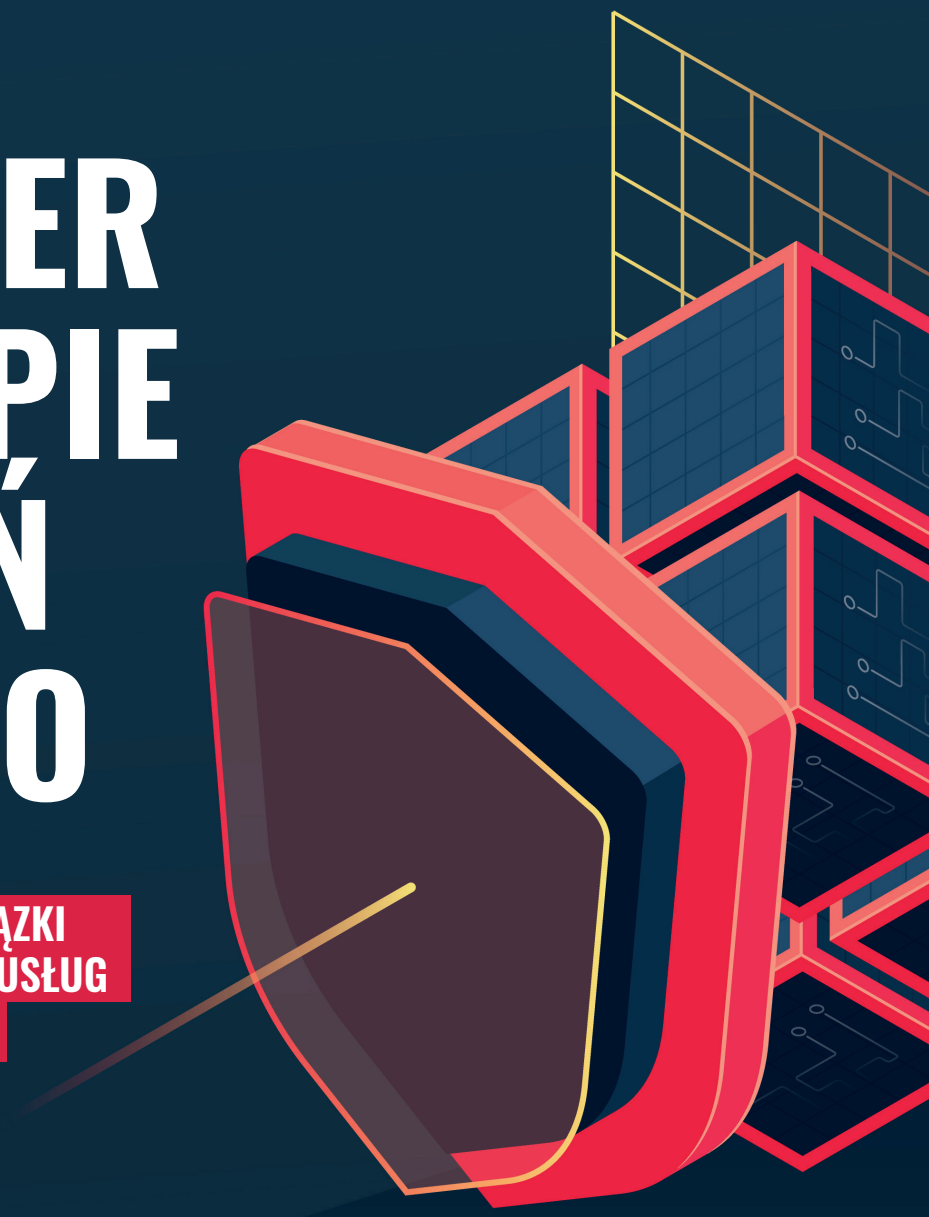
poleca:

DZIENNIK GAZETA PRAWNA

CYBER BEZPIE CZEŃ STWO



ROLA I OBOWIĄZKI OPERATORÓW USŁUG KLUCZOWYCH

21 PAŹDZIERNIKA 2019
WARSZAWA

IDEORIA
Grupa INFOR PL

www.ideoria.pl

IDEORIA

Grupa INFOR PL

CYBERBEZPIECZEŃSTWO

– ROLA I OBOWIĄZKI OPERATORÓW USŁUG KLUCZOWYCH

21

PAŹDZIERNIKA 2019

Golden Floor Tower, ul. Chłodna 51, Warszawa

W dniu 28 sierpnia 2018r. weszła w życie Ustawa krajowym systemie cyberbezpieczeństwa (UKSC), która zobowiąże część przedsiębiorców do uczestniczenia w krajowym systemie cyberbezpieczeństwa.

