Konferencja Naukowa

DZIAŁALNOŚĆ W ZAKRESIE CYBERBEZPIECZEŃSTWA. ASPEKTY PRAWNE, ORGANIZACYJNE I TECHNICZNE

Warszawa, 7 sierpnia 2020 r., godz. 10.00-14.00

Platforma komunikacyjna PTI - MS Teams PTI

Potrzeby kwalifikacji, wiedzy i umiejętności w zakresie cyberbezpieczeństwa

Dr Arwid Mednis, Wydział Prawa i Administracji Uniwersytetu Warszawskiego

Potrzeby kwalifikacji, wiedzy i umiejętności w zakresie cyberbezpieczeństwa – uwagi praktyków

Praktycy:

- Szefowie działów bezpieczeństwa/cyberbezpieczeństwa:
  - Instytucji finansowych (operatorów usług kluczowych)
  - Przedsiębiorstwa z branży paliwowej (operatora usług kluczowych)

- Doradcy/dostawcy usług z zakresu cyberbezpieczeństwa z:
  - Dużych firm konsultingowych
  - Małej firmy konsultingowej

Potrzeby kwalifikacji, wiedzy i umiejętności w zakresie cyberbezpieczeństwa – omówione tematy

Praktycy:

- „Idealny kandydat” do zespołu zajmującego się cyberbezpieczeństwem (kwalifikacje, wiedza, umiejętności);
- Rola kształcenia (studia, szkolenia, itp.), problem praktyk;
- Rola certyfikacji;
- Rola dokształcania i utrzymania poziomu wiedzy;
- Zakres wiedzy na temat cyberbezpieczeństwa przekazywanej wszystkim pracownikom organizacji.

Potrzeby kwalifikacji, wiedzy i umiejętności w zakresie cyberbezpieczeństwa – „kandydat idealny”

Potrzeba wiedzy technicznej i organizacyjno-prawnej.

- Szefowie działów:
  - W większym stopniu stawiają na zróżnicowanie kandydatów (w tym: wykształcenie, płeć, środowisko kulturowe)
  - Nie oczekują od kandydatów dużego poziomu wiedzy („zwracam uwagę na to co kandydat potrafi, a nie czego ja bym od niego oczekiwał”)
  - Przywiązują dużą wagę do poznania specyfiki danego sektora
  - Ważne: holistyczne podejście do cyberbezpieczeństwa

- Doradcy:
  - Większa waga kryteriów formalnych (certyfikaty) (docenia to również jeden z szefów działu, bo „wie ile czasu i wysiłku kosztowało go ich zdobycie”)
  - Pożądana wiedza i umiejętności zależą w znacznym stopniu od stanowiska, które kandydat obejmuje (procesy, organizacja – IT – testowanie, audyty)

Potrzeby kwalifikacji, wiedzy i umiejętności w zakresie cyberbezpieczeństwa – źródła wiedzy

- Szefowie działów:
  - Mniejsze znaczenie przygotowania teoretycznego, „dopiero praktyka daje wiedzę”;
  - Potrzeba kilku lat praktyki;
  - Nauka i dokształcanie powinny być w jak największym stopniu oparte o przykłady z życia;
  - Mniejsze zaufanie do narzędzi e-learningowych;
  - Problem praktyk podczas studiów (m. in. dopuszczenie do tajemnic).

- Doradcy:
  - Dokształcanie jest wymagane przez certyfikaty;
  - Duża rola studiów, szkoleń bardzo skoncentrowanych na konkretnych ww. obszarach, mogą to być szkoły zawodowe i studia I stopnia, wiedza praktyczna: jak działa sieć, elementy prawne.

Potrzeby kwalifikacji, wiedzy i umiejętności w zakresie cyberbezpieczeństwa – certyfikacja

Certyfikacja powinna być oparta na faktycznych umiejętnościach, a nie wyłącznie na wiedzy książkowej.

Duże znaczenie etyki zawodowej, w tym certyfikatów typu „certified ethical hacker”

Potrzeby kwalifikacji, wiedzy i umiejętności w zakresie cyberbezpieczeństwa – awareness w organizacji

Uświadamianie w zakresie cyberbezpieczeństwa jest kluczowym elementem utrzymywania bezpieczeństwa organizacji.
Kształcenie nie powinno prowadzić do ujawnienia szczegółów zabezpieczeń stosowanych w organizacji.

- Szefowie działów:
  - Najważniejsze jest zrozumienie po co chronimy (wspólny interes pracodawcy i pracownika);
  - W niektórych firmach podczas szkoleń wplata się wątki bezpieczeństwa indywidualnego (np. bezpieczne korzystanie z domowego wi-fi, itp.).

- Doradcy:
  - Waga skuteczności procedur (czy procedury działają).

Dziękuję za uwagę

arwid.mednis@uw.edu.pl