Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.168.2025
Warszawa, 10 października 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 26 września br. Posła na Sejm RP Pana Piotra Górnikiewicza w sprawie integralności systemów wspierających procesy legislacyjne (interpelacja nr 12349)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na pytania Posła RP Piotra Górnikiewicza.

Ad 1) Czy znany jest powód wystąpienia ostatnich błędów związanych z konsultacjami sejmowymi?

Sejm Rzeczypospolitej Polskiej - zgodnie z Regulaminem Sejmu Rzeczypospolitej Polskiej[1] - do prowadzenia konsultacji społecznych wykorzystuje System Informacyjny Sejmu (art. 34a). System ten jest prowadzony przez Sejm RP (art. 201a). W związku z tym adresatem pytania powinna być Kancelaria Sejmu RP.

Ad 2) Czy w ostatnim okresie odnotowano inne incydenty wpływające na wyniki e-konsultacji lub inne procesy legislacyjne (np. błędne przypisania)?

Zgodnie z art. 22 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[2] (ustawa o KSC) podmioty Krajowego Systemu Cyberbezpieczeństwa (KSC), w tym podmioty publiczne (które wykorzystują systemy elektroniczne wspierające konsultacje i procesy legislacyjne) zobowiązane są zgłaszać incydenty cyberbezpieczeństwa do właściwego jednego z trzech zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego, o których mowa w art. 2 pkt 1-3 ustawy o KSC:

a) CSIRT GOV - prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
b) CSIRT NASK - prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
c) CSIRT MON - prowadzony przez Ministra Obrony Narodowej;

zgodnie z zakresem odpowiedzialności poszczególnych CSIRT określonym w art. 26 ustawy o KSC.

Dane przekazywane przez zespoły CSIRT do Ministerstwa Cyfryzacji nie wskazywały na incydenty cyberbezpieczeństwa dotyczące systemów konsultacji elektronicznych lub innych procesów legislacyjnych.

Ad 3) Czy ministerstwo przewiduje w ciągu najbliższych 24 miesięcy dodatkowe działania lub zwiększenie finansowania mające na celu wzmocnienie, rozbudowę lub aktualizację

[1] M.P. z 2022 r. poz. 990 późn. zm.
[2] Dz.U. z 2024 r. poz. 1077 z późn. zm.

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

ul. Królewska 27
00-060 Warszawa

systemów Sejmu i Senatu? Jeśli tak — proszę o krótką informację o zakresie planowanych działań.

Mając na względzie niezależność władzy ustawodawczej i wykonawczej Sejm RP i Senat RP są instytucjami, które same określają swój budżet. Zgodnie z art. 139 ust. 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych[3] Minister Finansów włącza do projektu ustawy budżetowej dochody i wydatki Kancelarii Sejmu, Kancelarii Senatu (i innych wskazanych w tym przepisie instytucji, które są niezależne od władzy wykonawczej). W związku z tym podmioty te powinny uwzględnić wydatki na wzmocnienie, rozbudowę lub aktualizację swoich systemów przy projektowaniu swojego budżetu.

Niezależnie od tego należy podkreślić, że Ministerstwo Cyfryzacji i inne instytucje KSC zapewniające cyberbezpieczeństwo na poziomie krajowym prowadzą szereg działań wspierających cyberbezpieczeństwo podmiotów KSC, w tym instytucji publicznych. Szczegółowo opisane są one w Sprawozdaniu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2024 rok[4]. Wśród działań, których beneficjentem są m.in. Sejm RP i Senat RP, warto wymienić m.in.:

- osłonę przed atakami typu DDoS, którą Ministerstwo Cyfryzacji we współpracy z NASK-PIB zapewnia centralnie dla kilkudziesięciu kluczowych instytucji administracji publicznej;
- prowadzony przez Ministerstwo Cyfryzacji we współpracy z NASK-PIB projekt SecureV – dedykowane szkolenia cyberbezpieczeństwa dla najważniejszych osób w państwie;
- system rozpoznawania zagrożeń w cyberprzestrzeni (CTI), który Ministerstwo Cyfryzacji udostępnia dla instytucji zapewniających bezpieczeństwo teleinformatyczne państwa, które wykorzystują go do wspierania podmiotów KSC.

Ad 4) Czy systemy parlamentarne są częstymi celami ataków? Czy ministerstwo prowadzi statystyki obejmujące ich liczbę, rodzaj oraz kierunek, z których pochodzą?

Zgodnie z art. 22 ust. 1 pkt 2 ustawy o KSC Sejm RP i Senat RP i ich kancelarie, jako podmioty publiczne, zobowiązane są zgłaszać incydenty cyberbezpieczeństwa do właściwego zespołu CSIRT poziomu krajowego. Zgodnie z art. 26 ust. 7 pkt 1 właściwym zespołem CSIRT dla Sejmu RP i Senatu RP jest CSRIT GOV prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego. Dane udostępniane przez CSIRT GOV nie wyszczególniają incydentów zgłaszanych przez Sejm RP i Senat RP.

W przypadku incydentów dotyczących kluczowych elementów KSC, w tym takich jak organy władzy publicznej, sprawa ta jest koordynowana w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), w którym pod auspicjami Ministerstwa Cyfryzacji współpracują najważniejsze instytucje dla bezpieczeństwa teleinformatycznego RP. PCOC działa w trybie niejawnym.

Należy także zwrócić uwagę, że serwisy parlamentu są częstym celem ataków DDoS. Zgodnie z informacją udzieloną w odpowiedzi na pytanie nr 3 Ministerstwo Cyfryzacji zapewnia centralnie ochronę przed tego rodzajami atakami.

Z wyrazami szacunku
Paweł Olszewski

---

[3] Dz.U. z 2024 r. poz. 1530 z późn. zm.
[4] https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie

Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

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

ul. Królewska 27
00-060 Warszawa