Krajowy system cyberbezpieczeństwa zostanie stworzony m.in. przez takie sektory jak: Energia, Transport, Banki, Ochrona Zdrowia oraz Cloud Computing.
Brak uczestniczenia w systemie cyberbezpieczeństwa może być związany z poniesieniem kar finansowych do 1 000 000 złotych. Kary mogą także dotyczyć osób zarządzających przedsiębiorstwami do kwot 200% miesięcznego wynagrodzenia.
W konsekwencji sektory Energii, Transportu, Banków, Ochrony Zdrowia oraz Cloud Computing mają obowiązek sprawdzić czy ich systemy informatyczne oraz organizacja spełniają wymogi systemu cyberbezpieczeństwa. Przedsiębiorcy z sektora Energii, Transportu, Banków oraz Ochrony Zdrowia będą musieli także zgłaszać poważne incydenty oraz przeprowadzać raz na dwa lata audyt bezpieczeństwa.
Szkolenie skierowane jest do pracowników działów Compliance, Prawnego, Bezpieczeństwa IT oraz osób odpowiedzialnych za utrzymanie infrastruktury krytycznej.

Uczestnicy szkolenia uzyskają praktyczną wiedzę w zakresie stosowania przepisów UKSC oraz przepisów wykonawczych do w/w ustawy.

IDEORIA

Grupa INFOR PL

AGENDA

WARSZAWA 21 października 2019,
Golden Floor Tower, ul. Chłodna 51

9.00 – 9.30 REJETSRACJA GOŚCI

9.30 – ROZPOCZĘCIE

9.30 – 12 30 – I CZĘŚĆ PRAWNA

Założenia ramowe Ustawy o krajowym systemie cyberbezpieczeństwa (UKSC):

- cel UKSC i zakres przedsiębiorców objętych regulacją
- terminologia użyta w UKSC
- operatorzy usług kluczowych (OUK) oraz dostawcy usług cyfrowych (DUC)
- elementy krajowego systemu cyberbezpieczeństwa

Decyzja o uznaniu przedsiębiorcy za operatora usługi kluczowej (OUK)

- charakter decyzji
- skutki decyzji o uznaniu przedsiębiorcy za operatora usługi kluczowej (OUK)
- wykaz OUK

PRZERWA KAWOWA

Organy krajowego systemu cyberbezpieczeństwa właściwe wobec operatora usługi kluczowej (OUK)

- organy krajowego systemu cyberbezpieczeństwa (KSC)
- uprawnienia kontrolne organu
- administracyjne kary pieniężne
- przepisy KPA, a możliwość nałożenia kary na podstawie Ustawy o krajowym systemie cyberbezpieczeństwa

Obowiązki operatora usługi kluczowej (OUK) o charakterze prawno-organizacyjnym:

- wewnętrzna struktura cyberbezpieczeństwa, a zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (aspekty organizacyjno-prawne)
- wymagana dokumentacja dot. cyberbezpieczeństwa:
- dokumentacja normatywna,
- dokumentacja operacyjna
- zgłoszenie incydentu poważnego / klasyfikacja incydentów / właściwość CSIRT
- zasady przetwarzania danych osobowych i udostępniania informacji
- audyt bezpieczeństwa

Zależności pomiędzy OUK, a DUC

12.30 – 13.00 Lunch

IDEORIA
Grupa INFOR PL

AGENDA

WARSZAWA 21 października 2019,
Golden Floor Tower, ul. Chłodna 51

13.00 – 15.30 II. CZĘŚĆ TECHNICZNA

Obowiązki operatora usługi kluczowej (OUK) o charakterze techniczno-organizacyjnym:

- zarządzanie ryzykiem / szacowanie ryzyka
- zarządzanie incydentami
- wdrożenie środków technicznych i organizacyjnych, w tym:
- utrzymanie i bezpieczną eksploatację systemu informacyjnego,
- bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
- bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
- wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
- objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym.
- warunki organizacyjne i techniczne jakie są obowiązane wdrożyć wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa
- zbieranie informacji o zagrożeniach i podatnościach
- stosowanie środków zapobiegających i ograniczających wpływ incydentów tj.
- mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
- dbałość o aktualizację oprogramowania,
- ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
- niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa.
- dysponowanie środkami łączności do komunikacji z właściwym CSIR

Pytania z Sali

15.30 - ZAKOŃCZENIE