

OPIS SZKOLEŃ

Bezpieczeństwo informacji

Kod	Nazwa szkolenia	Czas trwania	Opis
BI01	„Tajemnice firmy” Szkolenie dla pracowników	1 dzień	W trakcie szkolenia przedstawione zostaną podstawy prawne ochrony informacji oraz odpowiedzialność pracowników za dane osobowe, tajemnicę przedsiębiorstwa, informacje służbowe. Większa część szkolenia poświęcona jest praktycznym aspektom ochrony danych. Kursanci poznają najważniejsze pojęcia związane z ochroną danych, właściwe sposoby postępowania i zachowania w otoczeniu biznesowym. Omawiane są zagadnienia związane zarówno z ochroną danych w systemie informatycznym, jak i innych danych. Po zakończeniu szkolenia kursant jest świadomy wagi ochrony danych, rozumie mechanizmy stosowane do ochrony danych a także ma wpojone zasady zachowania, które są konieczne dla zachowania poufności danych. Jest również odporny na ataki socjotechniczne
BI02	„Tajemnice firmy” Szkolenia dla kadry zarządzającej	1 dzień	W czasie szkolenia przedstawione zostaną wymagania prawne stawiane firmom i kadrze zarządzającej w związku z ochroną danych. Przedstawiony będzie zakres odpowiedzialności spoczywającej na kierownictwie oraz struktury funkcyjne związane z ochroną danych a wymagane przez odpowiednie przepisy. Wyjaśnione zostaną najistotniejsze pojęcia związane z ochroną danych. W części praktycznej kursanci poznają właściwe sposoby postępowania i zachowania w otoczeniu biznesowym. Omawiane są zagadnienia związane zarówno z ochroną danych w systemie informatycznym, jak i innych danych. Po zakończeniu szkolenia kursant jest świadomy wagi ochrony danych i swojej odpowiedzialności. Rozumie strukturę odpowiedzialności za bezpieczeństwo informacji w firmie, rozumie mechanizmy stosowane do ochrony danych a także ma wpojone zasady zachowania, które są konieczne dla zachowania poufności danych. Rozumie rolę dokumentacji związanej z bezpieczeństwem informacji
BI03	Testy bezpieczeństwa z wykorzystaniem metod socjotechnicznych – praktyczne podejście do zagadnienia	1 dzień	W czasie szkolenia przybliżone zostaną zasady przeprowadzania audytów z wykorzystaniem metod socjotechnicznych. Zaprezentowane i omówione zostanie kilka przykładowych scenariuszy audytowych. Prowadzący podzieli się także swoimi doświadczeniami i spostrzeżeniami zdobytymi przy realizacji tego typu audytów. Podczas szkolenia omówione zostaną te kwestie, na które należy w szczególności zwrócić uwagę przed, w trakcie oraz po wykonaniu audytu metodami socjotechnicznymi. Omówione zostaną również sposoby zabezpieczenia prawnego tego rodzaju audytu przed ewentualnymi konsekwencjami.
BI04	Czym powinien zajmować się zespół ds. bezpieczeństwa? – praktyczne podejście do zagadnienia	1 dzień	W czasie szkolenia zaprezentowane i omówione zostaną te procesy, zagadnienia oraz obszary IT, które powinny znaleźć się w kręgu zainteresowania zespołu ds. bezpieczeństwa. Przedstawione zostaną także kompetencje oraz zakresy odpowiedzialności pracowników typowych komórek zajmujących się bezpieczeństwem informacji.
BI05	Pozyskiwanie informacji o firmach i ich pracownikach z ogólnie dostępnych w Internecie źródeł - praktyczne podejście do zagadnienia	1 dzień	Szkolenie obejmuje omówienie zagadnień związanych z pozyskiwaniem informacji o firmach i ich pracownikach z ogólnie dostępnych w Internecie źródeł. Prowadzący podzieli się swoimi doświadczeniami, jak skutecznie wyszukać właściwe informacje i zaprezentuje w praktyce jak takie informacje pozyskać.
BI06	Odzyskiwanie i bezpieczne usuwanie danych – normy, praktyka, narzędzia	1 dzień	W czasie szkolenia omówione zostaną zagadnienia dotyczące odzyskiwania utraconych danych z komputerowych dysków twardych oraz przenośnych dysków twardych a także bezpiecznego usuwania danych. Przybliżone zostaną także normy dotyczące procesu odzyskiwania/usuwania danych a także popularne narzędzia.

BI07	Bezpieczeństwo sieci bezprzewodowych	1 dzień	W trakcie szkolenia omówione zostaną zagadnienia dotyczące standardów zabezpieczeń sieci bezprzewodowych oraz praktycznych ataków na sieci bezprzewodowe
BI08	Techniki przełamania zabezpieczeń systemów i aplikacji	3 dni	W trakcie szkolenia omówione zostaną zagadnienia dotyczące: - technik przełamania zabezpieczeń systemów i aplikacji - narzędzia wykorzystywane do przeprowadzania testów penetracyjnych - praktyczne testy wykorzystujące przedstawione techniki - sposoby na zminimalizowanie ryzyka wykorzystania błędów w systemach i aplikacjach
BI09	Podstawy podpisu elektronicznego	1 dzień	W trakcie szkolenia omówione zostaną zagadnienia dotyczące: - podstawy kryptografii, które stanowią podstawę podpisu elektronicznego - certyfikaty klucza publicznego - różnica pomiędzy certyfikatem kwalifikowanym a powszechnym - zastosowanie certyfikatów w różnych dziedzinach życia
BI10	Podstawy Infrastruktury Klucza Publicznego (PKI)	1 dzień	W trakcie szkolenia omówione zostaną zagadnienia dotyczące: - podstawy kryptografii - standardy PKCS - certyfikaty klucza publicznego - elementy infrastruktury klucza publicznego - usługi oferowane przez PKI
BI11	Podstawy kryptografii	1dzień	W trakcie szkolenia omówione zostaną zagadnienia dotyczące: - historii kryptografii - rodzajów szyfrów - metody łamania szyfrów - zastosowanie kryptografii

Zarządzanie projektami - aspekty praktyczne

Kod	Nazwa szkolenia	Czas trwania	Opis
PM01	Skuteczny Kierownik Projektu w oparciu o metodykę PRINCE2 (TM)	3 dni lub intensywny 2 dni	W trakcie szkolenia zostaną przedstawione praktyczne zagadnienia zarządzania projektami. Szczegółowa omówiona zostanie metodyka Prince2 oraz praktyczne zagadnienia jej stosowania. Omówione będą najczęstsze przyczyny niepowodzenia projektów oraz sposoby eliminowania takich przyczyn. Omówione będą zagadnienia związane z komunikacją, zarządzaniem zespołem projektowym, delegowaniem zadań. Podczas szkolenia uczestnicy uczestniczą w grze symulacyjnej, której celem jest zrozumienie głównych procesów w projekcie i zależności między nimi

RATELS s.c.