

Szczegółowy zakres usługi

1. AUDYT DOKUMENTACJI Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) wykonany w oparciu o:

- 1) zapisy Ustawy z dnia 23 stycznia 2026r o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, wdrażającej tzw. Dyrektywę NIS2
- 2) zapisy Rozporządzenia Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanego ogólnym Rozporządzeniem o ochronie danych osobowych (RODO),
- 3) wymogi ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych

z uwzględnieniem wymogów normy ISO 27001, w tym w szczególności:

- 1) przeprowadzenie analizy występowania ryzyka w Urzędzie Gminy Lutocin oraz jednostkach podległych jako podmiotów ważnych lub kluczowych w rozumieniu przepisów ustawy o krajowym systemie cyberbezpieczeństwa,
- 2) weryfikacja prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu bezpieczeństwa informacji oraz zarządzania tym ryzykiem;
- 3) weryfikacja wdrożenia odpowiednich i proporcjonalnych do oszacowanego ryzyka środków organizacyjnych, w szczególności:
 - a) polityk szacowania ryzyka oraz bezpieczeństwa systemu informatycznego, w tym polityki tematycznych,
 - b) zasad bezpieczeństwa w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowania systemu informacyjnego,
 - c) procedur w zakresie bezpieczeństwa fizycznego i środowiskowego uwzględniającego kontrole dostępu,
 - d) procedur w zakresie bezpieczeństwa zasobów ludzkich,
 - e) procedur w zakresie bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy funkcjonowanie Urzędu Gminy, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a Gminą Lutocin oraz jednostkami podległymi.
 - f) procedur i dokumentacji operacyjnej w zakresie wdrażania, dokumentowania, testowania i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usług oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych, oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informatycznego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,
 - g) procedur odzwierciedlających objęcie systemu informatycznego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,
 - h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
 - i) dokumentacji edukacji z zakresu cyberbezpieczeństwa dla personelu podmiotu,
 - j) dokumentacji rozliczającej wprowadzenie podstawowych zasady cyberhigieny,
 - k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,
 - l) procedur regulujących stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach;
 - m) procedur dotyczących zarządzania aktywami,
 - n) polityki kontroli dostępu;
- 4) weryfikacja zbierania informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;
- 5) weryfikacja procedur w zakresie zarządzania incydentami;
- 6) weryfikacja procedur w zakresie stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informatycznego wykorzystywanego do świadczenia usługi, w tym w szczególności w zakresie:
 - a) stosowania mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informatycznym,
 - b) sformalizowanego obowiązku regularnego przeprowadzania aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,
 - c) ochrony przed nieuprawnioną modyfikacją w systemie informacyjnym,

- d) niezwłocznego podejmowania działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowego ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu, które może skutkować zakłóceniem funkcjonowania, mając na uwadze konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.
- 7) weryfikacja procedur/zasad bezpieczeństwa współpracy z podmiotami ICT, uwzględniających:
 - a) podatności związane z dostawą sprzętu lub oprogramowania;
 - b) ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania;
 - c) wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555”;
- 8) weryfikacja procedur w zakresie kontroli, monitorowania i testowania wprowadzonych środków bezpieczeństwa, w tym audytów i przeglądów dokumentacji,
- 9) weryfikacja dokumentacji ochrony danych osobowych.

Audyt zostanie przeprowadzony w siedzibie Zleceniodawcy w uzgodnionym terminie (maksymalnie w ciągu dwóch dni roboczych). Sprawozdanie z audytu wraz z zaleceniami zostanie przesłane w ciągu 14 dni roboczych od zakończenia audytu.

2. DOKUMENTACJA SZBI

Po przedstawieniu raportu z audytu oraz omówienia jego wyników ustalone zostaną dalsze działania (ustalenie strategii działania, zespołu wdrożeniowego, budżetu, harmonogramu działań).

Po ustaleniu Strategii, opracowana zostanie dokumentacja SZBI, obejmująca wymogi NIS2, z uwzględnieniem wymogów normy ISO 27001, w tym m.in.:

- 1) zarządzanie incydentami bezpieczeństwa i cyberatakami,
- 2) zarządzanie ryzykiem cyberbezpieczeństwa,
- 3) zarządzanie podatnościami i procesem aktualizacji zabezpieczeń,
- 4) monitorowanie bezpieczeństwa oraz analiza zdarzeń,
- 5) zarządzanie dostawcami i bezpieczeństwem łańcucha dostaw,
- 6) zarządzanie aktywami informacyjnymi i ich klasyfikacją,
- 7) ciągłość działania i odtwarzanie po awarii,
- 8) raportowanie cyberbezpieczeństwa do kierownictwa,
- 9) okresowa ocena skuteczności wdrożonych zabezpieczeń.

3. SZKOLENIE Z PRZEPISÓW NIS2 I ZASAD CYBERBEZPIECZEŃSTWA

Przeprowadzenie dedykowanego stacjonarnego szkolenia dla pracowników Urzędu Gminy oraz jednostek organizacyjnych w co najmniej dwóch grupach szkoleniowych. Każdy pracownik otrzyma certyfikat.

Szkolenie mogą prowadzić osoby posiadające odpowiednie certyfikaty uprawniające do ich przeprowadzenia