KSC w starostwach dla kadry zarządzającej

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

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

Na czym polega identyfikacja podmiotów w KSC?

Podczas szkolenia specjalista pokaże, jak skutecznie zorganizować realizację obowiązków wynikających z krajowego systemu cyberbezpieczeństwa w starostwie. Omówione zostaną kluczowe obowiązki prawne, zasady identyfikacji starostwa jako podmiotu kluczowego lub ważnego oraz odpowiedzialność kadry zarządzającej. Uczestnicy dowiedzą się, jak przełożyć wymagania systemowe na praktyczne działania w urzędzie – od przygotowania struktury organizacyjnej, przez przypisanie obowiązków, po zapewnienie zgodności z przepisami.

W programie m.in.:

- Jak organizacyjnie rozdzielić obowiązki w starostwie?
- Jak interpretować przepisy nowelizacji ustawy o KSC? Jak przełożyć teorię ustawową na realne procedury wewnątrz starostwa?
- Jak często przeprowadzać przegląd i aktualizację środków bezpieczeństwa?
- Jakie są kary są związane z niedopełnieniem obowiązków?
- Jakie są różnice pomiędzy podmiotem kluczowym a podmiotem ważnym?
- Jak wyłonić osobę pełniącą funkcję odpowiedzialnej za cyberbezpieczeństwo (inspektora ds. cyberbezpieczeństwa)?
- Na czym polega program „Cyberbezpieczny Samorząd”?

Szczegółowy program szkolenia:

1. Status starostwa i obowiązki wynikające z KSC 2.0

- Na czym polega identyfikacja podmiotów w KSC?
- Jakie są różnice pomiędzy podmiotem kluczowym a podmiotem ważnym?
- Które jednostki organizacyjne podległe starostwu 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. Wdrożenie i organizacja KSC w starostwie

- Jak od podstaw powinno wyglądać wdrożenie KSC w starostwie?
- Jak przygotować starostwo do nowych obowiązków?
- Jak organizacyjnie rozdzielić obowiązki w starostwie?
- Jak przełożyć wymagania ustawowe na realne procedury wewnętrzne?
- Jakie wymagania i środki bezpieczeństwa starostwo powinno 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. Interpretacja przepisów i odpowiedzialność kierownictwa

- Jak interpretować przepisy nowelizacji ustawy o KSC oraz dyrektywy NIS2?
- Jakie nowe obowiązki wynikają z nowelizacji KSC dla starostwa?
- 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. Audyty, analiza ryzyka i zgodność

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

5. Finansowanie i utrzymanie cyberbezpieczeństwa

- 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. KSC przy ograniczonych zasobach

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