Ministerstwo Cyfryzacji

PWCyber

(CYBER)SZKOLENIA
KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

Departament Cyberbezpieczeństwa

SZKOLENIE ONLINE DLA PODMIOTÓW KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

29 grudnia 2026 r.
Typ 100
Wprowadzenie do zarządzania ryzykiem i ciągłości działania
Trecom S.A. sp. k.

10.00 - 10.05 **Zasady organizacyjne przebiegu szkolenia**

Przedstawiciel Departamentu Cyberbezpieczeństwa MC

10.05 - 10.15 **Zarządzanie ryzykiem i ciągłość działania w kontekście UKSC**

- powiązanie obu procesów z systemem zarządzania bezpieczeństwem informacji
- pole kierownictwa, właścicieli usług, zespołów IT i cyberbezpieczeństwa

Ekspert Trecom: ***Cyprian GUTKOWSKI***

10.15 - 10.45 **Od identyfikacji ryzyka do decyzji o zabezpieczeniach**

- identyfikacja usług, zasobów i zależności
- budowanie scenariuszy ryzyka, ocena prawdopodobieństwa i skutków, dobór zabezpieczeń oraz akceptacja ryzyka rezydualnego
- omówienie przykładowego wpisu w rejestrze ryzyka

Ekspert Trecom: ***Cyprian GUTKOWSKI***

10.45 - 11.10 **Analiza wpływu na działalność (BIA)**

- ocena skutków przerwy w świadczeniu usługi w czasie
- ustalanie priorytetów odtworzenia, minimalnego poziomu działania usługi, docelowego czasu odtworzenia (RTO) oraz dopuszczalnej utraty danych wyrażonej w czasie (RPO)

Ekspert Trecom: ***Cyprian GUTKOWSKI***

11.10 - 11.45 **Planowanie ciągłości działania i odtwarzania usług**

- powiązanie planu ciągłości działania z planem odtworzenia IT
- kryteria uruchomienia planu, podział odpowiedzialności, komunikacja, tryb zastępczy oraz kolejność przywracania usług
- rola kopii zapasowych i zależności od dostawców

Ekspert Trecom: ***Cyprian GUTKOWSKI***

11.45 - 12.00 **Testowanie i aktualizacja planów**

- ćwiczenie sztabowe i techniczny test odtworzenia
- omówienie na przykładzie niedostępności systemu, jak sprawdzić osiągnięty czas odtworzenia, ustalić zakres utraty danych i przełożyć wnioski z testu na aktualizację planu

Ekspert Trecom: ***Cyprian GUTKOWSKI***

12.00 - 12.10 **Sesja pytań i odpowiedzi**