



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.187.2026
Warszawa, 04 października 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 14 września br. Postów na Sejm RP Panów Michała Wosia oraz Dariusza Mateckiego w sprawie narastającej fali skoordynowanych ataków DDoS na lokalnych operatorów telekomunikacyjnych oraz niewystarczającego systemowego wsparcia państwa dla podmiotów zapewniających łączność mieszkańcom i instytucjom publicznym (interpelacja nr 19640)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Postów pytania.

Ministerstwo Cyfryzacji posiada wiedzę na temat ataków DDoS wymierzonych w lokalnych dostawców usług internetowych (ISP) w Polsce i podejmuje we współpracy z innymi instytucjami odpowiednie działania w tej sprawie. Temat ten był m.in. przedmiotem prac Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), jak również ustaleń w innych formatach.

W czerwcu br. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa wydał rekomendację dotyczącą ochrony ISP przed atakami typu DDoS¹. Dokument ten określa konkretne wytyczne wdrożeniowe w zakresie bezpiecznej konfiguracji urządzeń sieciowych, automatyzacji wykrywania anomalii oraz mitygacji skutków ataków wolumetrycznych. Obecnie planowane jest przygotowanie aktualizacji tej rekomendacji.

Zwracam jednocześnie uwagę, że organem właściwym do spraw cyberbezpieczeństwa dla podsektora komunikacji elektronicznej (w tym dostawców usług internetowych), zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa², jest Prezes Urzędu Komunikacji Elektronicznej (UKE). Ministerstwo Cyfryzacji koordynuje działania w tej sprawie m.in. z UKE.

UKE powołał zespół roboczy, który jest w stałym kontakcie z operatorami ISP. W ramach prac zespołu UKE dostawcy usług internetowych mają zapewnione wsparcie merytoryczne i techniczne, obejmujące m.in. pomoc w prawidłowej konfiguracji urządzeń w celu minimalizacji skutków incydentów.

Warto również wskazać, że Ministerstwo Cyfryzacji prowadzi darmowe szkolenia dla podmiotów KSC³, co pozwala podnieść poziom kompetencji pracowników odpowiedzialnych za cyberbezpieczeństwo.

Odnosząc się do kwestii wsparcia finansowego należy zwrócić uwagę, że takie działania muszą odbywać się z poszanowaniem zasad uczciwej konkurencji i nie mogłoby być niedozwoloną pomocą publiczną. Dostawcy ISP są prywatnymi podmiotami konkurującymi ze sobą na rynku komercyjnym. Podmioty te powinny w swojej działalności uwzględniać inwestycje w cyberbezpieczeństwo nie tylko z uwagi ryzyka występujące w działalności gospodarczej, ale też, aby spełniać wymogi cyberbezpieczeństwa określone w art. 8 ustawy o KSC. Po wejściu w życie 3 kwietnia 2026 r. nowelizacji ustawy o KSC, dostawcy usług

¹ <https://www.gov.pl/web/baza-wiedzy/rekomendacja-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa-dotyczaca-ochrony-isp-przed-atakami-typu-ddos>

² Art. 41 pkt 8a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.) (dalej: ustawa o KSC)

³ <https://www.gov.pl/web/baza-wiedzy/szkolenia>

internetowych (przedsiębiorcy komunikacji elektronicznej) zostali objęci podwyższonymi wymogami cyberbezpieczeństwa. Nakłada to na tych dostawców obowiązek m.in. wdrożenia systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniającego w szczególności:

- 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
- 2) 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, w szczególności:
 - a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
 - b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
 - c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu,
 - d) bezpieczeństwo zasobów ludzkich,
 - e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
 - f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,
 - g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym.

Niezależnie od powyższego Ministerstwo Cyfryzacji planuje działania mające na celu minimalizację skutków dla obywateli oraz podmiotów i usług publicznych w przypadku braku dostępności internetu spowodowanej atakami DDoS na ISP.

Należy również nadmienić, że Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) pod nadzorem prokuratury prowadzi śledztwo dotyczące ataków DDoS.

Działania w tej sprawie realizuje również zespół reagowania na incydenty bezpieczeństwa komputerowego CSIRT NASK, zgodnie ze swoim zakresem odpowiedzialności określonym w art. 26 ustawy o KSC.

Zwracam także uwagę, że Ministerstwo Cyfryzacji zapewnia rozwiązanie AntyDDoS, którego celem jest zapewnienie ochrony przed atakami DDoS dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP. System ten chroni ok. 80 podmiotów, w tym m.in. Siły Zbrojne RP. Projekt ten w swoim założeniu nie obejmuje dostawców ISP.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych