliwiające dystrybucję reguł filtrowania ruchu (tzw. flow specifications) w sieci, pozwalających na dynamiczne sterowanie przepływami danych na podstawie takich parametrów jak adresy IP, porty czy protokoły.

¹⁰ BCP 38 (Best Current Practice 38) – dobra praktyka opisana w RFC 2827, polegająca na filtrowaniu ruchu przychodzącego do sieci operatora w celu blokowania pakietów z podrobionym adresem źródłowym IP.

¹¹ uRPF to mechanizm bezpieczeństwa na routerach sieciowych, który walczy z fałszowaniem adresów IP (IP spoofing) poprzez sprawdzanie czy pakiet przybył z kierunku, który w tablicy routingu jest poprawną drogą powrotną do jego nadawcy.

¹² Bogon (adres bogonowy) – nieformalny termin określający adres IP, który nie powinien pojawiać się w publicznym ruchu internetowym, ponieważ jest niezarezerwowany, nieprzydzielony przez IANA/RIR lub przeznaczony do specjalnych zastosowań (np. adresy prywatne, loopback).

8. **Ochrona i separacja warstwy zarządzania:** wdrożenie mechanizmów ochrony warstwy zarządzania urządzeniami przed wpływem czynników z nią niepowiązanych. Zalecamy izolację sieci zarządzania od sieci realizującej ruch użytkowników (izolacja fizyczna lub logiczna) oraz rygorystyczne ograniczenie dostępu administracyjnego do zaufanych urządzeń, np. z wykorzystaniem list kontroli dostępu (ACL) z regułami zezwalającymi.
9. **Uzyskanie wsparcia od operatorów upstream:** przygotowanie procedury bieżącego kontaktu 24/7 z operatorami upstream w trakcie mitygacji ataków DDoS. Ponadto zaleca się uzgodnienie z operatorami upstream możliwości wdrożenia mechanizmów D/RTBH (Destination-based Remotely Triggered Black Hole) oraz S/RTBH (Source-based Remotely Triggered Black Hole). Należy zaznaczyć, że dla skutecznego działania mechanizmu S/RTBH niezbędne jest uruchomienie mechanizmu uRPF na interfejsach, na których filtrowanie jest realizowane.
10. **Zapewnienie możliwości skierowania ruchu do zewnętrznego scrubbing center:** zapewnienie przez operatorów możliwości przekierowania ruchu sieciowego do zewnętrznego punktu filtrowania ruchu (scrubbing center) w trakcie ataku DDoS. Obejmuje to zawarcie odpowiednich umów z dostawcami usług scrubbingowych oraz przygotowanie technicznej gotowości do przekierowania ruchu. Procedura przekierowania ruchu powinna być regularnie testowana.
11. **Aktualizacja sprzętowej infrastruktury sieciowej** na posiadającą wsparcie producenta oraz dla której wydawane są aktualizacje oprogramowania oraz aktualizacje bezpieczeństwa.
12. **Architektura sieci**
 - a) Rozdzielenie funkcji. Router BGP, CGNAT¹³ i BRAS¹⁴ na jednym, kilkunastoletnim urządzeniu to pojedynczy punkt awarii. Stanowy CGNAT podczas intensywnego ruchu lub ataku wolumetrycznego może doprowadzić do wyczerpania tablic sesji, pamięci albo zasobów obliczeniowych urządzenia. Należy wziąć pod uwagę również ochronę control plane, zabezpieczenie sesji BGP oraz nieogłaszanie adresacji infrastruktury i połączeń punkt-punkt do Internetu.
 - b) Dywersyfikacja upstreamów i przygotowany BGP. Potrzebnych jest co najmniej dwóch niezależnych dostawców tranzytu oraz uzgodnione i przetestowane community do RTBH lub selektywnego blackholingu. Jeśli podmiot korzysta ze scrubbingu, powinien przygotować zawnazu ROA¹⁵ w RPKI¹⁶ dla AS dostawcy oraz upoważnienie (LOA¹⁷), żeby w trakcie ataku nie tracić czasu na formalności i odrzucane ogłoszenia.

¹³ CGNAT (Carrier Grade NAT) - Wielkoskalowa translacja adresów IP dla tysięcy abonentów na brzegach sieci.

¹⁴ BRAS (Broadband Remote Access Server) - Serwer dostępowy kończący sesje szerokopasmowe abonentów i odpowiadający za ich autoryzację.

¹⁵ ROA (Route Origin Authorization) - wskazuje, który system autonomiczny (AS) jest uprawniony do ogłaszania danego bloku adresów.

¹⁶ ROKI (Resource Public Key Infrastructure) - System kryptograficznej weryfikacji prawa do ogłaszania prefiksów w BGP.

¹⁷ LOA (Letter of Authorization) - Formalne upoważnienie wydawane dostawcy scrubbing center do ogłaszania prefiksów IP należących do operatora w protokole BGP.

