KSC w starostwach dla informatyków i działów IT

Jakie kroki powinien podjąć informatyk po wykryciu zagrożenia? Jakie są wymogi techniczne wynikające z nowelizacji ustawy o KSC? Jak przeprowadzać analizę ryzyka w starostwie?

Wideoszkolenie dla pracowników działów IT oraz informatyków w starostwach powiatowych, odpowiedzialnych za techniczne wdrażanie krajowego systemu cyberbezpieczeństwa.

Jakie są kryteria kwalifikacji zdarzenia jako incydent bezpieczeństwa?

Podczas szkolenia specjalista pokaże, jak w praktyce realizować zadania wynikające z krajowego systemu cyberbezpieczeństwa w starostwie z perspektywy działów IT i informatyków. Omówione zostaną kluczowe obowiązki techniczne wynikające z KSC, w tym ochrona systemów informatycznych oraz obsługa incydentów. Uczestnicy dowiedzą się, jak wdrażać wymagania KSC w środowisku IT – od zabezpieczenia infrastruktury, przez prawidłowe reagowanie na incydenty i przygotowanie do audytów, po dobór i stosowanie odpowiednich narzędzi wspierających cyberbezpieczeństwo.

W programie m.in.:

- Jak zabezpieczać własne stanowisko pracy?
- Jak powinna wyglądać dokumentacja z audytu?
- Jak przeprowadzać analizę ryzyka w starostwie?
- Jak tworzyć dokumentację w ramach Systemu Zarządzania Bezpieczeństwem Informacji?
- Jaka metoda szyfrowania jest najskuteczniejsza i jak dobrać odpowiednią?
- Jak korzystanie z narzędzi AI w starostwie może wesprzeć w obowiązkach w kwestii bezpieczeństwa informacji?
- Jak uświadomić kierownikom, naczelnikom i przełożonym, że po nowelizacji wzrosła ich odpowiedzialności za cyberbezpieczeństwo?

Szczegółowy program szkolenia:

Wymagania techniczne KSC i nowe obowiązki

- Jakie są wymogi techniczne wynikające z nowelizacji ustawy o KSC?
- Jakie są wymagania dotyczące sprzętu w starostwach?
- Jakie nowe obowiązki mają obowiązywać pracowników IT/ informatyków?
- Jakie są konkretne etapy wdrażania KSC pod względem technicznym?
- Jakie nowe obowiązki mają pracownicy w zakresie technicznym?
- Omówienie całej polityki cyberbezpieczeństwa w kontekście KSC.
- Co dokładnie muszą wykonać pracownicy i na co powinni zwracać uwagę?
- Skąd pozyskać środki na dostosowanie techniczne jednostki?
- Czym jest System S46 w ramach Krajowego Systemu Cyberbezpieczeństwa?
- Jaką rolę pełni System S46 w KSC?
- Czy starostwa mają być podłączone do systemu S46?
- Czy jest uregulowane w ustawie użytkowanie systemu S46?

Praktyczne zarządzanie incydentami bezpieczeństwa

- Jakie zmiany zaszły w zakresie zgłaszania incydentów po nowelizacji?
- Jakie są kryteria kwalifikacji zdarzenia jako incydent?
- Jak powinna wyglądać prawidłowa procedura obsługi incydentu od podstaw?
- Jakie konkretne kroki powinien podjąć informatyk po wykryciu zagrożenia?
- Jak zmienił się czas zgłaszania incydentów?
- Jakie są kryteria, które incydenty trzeba zgłaszać do określonych godzin?
- Gdzie i w jaki sposób skutecznie zgłosić incydent?
- Jak poprawnie zgłosić incydent do NASK?
- Jaka jest różnica w incydentach, które się zgłasza się do NASK, a przy których wystarczy notatka wewnętrzna?
- Jakie są najczęstsze błędy popełniane podczas raportowania incydentów do NASK?
- Kiedy incydent wymaga zgłoszenia do jednostek nadrzędnych?
- Jak uniknąć przeciążenia poprzez nadmiarowe zgłaszanie drobnych zdarzeń?

Metody analizy i szacowania ryzyka w cyberbezpieczeństwie

- Jak przeprowadzać analizę ryzyka w starostwie?
- Jak powinna wyglądać dokumentacja analizy ryzyka?
- Jak pod względem technicznym przeprowadzać analizę ryzyka?
- Jak pracownik powinien podejść do analizy ryzyka i co jest kluczowe?
- Jakie są procedury przeprowadzenia analizy ryzyka w starostwie?
- Jak dopasować procedurę do konkretnego zagrożenia?
- Jakie są różnice w tych procedurach i jak je rozróżniać?
- Jak pracownik powinien przygotować się do szacowania ryzyka?
- Jak poprawnie oszacować ryzyko w starostwie?
- Jakie są metody na szacowanie ryzyka i które są najskuteczniejsze?
- Jak powinna wyglądać dokumentacja szacowania ryzyka?
- Jakie są najczęstsze błędy w analizie ryzyka?
- Na co zwracać szczególną uwagę, aby uniknąć błędów?
- Jakie narzędzia mogą zautomatyzować wykonywanie analizy ryzyka?
- Jak odróżnić standardowe działanie systemów ochronnych (np. antywirusa) od sytuacji kryzysowej?

