# Środki ochrony w zakresie cyberbezpieczeństwa

KLST – Krytyczne lotnicze systemy teleinformatyczne są to krytyczne systemy technologii informacyjno-komunikacyjnych, rozumiane jako systemy informacyjne w rozumieniu ustawy KSC, przeznaczone do przetwarzania danych wykorzystywanych dla bezpieczeństwa, ochrony lub dostępności operacji lotniczych.

TU WPISZ: nazwa podmiotu TU WYBIERZ: nie został uznany /został uznany za operatora usługi kluczowej oraz TU WYBIERZ: nie znajduje się/znajduje się na liście operatorów usług kluczowych prowadzonym przez ministra właściwego ds. informatyzacji, zgodnie z przepisami ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i poz. 2445).

TU WPISZ: Nazwa podmiotu zidentyfikował następujące krytyczne lotnicze systemy teleinformatyczne (KLST) oraz dane, przetwarzane w postaci elektronicznej, wykorzystywane dla bezpieczeństwa, ochrony lub dostępności operacji lotniczych:

Proszę podać rodzaj i nazwę krytycznych lotniczych systemów teleinformatycznych występujących w Państwa podmiocie, przykładowo:

1. System kontroli dostępu
2. Urządzenia wykorzystywane do kontroli bezpieczeństwa
3. System CCTV
4. System sygnalizacji włamania i napadu
5. System sygnalizacji pożaru
6. Systemy, w których przechowuje się informacje o przeszukaniu statków powietrznych
7. Systemy służące do zabezpieczenia statku powietrznego przed nieuprawnionym dostępem
8. Systemy odprawy, transportu oraz łączenia bagażu z pasażerem
9. Systemy do przesyłania informacji o statusie ochrony ładunku i poczty
10. Systemy zarządzania zasilaniem, w tym awaryjnym
11. Systemy ATM/ANS
12. Systemy służące do planowania operacji lotniczych
13. Systemy służące do obsługi naziemnej statku powietrznego

KLST chronione są przed zagrożeniami, które mogą wpłynąć na poufność, dostępność lub integralność przetwarzanych informacji ze strony człowieka, sprzętu, oprogramowania oraz siły wyższej, a w szczególności związanych z:

1. awariami systemów teleinformatycznych,
2. awariami infrastruktury,
3. zagrożeniami wewnętrznymi (insider),
4. wykorzystaniem podatności/luki bezpieczeństwa,
5. atakiem z użyciem złośliwego oprogramowania,
6. atakiem ransomware,
7. atakiem DoS,
8. kradzieżą nośników danych,
9. kradzieżą własności intelektualnej i przemysłowej,
10. kradzieżą lub złamanie poufności tajemnic prawnie chronionych,
11. szpiegostwem, w tym szpiegostwem przemysłowym,
12. wyciekiem danych,
13. kradzieżą danych.

W związku z powyższym TU WPISZ: nazwa podmiotu przeprowadził ocenę ryzyka, o której mowa w § 86 pkt. 2 KPOLC, w celu określenia i wdrożenia środków mających na celu ochronę wyżej wymienionych KLST. TU WPISZ: Nazwa podmiotu stosuje następujące środki bezpieczeństwa:

Proszę wymienić środki ochrony stosowane w Państwa podmiocie, przykładowo:

1. Politykę Bezpieczeństwa Informacji
2. Politykę/ zasadę czystego biurka
3. Politykę/ zasadę czystego ekranu
4. Zasady budowania haseł
5. Umowę o Zachowaniu Poufności
6. Procedury postępowania w przypadku wystąpienia incydentu bezpieczeństwa
7. Rejestr urządzeń
8. Politykę kluczy
9. Politykę Korzystania ze Sprzętu Prywatnego
10. Plany postępowania awaryjnego
11. Program antywirusowy
12. Program antyspamowy
13. Firewall
14. Zasilanie awaryjna
15. Logowania do systemu z wykorzystaniem loginu i hasła
16. VPN
17. Kopie zapasowe
18. Szyfrowanie danych (proszę podać stosowany ALGORYTM)
19. Blokowanie portów
20. Szkolenia osób zatrudnionych w podmiocie
21. Skanery podatności
22. Testy penetracyjne i audyty bezpieczeństwa
23. Plany / procedury postępowania awaryjnego na wypadek incydentu / naruszenia bezpieczeństwa KLST, włącznie z reagowaniem na zdarzenie i odtwarzaniem infrastruktury.

TU WPISZ: Nazwa podmiotu zapewnia, że osoby wdrażające wyżej wymienione środki bezpieczeństwa, posiadają odpowiednie kwalifikacje i umiejętności niezbędne do skutecznego wykonywania wyznaczonych zadań oraz są one informowane o istotnych przypadkach zagrożeń dla cyberbezpieczeństwa, zgodnie z zasadą ograniczonego dostępu.

Osobami odpowiedzialnymi za wdrażanie wyżej wymienionych środków bezpieczeństwa są TU WPISZ imię i nazwisko osoby lub nazwę komórki organizacyjnej lub nazwę firmy zewnętrznej.

TU WPISZ: Nazwa podmiotu opracował procedurę postępowania na wypadek naruszenia bezpieczeństwa KLST. W przypadku wystąpienia incydentu bezpieczeństwa KLST należy niezwłocznie powiadomić wyznaczonego pracownika – TU WPISZ imię i nazwisko osoby lub nazwę komórki organizacyjnej lub nazwę firmy zewnętrzne oraz sposób powiadamiania np. adres e-mail, numer telefonu .

W przypadku wystąpienia poważnego zagrożenia cyberbezpieczeństwa, wyznaczony pracownik powiadamia:

1. TU WYBIERZ: CSIRT NASK: na e-mail: ksc@cert.pl, lub poprzez formularz: <https://incydent.cert.pl/#!/lang=pl> lub CSIRT GOV na e-mail: incydent@csirt.gov.pl lub poprzez formularz: [https://csirt.gov.pl/cer/zglaszanie-incydentu/16,Zglaszanie-incydentu.html](https://csirt.gov.pl/cer/zglaszanie-incydentu/16%2CZglaszanie-incydentu.html).
2. Prezesa ULC

W przypadku podejrzenia popełnienia przestępstwa wyznaczony TU WPISZ: nazwa podmiotu zawiadamia również Policję lub ABW.

Administratorzy oraz użytkownicy KLST podlegają szkoleniu, o którym mowa w pkt. 11.2.8 załącznika do Rozporządzenia 2015/1998.

Wszystkie osoby wdrażające środki ustanowione w pkt. 1.7.2 załącznika do Rozporządzenia 2015/1998 posiadają kwalifikacje i umiejętności niezbędne do skutecznego wykonywania wyznaczonych zadań oraz są informowane o istotnych przypadkach zagrożeń dla cyberbezpieczeństwa zgodnie z zasadą ograniczonego dostępu.