Wiceprezes Rady Ministrów
Minister Cyfryzacji

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Krzysztof Gawkowski

DC.WAC.5555.40.2026
Warszawa, 29 czerwca 2026

Rekomendacja Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa

nr 2026/67a/5

dotycząca ochrony ISP przed atakami typu DDoS[1]

Niniejsza rekomendacja została wydana na podstawie art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[2]. Jej celem jest podniesienie poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa (KSC), w związku z zagrożeniem ataków 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. Polega on na zasypaniu serwera, aplikacji lub infrastruktury sieciowej ogromną liczbą żądań pochodzących z wielu rozproszonych źródeł. Działanie to jest skuteczne z tego powodu, że żaden system nie dysponuje nieograniczonymi zasobami. Każda usługa internetowa opiera się na określonej mocy obliczeniowej (procesor, pamięć), przepustowości łącza oraz możliwości obsługi jednoczesnych połączeń. Gdy liczba żądań przekroczy te możliwości, system przestaje odpowiadać poprawnie co sprawia, że usługa nie działa prawidłowo. Najpopularniejsze ataki DDoS:

1. Ataki Wolumetryczne (Volumetric attacks) – Ich celem jest zajęcie całej przepustowości łącza internetowego. Atakujący generuje ogromną ilość ruchu (np. gigabity na sekundę), aby zapchać sieć (np. UDP Flood),
2. Ataki na protokoły (Protocol attacks) – Skupiają się na wykorzystaniu słabości w protokołach sieciowych i przeciążeniu urządzeń takich jak serwery lub firewalle (np. SYN flood),
3. Ataki na warstwę aplikacji – Najbardziej wyrafinowane, mniejsze objętościowo, ale bardzo trudne do wykrycia, ponieważ naśladują zachowanie prawdziwych użytkowników (np. HTTP flood).

Rekomendacja

Zespoły CSIRT poziomu krajowego wskazują, że podmioty krajowego systemu cyberbezpieczeństwa często nie są przygotowane na ataki DDoS, co może prowadzić do nieprawidłowego funkcjonowania udostępnianych usług. W związku z powyższym rekomenduję wdrożenie niżej wymienionych zaleceń:

1. **Konfiguracja telemetrii:** wdrożenie próbkowania ruchu obejmującego warstwy L2-L4 modelu ISO/OSI na routerach brzegowych oraz na przełącznikach. Zbierane

[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).

telefon: +48 22 245 54 42
adres email: sekretariat.BM@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

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.

2. **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 skalę automatyzacji powinny być dostosowane do specyfiki danej sieci. Rozwiązanie to może polegać np. na automatycznej mitygacji z wykorzystaniem BGP Flowspec[3]. W przypadku braku możliwości jej zastosowania, rekomenduje się implementację bezstanowych filtrów firewall oraz konfigurację sprzętowych ograniczników pasma (policerów) na interfejsach WAN.
3. **Weryfikacja adresów źródłowych (BCP 38):** wdrożenie uRPF[4] 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.
4. **Filtracja adresów Bogon**[5]: Na portach dostępowych zaleca się wdrożyć prefix-listy odrzucające pakiety z źródłowymi lub docelowymi adresami Bogon (przestrzenie prywatne RFC 1918, adresy lokalne, multicast oraz nieprzydzielone przez IANA).
5. **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).
6. **Ochrona i separacja warstwy zarządzania**: wdrożenie mechanizmów ochrony warstwy zarządzania urządzeniami przed wpływem czynników z nią niepowiązanych. Zaleca się 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.
7. **Kontakt z zespołami CSIRT poziomu krajowego i sektorowego**: Zaleca się przygotowanie procedury kontaktu z zespołem CSIRT 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

[3] 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.

[4] 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.

[5] 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).

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).

8. Uzyskanie wsparcia od dostawcy usług internetowych (ISP) w zakresie przeciwdziałania atakom DDoS, obejmujące m.in. filtrację ruchu na poziomie sieci operatorskiej, przekierowanie ruchu do centrów scrubbingowych (scrubbing centers).

Rekomendacja została opracowana dzięki współpracy Ministerstwa Cyfryzacji oraz CSIRT NASK, CSIRT MON i CSIRT GOV.

Krzysztof Gawkowski
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Wiceprezes Rady Ministrów
Minister Cyfryzacji
/dokument podpisany elektronicznie/