Krajowy System Cyberbezpieczeństwa w urzędach

Jak zaktualizować dokumentację pod kątem nowelizacji KSC? Jakie działania musi podjąć przełożony/kierownik/naczelnik w urzędzie? Jak wygląda zmiana na osobistą odpowiedzialność kierowników w praktyce? Przygotowanie do audytu.

Wideoszkolenie dla kierowników, naczelników, dyrektorów oraz sekretarzy i informatyków w urzędach, którzy realizują zadania w ramach krajowego systemu cyberbezpieczeństwa.

Na czym polega identyfikacja podmiotów w KSC? Jak zorganizować KSC w urzędzie i przygotować się do obowiązków na 3 kwietnia 2027 r.?

Szkolenie dla kadry zarządzającej urzędów porządkuje identyfikację podmiotów objętych KSC oraz organizację obowiązków w urzędzie. Ekspert Mariusz Lis omówi podział zadań między kierownictwem a IT, wdrożenie i aktualizację SZBI, analizę ryzyka i przygotowanie do audytów. Program uwzględnia weryfikację obowiązków rejestracyjnych oraz przygotowanie do terminu 3 kwietnia 2027 r. Osobne miejsce zajmują finansowanie, utrzymanie wdrożonych rozwiązań i praca przy ograniczonych zasobach.

W programie m.in.:

- **Status podmiotu w KSC** – identyfikacja jednostek organizacyjnych oraz rozróżnienie podmiotów kluczowych i ważnych.
- **Terminy wdrożenia** – weryfikacja obowiązków dotyczących wykazu KSC oraz przygotowanie do wymagań przewidzianych na 3 kwietnia 2027 r.
- **Organizacja odpowiedzialności** – podział zadań w urzędach, obowiązki kierownictwa oraz współpraca osoby odpowiedzialnej za cyberbezpieczeństwo z IT.
- **Dokumentacja i SZBI** – przełożenie wymagań ustawowych na procedury wewnętrzne oraz dobór środków bezpieczeństwa.
- **Ryzyko i audyty** – szacowanie ryzyka, przeglądy zabezpieczeń, przygotowanie dokumentacji oraz realizacja zaleceń poaudytowych.
- **Finansowanie** – wykorzystanie programu Cyberbezpieczny Samorząd i planowanie utrzymania systemów po zakończeniu projektu.
- **Ograniczone zasoby** – priorytety przy małym budżecie, organizacja monitoringu, szkolenie pracowników i korzystanie ze wsparcia zewnętrznego.

Szczegółowy program szkolenia:

Nowości w programie

Zagadnienia programowe

- **Terminy wykonania obowiązków KSC przypadające w okresie 2026–2027.**
- **Weryfikacja wpisu do wykazu oraz przygotowanie SZBI i obsługi incydentów do 3 kwietnia 2027 r. z uwzględnieniem statusu konkretnej jednostki.**

Pytania:

- Jak zweryfikować wpis jednostki do wykazu KSC, w tym wpis z urzędu, oraz wykonanie obowiązków, dla których termin upłynął 3 października 2026 r.?
- Jak zaplanować wdrożenie obowiązków wymaganych do 3 kwietnia 2027 r., w tym SZBI, obsługi incydentów i podłączenia do S46, jeżeli jednostka spełniała ustawowe kryteria w dniu wejścia w życie nowelizacji?

1. Status jednostek organizacyjnych

Zagadnienia programowe

- Identyfikacja podmiotu w KSC.
- Kryteria podlegania obowiązkom
- Jednostki organizacyjne i właściwy tryb realizacji obowiązków rejestracyjnych.

Pytania:

- Na czym polega identyfikacja podmiotów w KSC?
- Jakie są różnice pomiędzy podmiotem kluczowym a podmiotem ważnym?
- Które jednostki organizacyjne podległe mogą podlegać pod KSC i na jakich zasadach?
- Do kiedy należy zrealizować obowiązki wynikające z nowelizacji KSC?
- Gdzie i w jaki sposób realizowane będą obowiązki rejestracyjne wynikające z KSC?

2. Organizacja wdrożenia i dokumentacja SZBI

Zagadnienia programowe

- Etapy wdrożenia
- Przypisanie obowiązków
- Procedury, dokumentacja i środki bezpieczeństwa
- Budowanie świadomości pracowników od początku wdrożenia.

Pytania:

- Jak od podstaw powinno wyglądać wdrożenie KSC w urzędzie?
- Jak przygotować urząd do nowych obowiązków?
- Jak organizacyjnie rozdzielić obowiązki w urzędzie?
- Jak przełożyć wymagania ustawowe na realne procedury wewnętrzne?
- Jakie wymagania i środki bezpieczeństwa urząd powinien wdrożyć?
- Kiedy jednostka musi podejmować kolejne działania wdrożeniowe?
- Jak zaktualizować dokumentację pod kątem nowelizacji KSC?
- Jak wdrożyć poprawny i dobrze funkcjonujący SZBI?
- Jakie wzory dokumentów i dobre praktyki mogą wspierać wdrożenie?
- Jak budować świadomość pracowników od początku wdrożenia?