- c) Zarządzanie out-of-band. Rekomendacja mówi o separacji sieci zarządzania. Warto pójść dalej i zapewnić dostęp OOB¹⁸ fizycznie niezależny od sieci produkcyjnej, np. przez LTE, osobne łącze i serwery konsolowe. Kiedy łącza są przepełnione, administrator nadal musi mieć dostęp do interfejsów zarządzania urządzeń sieciowych.
13. **Monitorowanie ruchu wychodzącego:** zaleca się ciągłą analizę anomalii w ruchu wychodzącym z sieci ISP. Zainfekowane urządzenia klienckie (w tym routery brzegowe oraz urządzenia IoT) stanowią potencjalny zasób do budowy sieci botnet, w wyniku czego infrastruktura operatora może stać się nie tylko celem ataku, ale również wektorem jego realizacji. Oprócz blokowania amplifikacji na wejściu warto regularnie skanować własną sieć w poszukiwaniu otwartych resolverów DNS, usług SSDP¹⁹, memcached²⁰ i podobnych, a zainfekowane urządzenia izolować i kontaktować się z abonentami.
14. **Kontakt z zespołami CSIRT poziomu krajowego i sektorowego:** przygotowanie procedury kontaktu z zespołem CSIRT²¹ w przypadku ataku DDoS oraz natychmiastowe zgłoszenie incydentu poprzez dostępny kanał (system S46 lub formularz na stronie <https://cyber.gov.pl>).
- Zgłoszenie powinno zawierać: zakres atakowanej adresacji lub adresacji użytej do ataku bez wiedzy właściciela/użytkownika, numer AS operatora, informację o czasie trwania ataku i jego aktualnym wpływie na infrastrukturę (w szczególności czy problemy z dostępnością dotyczą podmiotów publicznych), dane kontaktowe osoby odpowiedzialnej za obsługę incydentu (numer telefonu, adres e-mail). Ponadto możliwe jest występowanie do właściwego zespołu CSIRT o wsparcie w procesie odblokowywania adresacji operatora z list blokujących (blacklist) utrzymywanych przez instytucje zewnętrzne (w szczególności państwowe), w sytuacji gdy adresacja ta zostanie na nie wpisana w wyniku ataków wykorzystujących odbicie (DRDoS) zrealizowanych z fałszowaniem adresów źródłowych (IP spoofing).
- Należy zgłaszać także ataki odparte i te, w których sieć ISP była źródłem. Dopiero dane od wielu operatorów pozwalają CSIRT zobaczyć całą kampanię. Dane flow i logi z incydentu należy przechowywać jako materiał dowodowy. Pozwalają również na przekazanie informacji do dostawców usług, w szczególności usług o istotnym znaczeniu z punktu widzenia bezpieczeństwa państwa oraz porządku publicznego.
15. **Zgłoszenie przestępstwa:** wszystkie próby wyłudzeń należy zgłaszać do Policji, aby mogła skutecznie zebrać materiał dowodowy oraz ocenić skalę takiej działalności. Odpowiednie rozpoznanie i dostarczenie informacji skutecznie wspierają prowadzone przez służby postępowania²².

¹⁸ OOB (Out-of-Band) - Niezależny, fizycznie wyodrębniony kanał dostępu administracyjnego do urządzeń (np. przez modem LTE i serwery konsolowe), działający nawet przy całkowitym wysyceniu łącza produkcyjnych.

¹⁹ SSDP (Simple Service Discovery Protocol) to protokół sieciowy służący do automatycznego wykrywania urządzeń i usług w sieci lokalnej bez konieczności ich wcześniejszej konfiguracji czy udziału serwerów DHCP/DNS.

²⁰ Memcache - System rozproszonego buforowania danych w pamięci RAM.

²¹ Do czasu ustanowienia CSIRT sektorowego dla podsektora komunikacji elektronicznej przez organ właściwy do spraw cyberbezpieczeństwa dla tego podsektora (tj. Prezes Urzędu Komunikacji Elektronicznej) incydenty należy zgłaszać do CSIRT NASK będącym CSIRT-em poziomu krajowego. Jednocześnie przedsiębiorca telekomunikacyjny może skontaktować się z UKE wysyłając wiadomość na adres uksc@uke.gov.pl, aby przekazać informacje o sytuacji i uzyskać wsparcie w zakresie właściwym dla Urzędu.

²² <https://www.gov.pl/web/gov/zglos-przestepstwo>

Rekomendacja została opracowana w ramach współpracy Ministerstwa Cyfryzacji oraz CSIRT NASK, CSIRT GOV oraz Urzędu Komunikacji Elektronicznej.

Krzysztof Gawkowski

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Wiceprezes Rady Ministrów

Minister Cyfryzacji

/dokument podpisany elektronicznie/