Sudhara International
+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

DYREKTYWA NIS 2 (NETWORK AND INFORMATION SYSTEMS DIRECTIVE 2)

PROGRAM SZKOLENIA

🎯 **Cel szkolenia**

Celem szkolenia jest kompleksowe przygotowanie uczestników do praktycznego wdrażania wymagań dyrektywy NIS 2 w organizacji, z uwzględnieniem aspektów prawnych, organizacyjnych, technicznych oraz zarządczych. Szkolenie rozwija umiejętność interpretacji obowiązków wynikających z regulacji, prowadzenia analizy i oceny ryzyka w oparciu o ISO/IEC 27005, ISO 31000 i IEC 31010, a także projektowania adekwatnych środków bezpieczeństwa dla systemów, procesów i łańcucha dostaw. Uczestnicy poznają również zasady budowania mechanizmów nadzoru, raportowania incydentów, ciągłości działania i doskonalenia systemu cyberbezpieczeństwa zgodnie z wymaganiami NIS 2 oraz dobrymi praktykami norm ISO.

- Poznanie szczegółowych wymagań dyrektywy NIS 2, w tym definicji podmiotów istotnych i ważnych oraz zasad wyznaczania tzw. „operatorów kluczowych usług".
- Zrozumienie, w jaki sposób normy ISO/IEC 27005 i ISO 31000 wspierają proces zarządzania ryzykiem w organizacji oraz jak powiązać je z ustawą o krajowym systemie cyberbezpieczeństwa.
- Wykształcenie umiejętności tworzenia polityk i procedur bezpieczeństwa, prowadzenia analizy ryzyka, planowania środków technicznych (MFA, szyfrowanie, segmentacja sieci, IDS/IPS) oraz oceny bezpieczeństwa dostawców.
- Przygotowanie do prawidłowego raportowania incydentów i tworzenia planów ciągłości działania zgodnych z ISO 22301.

Program szkolenia

Pre - test

1. **Wprowadzenie do NIS 2 i otoczenia prawnego.**
   - Zakres dyrektywy, definicje podmiotów istotnych i ważnych, terminy implementacji.
   - Powiązanie z ustawą o KSC i innymi regulacjami (RODO, ustawa o ochronie danych).
2. **Ramy normatywne zarządzania ryzykiem.**
   - Omówienie ISO/IEC 27005 (zarządzanie ryzykiem bezpieczeństwa informacji) i ISO 31000 (ogólne zarządzanie ryzykiem) jako podstaw metodyki oceny i postępowania z ryzykiem.
   - Wskazanie technik oceny ryzyka z IEC 31010 oraz ich zastosowania do systemów IT.
3. **Analiza i ocena ryzyka.**
   - Identyfikacja aktywów, zagrożeń i podatności.
   - Budowa macierzy prawdopodobieństwo/skutki.
   - Określanie apetytu na ryzyko.
   - Ustalanie priorytetów.

- Uwzględnianie zagrożeń łańcucha dostaw.
- **Ćwiczenie: wykonanie analizy ryzyka dla fikcyjnego przedsiębiorstwa, w tym ocena usług dostawcy chmurowego.**

4. **Zarządzanie środkami ochrony.**
   - Dobór zabezpieczeń technicznych (uwierzytelnianie wieloskładnikowe, szyfrowanie danych, IDS/IPS, kopie zapasowe), organizacyjnych (polityki, procedury, procesy) i personalnych (szkolenia, świadomość).
   - Odwołanie do kontroli z ISO/IEC 27002.
5. **Odpowiedzialność kadry kierowniczej i governance.**
   - Rola zarządu w zatwierdzaniu strategii bezpieczeństwa, nadzorze i rozliczalności.
   - Przypisanie odpowiedzialności i uprawnień.
   - Integracja wyników analizy ryzyka z planowaniem strategicznym.
6. **Raportowanie incydentów.**
   - Procedury zgłaszania incydentów zgodnie z NIS 2 (alert wstępny w ciągu 24 h, raport szczegółowy w ciągu 72 h, raport końcowy) oraz wewnętrzne ścieżki eskalacji.
   - Współpraca z CSIRT-ami.
   - **Ćwiczenie: przygotowanie przykładowego raportu incydentu i matrycy komunikacji.**
7. **Ciągłość działania i odporność.**
   - Tworzenie i testowanie planów ciągłości działania.
   - Powiązanie z ISO 22301.
   - Planowanie zasobów, odzyskiwanie systemów, zespoły kryzysowe i procedury DR (Disaster Recovery).
8. **Audyt i doskonalenie.**
   - Przygotowanie do audytów zewnętrznych, integracja NIS 2 z ISO/IEC 27001 oraz innymi standardami.
   - Planowanie działań korygujących, monitorowanie skuteczności.

Post - test

👥 Grupa odbiorcza

Szkolenie jest skierowane do:

- członkowie zarządu i kadra kierownicza,
- menedżerowie IT,
- menedżerowie ds. zgodności i zarządzania ryzykiem,
- specjaliści ds. cyberbezpieczeństwa,
- auditorzy wewnętrzni,
- osoby odpowiedzialne za ciągłość działania,
- właściciele procesów,
- przedstawiciele działów zakupów i zarządzania dostawcami,
- osoby odpowiedzialne za nadzór nad łańcuchem dostaw,

✅ Korzyści po szkoleniu

Uczestnicy zdobędą praktyczne zrozumienie wymagań dyrektywy NIS 2 oraz ich przełożenia na realia funkcjonowania organizacji:

- zrozumienie wymagań dyrektywy NIS 2 oraz ich praktycznego zastosowania w organizacji;
- umiejętność identyfikowania obowiązków podmiotów istotnych i ważnych;
- zdobycie wiedzy w zakresie analizy i oceny ryzyka zgodnie z ISO/IEC 27005 i ISO 31000;
- umiejętność definiowania priorytetów działań zabezpieczających;

+48 32 724 35 86
info@sudharapolska.com
www.sudharapolska.com

- lepsze przygotowanie do raportowania incydentów i współpracy z odpowiednimi podmiotami;
- uporządkowanie podejścia do oceny bezpieczeństwa dostawców i łańcucha dostaw;
- poznanie zasad budowania planów ciągłości działania i odporności operacyjnej;
- zwiększenie gotowości organizacji do spełnienia wymagań regulacyjnych i audytowych;
- wzmocnienie kompetencji kadry kierowniczej w zakresie nadzoru nad cyberbezpieczeństwem.

🛠️ **Metodyka szkolenia**

Szkolenie jest realizowane w formule łączącej część ekspercką z intensywną pracą warsztatową. Obejmuje:

- wykład ekspercki wprowadzający do wymagań prawnych i normatywnych;
- warsztaty praktyczne związane z analizą ryzyka i doborem środków bezpieczeństwa;
- analiza studiów przypadków;
- moderowane dyskusje problemowe;
- ćwiczenia dotyczące raportowania incydentów;
- ćwiczenia związane z planowaniem działań zabezpieczających i ciągłości działania;
- pre i post test sprawdzający poziom wiedzy wejściowej i wyjściowej;
- elementy podsumowujące i utrwalające kluczowe zagadnienia.

Czas trwania szkolenia: 2 dni