Praktyczny kurs IOD

Dzień IV – Dostosowanie IT

harmonogram

Dominik Kantorowicz
Koordynator ds. szkoleń

tel. 22 740 99 99
tel. kom. 690 004 852
e-mail: d.kantorowicz@odo24.pl

DOSTOSOWANIE IT (4 DZIEŃ)	GODZINY
MODUŁ I	
I. Rodzaje cyberzagrożeń. • metody socjotechniczne, zagrożenia i sposoby identyfikacji, • ataki spoofingowe, • zagrożenia wynikające z ataków DDoS. II. Systemy informatyczne – funkcjonalności bezpieczeństwa. • identyfikacja systemów informatycznych, • zarządzanie dostępem użytkowników, • polityka haseł i symulacja ataku na stronę logowania, • kontrola dostępu do systemów i aplikacji, • zarządzanie informacjami uwierzytelniającymi użytkowników, • privacy by design, privacy by default.	9.00 – 11.00
PRZERWA KAWOWA	11.00 – 11.15
MODUŁ II	
I. Bezpieczeństwo sieci i komunikacji. • bezpieczeństwo sieci LAN, • monitoring sieci, • bezpieczeństwo pracy zdalnej, • kryptografia. II. Bezpieczeństwo usług chmurowych. • kontrola dostępu, • zarządzanie tożsamością użytkowników, • szyfrowanie danych w chmurze, • niezbędne elementy umowy SLA.	11.15 – 13.30
LUNCH	13.30 – 14.00

MODUŁ III	
I. Techniczne środki ochrony danych osobowych. • ochrona antywirusowa, • kontrola dostępu fizycznego, • infrastruktura serwerowa, • zabezpieczenia przed nieuprawnionym dostępem fizycznym, • urządzenia mobilne, • systemy wydruku. II. Zarządzanie podatnościami technicznymi. • wykrywanie podatności, • zarządzanie ryzykiem, • reagowanie i eliminacja podatności, • narzędzia do wykrywania podatności. III. Dokumentacja przetwarzania danych osobowych. • wykrywanie podatności, • zarządzanie ryzykiem, • reagowanie i eliminacja podatności, • narzędzia do wykrywania podatności.	14.00 – 15.30
INDYWIDUALNE KONSULTACJE	15:30 – 16:00
TEST SPRAWDZAJĄCY POZIOM WIEDZY UCZESTNIKÓW	16:00 – 16:15
ZAKOŃCZENIE SZKOLENIA - WYDANIE CERTYFIKATÓW	16.15 - 16.30

MODUŁ III	
I. Przygotowanie raportu z audytu: • budowanie świadomości pracowników, • polityki ochrony danych osobowych, • privacy by design i privacy by default w praktyce (case study), • żądania osób, których dane dotyczą, • realizacja prawa dostępu (case study), • jak weryfikować gwarancje procesora, • ocena ról: współadministrowanie. II. Utrzymywanie zgodności na co dzień: • budowanie świadomości pracowników, • polityki ochrony danych osobowych, • privacy by design i privacy by default w praktyce (case study), • żądania osób, których dane dotyczą, • realizacja prawa dostępu (case study), • jak weryfikować gwarancje procesora, • ocena ról: współadministrowanie.	13.30 – 15.30
PRZERWA KAWOWA	15.30 – 15.45
MODUŁ IV	
I. Zarządzanie naruszeniami ochrony danych osobowych • procedura postępowania w razie stwierdzenia naruszenia, • jak oceniać i klasyfikować naruszenia (case study), • jak zgłaszać naruszenia (case study). II. Jak osiągnąć gotowość do kontroli PUODO • procedura postępowania w razie stwierdzenia naruszenia, • jak oceniać i klasyfikować naruszenia (case study), • jak zgłaszać naruszenia (case study).	15.45 – 17.15
INDYWIDUALNE KONSULTACJE	17.15 – 17.30