PROGRAM KURSU „ZARZĄDZANIE CYBERBEZPIECZEŃSTWEM W ORGANIZACJI”

Obszar kursu	Zagadnienia	Liczba godz.
Człowiek w domenie cyberbezpieczeństwa [3 godz.]	Przepisy prawne i standardy (UE, USA) dotyczące prywatności i ochrony danych osobowych oraz ich wpływ na organizacje (RODO/GDPR EU, CCPA, NIS, DORA, BYOD). Psychologiczne aspekty cyberbezpieczeństwa: ▪ podatność człowieka na manipulacje i socjotechniki - człowiek jako “najsłabsze ogniwo”, ▪ metody kradzieży danych osobowych oraz zawodowych, ▪ terroryzm cybernetyczny i cyberwojna Społeczne konteksty cyberbezpieczeństwa. Dylematy etyczne związane z cyberbezpieczeństwem.	3

Współczesne zagrożenia i ich skutki dla organizacji [3 godz.]	Ewolucja rynku i grup cyberprzestępczych. CyberCrime As Service. Świadomy i nieświadomy handel danymi. Krótko i długofalowe następstwa ataków Najczęściej występujące podatności i sposoby ich wykorzystania Cykl życia ataku cybernetycznego Wykorzystywane techniki i taktyki atakujących Metody mitygacji skutków ataku.	3
Rola oprogramowania w cyberbezpieczeństwie [3 godz.]	Architektura usług i mikroserwisów. Normy i standardy dotyczące oprogramowania. Dobre praktyki dotyczące tworzenia oprogramowania. Wdrożenie a utrzymanie systemów informatycznych w organizacji.	3
Dane w organizacji [8 godz.]	Rola danych w organizacji: ▪ cykl życia informacji ▪ klasyfikacja i ochrona danych, kryptografia ▪ monitorowanie i kontrola dostępu do informacji, ▪ zapobieganie wyciekom informacji, ▪ informatyka śledcza, ▪ normy i standaryzacje, ▪ aspekty prawne związane z ochroną danych. Usługi chmurowe: ▪ aspekty prawne w odniesieniu do chmury obliczeniowej, ▪ chmura prywatna (modele rozwiązań),	8

	▪ chmura publiczna, ▪ chmura hybrydowa, ▪ parametry wpływające na wybór dostawców chmury, ▪ usługi typu disaster recovery, zapasowe centra danych	
Środowisko [8 godz.]	Architektura bezpieczeństwa systemów teleinformatycznych, modele referencyjne, najlepsze praktyki. Bezpieczeństwo komunikacji i wymiany informacji (od urządzenia do oprogramowania). Zasady działania mechanizmów uwierzytelniania wieloskładnikowego (MFA). Monitorowanie dostępów uprzywilejowanych. Zasady działania systemów przemysłowych i zagrożenia z nimi związane. Wykorzystanie podatności w systemach teleinformatycznych. Programy wykorzystujące luki w systemach bezpieczeństwa. Kolekcjonowanie danych na potrzeby audytu i automatyzacji wykrywania naruszeń.	8
Polityki i koordynacja [3 godz.]	Zarządzanie ryzykiem. Mierzenie ryzyka i sposoby jego niwelowania. Standardy i najlepsze praktyki. Programy i polityki bezpieczeństwa teleinformatycznego. Zarządzanie podatnościami i aktualizacjami. Zarządzanie i reagowanie na incydenty cyber bezpieczeństwa. Polityki komunikacji wewnętrznej i zewnętrznej. Prawdy i mity o dokumentacji bezpieczeństwa w organizacji.	3