Audyty i dokumentacja w cyberbezpieczeństwie

- Jak pod względem technicznym przygotować się do audytu?
- Na co zwracać szczególną uwagę podczas audytu?
- Jak powinna wyglądać dokumentacja z audytu?
- Jak przygotować się do audytu KRI?
- Co dokładnie jest sprawdzane podczas audytu KRI?
- Jaki zakres powinien obejmować audyt?
- Jakie dokumenty są wymagane dla podmiotów kluczowych?
- Co się zmieniło w zakresie audytów zewnętrznych?
- Jak tworzyć dokumentację w ramach Systemu Zarządzania Bezpieczeństwem Informacji?
- Co jest kluczowe w dokumentacji SZBI?

Szyfrowanie i bezpieczeństwo informacji

- Jak informatycy mogą lepiej zabezpieczyć systemy?

- Jakie są sposoby na zabezpieczenie systemów w starostwie?
- Jak wygląda zabezpieczenie danych i aktywów z perspektywy pracownika?
- Jak najlepiej zabezpieczyć dane w starostwie?
- Jakie są sposoby zabezpieczenia przed phishingiem i innymi zagrożeniami?
- Jak zabezpieczać własne stanowisko pracy?
- Jak dbać o komfort pracy, aby nie narazić się na jakiekolwiek ataki?
- Jakie działania można podjąć, aby ograniczyć ryzyko ataków?
- Jakie są metody szyfrowania?
- Jaka metoda szyfrowania jest najskuteczniejsza i jak dobrać odpowiednią?
- Jak zapewnić ciągłość działania aktywów?
- Jak tworzyć aktywa i zapewnić ich ciągłość działania?
- Jak rozpoznać, gdy mail jest podstawiony?
- Czy przegląd bezpieczeństwa w jednostce należy wykonać przed czy po 24-ech miesiącach?
- Jakie są procedury podczas przeglądu bezpieczeństwa?

Narzędzia i technologie - automatyzacja KSC w praktyce

- Jakie rozwiązania można wdrożyć w prosty i mało kosztowny sposób, aby zautomatyzować obowiązki?
- Jakie narzędzia open source można wykorzystać?
- Czy istnieje wolne oprogramowanie dostępne na licencjach open source?
- Jak korzystanie z narzędzi AI w starostwie może wesprzeć w obowiązkach w kwestii bezpieczeństwa informacji?
- Jakie są nowoczesne technologie lub AI, które mogą wspierać pracowników IT przy brakach kadrowych?
- Jakie narzędzia wspierają administratorów i pracowników IT w procesie konsekwentnego realizowania obowiązków?
- Jak wdrożyć system SIEM w starostwie?
- Jak można zoptymalizować pracę starostwa?
- Jakie są wskazówki do użycia narzędzi jak AI?
- Jak można wykorzystać takie narzędzia opensources jak najbardziej efektywnie np. Linuxa?

Podział ról i odpowiedzialności w zakresie cyberbezpieczeństwa

- W jaki sposób zintegrować działania działu IT z zadaniami Inspektora Ochrony Danych (IOD) w ramach nowelizacji ustawy?
- Jak uświadomić kierownikom, naczelnikom i przełożonym, że po nowelizacji wzrosła ich odpowiedzialności za cyberbezpieczeństwo?
- Jak uświadomić przełożonym, że ponoszą osobistą odpowiedzialność i będą podlegać pod kary finansowe?
- Jak egzekwować odpowiedzialność osobistą na przełożonych, aby pracownicy nie byli tym obarczeni?

Prowadzący:

Młodszy Referent ds. Informatycznych w Wydziale Organizacyjno-Prawnym Starostwa Powiatowego. Zajmuje się zagadnieniami z obszaru bezpieczeństwa oraz ochrony danych w jednostkach administracyjnych. Odpowiada za dostosowanie Starostwa oraz jednostek podległych do wymogów dostępności cyfrowej, a także za nadzór nad oprogramowaniem i sprzętem.

Posiada Certyfikat Cisco I Stopnia oraz ukończył platformę szkoleniową UNISECO ePrimus.

Terminy i szkolenia

Data: 11 czerwca 2026 10:00-15:00
Miejsce: Wideoszkolenie