3. Kierownictwo i odpowiedzialność

Zagadnienia programowe

- Interpretacja wymagań KSC i NIS2.
- Zakres obowiązków kierownictwa
- Konsekwencje naruszeń oraz kompetencje i współpraca osoby odpowiedzialnej za cyberbezpieczeństwo.

Pytania:

- Jak interpretować przepisy nowelizacji ustawy o KSC oraz dyrektywy NIS2?
- Jakie nowe obowiązki wynikają z nowelizacji KSC dla urzędu?
- Jak nowe wymagania będą funkcjonowały w praktyce?
- Jakie obowiązki i odpowiedzialność spoczywają na kierownictwie?
- Jak wygląda odpowiedzialność za niedopełnienie obowiązków?
- Jakie są kary związane z naruszeniem wymagań KSC?
- Jakie działania krok po kroku powinno realizować kierownictwo jednostki?
- Jak wyznaczyć osobę odpowiedzialną za cyberbezpieczeństwo?
- Jakie kompetencje i wymagania powinna spełniać taka osoba?
- Jak zorganizować współpracę tej funkcji z działem IT?

4. Analiza ryzyka i przygotowanie do audytu

Zagadnienia programowe

- Szacowanie i aktualizacja ryzyka.
- Ustalenie wymagań audytowych właściwych dla jednostki, przeglądy środków bezpieczeństwa i realizacja zaleceń.

Pytania:

- Jak wygląda procedura szacowania ryzyka?
- Jak ocenić ryzyko w urzędzie?
- Jak często przeprowadzać analizę ryzyka?
- Jak zmieniły się wymagania dotyczące audytów?
- Jak przygotować urząd do audytu?
- Jak często przeprowadzać przeglądy środków bezpieczeństwa?
- Kto odpowiada za realizację zaleceń poaudytowych?

5. Finansowanie i utrzymanie rozwiązań

Zagadnienia programowe

- Program Cyberbezpieczny Samorząd

- Kwalifikowalność wydatków i źródła finansowania.
- Rosnące koszty usług oraz utrzymanie systemów po zakończeniu projektu.

Pytania:

- Na czym polega program Cyberbezpieczny Samorząd?
- Jakie wydatki mogą być finansowane ze środków programu?
- Jak pozyskiwać środki na wdrażanie wymagań KSC?
- Jak radzić sobie ze wzrostem kosztów usług i audytów?
- Jak utrzymać rozwiązania wdrożone w ramach Cyberbezpiecznego Samorządu?
- Jak finansować utrzymanie systemów po zakończeniu projektu?

6. Realizacja obowiązków przy ograniczonych zasobach

Zagadnienia programowe

- Priorytety przy ograniczonym budżecie i małym zespole.
- Dobór zabezpieczeń, monitoring, świadomość pracowników i usługi zewnętrzne.

Pytania:

- Jak spełnić wymagania KSC przy ograniczonym budżecie?
- Jak radzić sobie z nadmiarem obowiązków w małych zespołach?
- Jak postępować, gdy nie ma dodatkowych źródeł finansowania?
- Jak radzić sobie z ograniczeniami technicznymi?
- Jakie zabezpieczenia dają największy efekt przy najniższych kosztach?
- Jak budować świadomość cyberbezpieczeństwa wśród pracowników?
- Jak organizować monitoring bezpieczeństwa przy braku specjalistów?
- Kiedy warto korzystać z usług zewnętrznych (SOC, audyty, wsparcie eksperckie)?

Prowadzący:

Prowadzący aktualnie zajmuje stanowisko Kierownika Biura Informatyki, gdzie odpowiada za rozwój infrastruktury oraz wdrażanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). Wcześniej zdobywał doświadczenie zawodowe m.in. jako kierownik działu oraz administrator systemów w Wojewódzkim Pogotowiu Ratunkowym, a także pracował w firmach AlphaNet i ETTH. Do jego kluczowych osiągnięć należy koordynacja programu „Cyberbezpieczny Samorząd” oraz zarządzanie budżetem projektów IT o łącznej wartości około 2 mln zł. Z powodzeniem wdrożył zintegrowany system kopii zapasowych klasy enterprise oparty na rozwiązaniach Veeam oraz zaawansowane narzędzia klasy XDR do ochrony przed cyberzagrożeniami. Ponadto skutecznie przygotowywał postępowania o zamówienia publiczne i organizował szkolenia z zakresu cyberbezpieczeństwa dla pracowników urzędu.

Prowadzący jest inżynierem informatyki o specjalności Systemy i Sieci Komputerowe, który obecnie kontynuuje studia magisterskie z zakresu bezpieczeństwa systemów teleinformatycznych.

Terminy i szkolenia

Data: 04 grudnia 2026 09:00-14:00
Miejsce: Wideoszkolenie

Data: 07 stycznia 2027 10:00-15:00
Miejsce: Wideoszkolenie

Prawa autorskie do niniejszego programu przysługują Private Corporate Consulting Sp. z o.o. Udostępnianie, kopiowanie i przerabianie niniejszego programu bez pisemnej zgody Private Corporate Consulting Sp. z o.o., zagrożone jest odpowiedzialnością karną oraz cywilną