Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.175.2025
Warszawa, 20 października 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 3 października br. Posłów na Sejm RP Pani Lidii Czechak, Pani Wioletty Marii Kulpy oraz Pana Roberta Warwasa w sprawie zapewnienia stabilności systemu płatności bezgotówkowych oraz utrzymania gotówki jako alternatywnego środka płatniczego w Polsce (interpelacja nr 12541)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytanie będące we właściwości Ministra Cyfryzacji.

Ad 4) Czy Ministerstwo Cyfryzacji planuje współpracę z operatorami systemów płatności oraz bankami w celu opracowania i wdrożenia planów awaryjnych, które zapewnią ciągłość świadczenia usług płatniczych w przypadku wystąpienia awarii?

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa[1] organem właściwym do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych jest Komisja Nadzoru Finansowego.

Należy ponadto zaznaczyć, że w przypadku, gdy podmiot w danym sektorze wyznaczony został przez organ właściwy do spraw cyberbezpieczeństwa jako operator usługi kluczowej, zobowiązany jest realizować obowiązki określone w art. 8-16a ustawy o KSC w tym m.in. - zgodnie z art. 8 - wdrożyć system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający:

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, w tym:
   a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
   b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
   c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
   d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
   e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

[1] Art. 41 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 z późn. zm.) (dalej „ustawa o KSC")

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

ul. Królewska 27
00-060 Warszawa

3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
   a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
   b) dbałość o aktualizację oprogramowania,
   c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
   d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Z wyrazami szacunku

Paweł Olszewski
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