EUCIP

Doradca ds. Bezpieczeństwa

Doradca ds. Bezpieczeństwa musi być biegły w zagadnieniach związanych z identyfikacją wymagań odnośnie bezpieczeństwa dla systemów informatycznych oraz określaniu niezawodnych rozwiązań, którymi można zarządzać. Szeroka i gruntowna wiedza z zakresu informatyki powinna być połączona z umiejętnością współdziałania z innymi funkcjami informatycznymi by wspomóc integrację technologii zabezpieczających w obrębie infrastruktury informatycznej.

Stanowisko to wymaga minimalnego doświadczenia zawodowego udokumentowanego czynną pracą w tym temacie na poziomie minimum 36 miesięcy. W przypadku niespełnienia powyższego warunku, kandydat może przystąpić do egzaminu, lecz w wyniku certyfikacji uzyska jeden z niższych stopni przed tytułem Doradcy ds. Bezpieczeństwa

Przegląd wykonywanych zadań

Doradca ds. Bezpieczeństwa jest odpowiedzialny za spełnianie wymagań Organizacji dotyczących ochrony, zarządza ustalonymi standardami bezpieczeństwa informatycznego organizacji oraz określa odpowiednie rozwiązania wykorzystywane przez struktury informatyczne organizacji.

Współpracuje z pionem sieci komputerowej oraz pionem odpowiedzialnym za sprzedaż produktów i usług, by nie dopuścić do osłabienia działania sieci oraz zapewnić wykonanie zadań stawianych przez różne aplikacje.

Identyfikuje potencjalne słabe punkty wszystkich komponentów systemowych oraz określa priorytetowe zadania mające zminimalizować ekspozycję tych punktów do poziomu akceptowalnego przez kierownictwo organizacji.

Bierze udział w definiowaniu, planowaniu oraz ocenie (w aspekcie biznesowym) projektów, których celem jest uzyskanie odpowiedniego poziomu bezpieczeństwa w nawiązaniu do uprzednio zdefiniowanych zagrożeń oraz ograniczeń biznesowych.

Przygotowuje oraz bierze udział w przeprowadzaniu analizy ryzyka oraz działań mających na celu zmniejszenie tego ryzyka.

Jako członek grupy projektowej bierze udział w projektowaniu, rozwijaniu oraz fazach testowych projektów nowych aplikacji lub sieci, które wymagają określenia wymaganego poziomu bezpieczeństwa użytkowania, biorąc pod uwagę wymagania dot. bezpieczeństwa stawiane przez użytkownika końcowego oraz ograniczenia wynikające z działań wykonywanych przez system, jego funkcjonalności oraz kosztów.

Dokonuje przeglądów technologii bezpieczeństwa, oraz kosztów operacyjnych w porównaniu do zewnętrznych dostawców tych usług. Określa potrzeby związane z zapotrzebowaniem na nowe technologie. Ustala oraz ulepsza propozycje dotyczące dostępności sprzętu, oprogramowania oraz technologii bezpieczeństwa dostarczane przez dostawców.

Przeprowadza analizy danych oraz zasobów organizacji, wspiera administratorów systemów oraz kierowników projektów w definiowaniu taktyk związanych z kontrolą dostępu w połączeniu z wymaganiami bezpieczeństwa oraz funkcjonalnością usług.

Jest odpowiedzialny za planowanie, zarządzanie oraz wprowadzanie polityki bezpieczeństwa organizacji i kontroli dostępu, uwzględniając stosowane reguły ochrony danych.

Bierze odpowiedzialność za rozmieszczenie oraz aktualizację zastosowanych technik bezpieczeństwa, tj. bezpieczeństwa urządzeń sieciowych, serwerów aplikacji, baz danych, kopii zapasowych, stanowisk komputerowych oraz urządzeń mobilnych. Odpowiedzialność ta obejmuje także wszystkie środki komunikacji, takie jak Internet, Intranet, połączenia bezprzewodowe oraz typu „dial-up".

Bierze odpowiedzialność za efektywne zarządzanie bezpieczeństwem oraz przeprowadzanie testów utrzymujących aktualizacje systemowe bez konieczności wdawania się w negatywne efekty uboczne wynikające z nieprawidłowego zarządzania nimi.

Jest odpowiedzialny za architekturę bezpieczeństwa skonstruowaną z wielu komponentów sieciowych oraz urządzeń, rozproszonych systemów oraz sieci dedykowanych.

Wykorzystuje monitoring oraz narzędzia analizy wejść użytkowników do systemu, by nie dopuścić do sytuacji utraty bezpieczeństwa w organizacji oraz by identyfikować możliwe słabości w zarządzaniu bezpieczeństwem. Przygotowuje raporty pokazujące aktualny stopień bezpieczeństwa stosowanego w organizacji oraz przedkłada propozycje dotyczące jego ulepszenia.

Wykorzystuje techniki odpowiedzi na zdarzenia do diagnozowania oraz rozwiązywania problemów związanych ze zgłaszanymi przypadkami utraty bezpieczeństwa oraz do określania ich konsekwencji w zakresie awarii hostów, sieci, oraz przestoju sieci. Przygotowuje raporty dotyczące każdego z zaistniałych negatywnych zdarzeń.

Posiada bieżące informacje na temat obowiązujących na rynku trendów bezpieczeństwa struktur IT, alarmów, jest odpowiedzialny za informowanie kierownictwa kiedy wymagane jest podjęcie natychmiastowej reakcji w obliczu negatywnych zdarzeń mających wpływ na działania biznesowe organizacji.

Posiada świadomość konieczności wdrażania znaczących regulacji prawnych lub innych zewnętrznych regulacji, które wpływają na poziom bezpieczeństwa w zakresie każdej zdefiniowanej czynności wykonywanej w organizacji.

Kluczowe umiejętności behawioralne

Pełni rolę doradcy ochrony, bezpieczeństwa informatycznego w organizacji, stanowisko to wymaga od Kandydata posiadania zdolności przystosowywania się do stresujących warunków, racjonalności w postępowaniu, umiejętności koncepcyjnego oraz analitycznego myślenia, szczególnie w sytuacjach trudnych.

Wymagane są również umiejętności związane ze współpracą z Klientem, zbierania informacji oraz wrażliwości organizacyjnej, mającej wspomóc rozumienie potrzeb Klienta.

Wymagane są umiejętności zarządzania bezpieczeństwem w organizacji polegające na opracowaniu wizji strategicznej, zdolności lawirowania między różnymi, często sprzecznymi wymaganiami składanymi przez klienta (szczególnie na linii biznes - bezpieczeństwo) oraz umiejętności skupiania się na najefektywniejszych sposobach redukcji ryzyka.

Ważnymi umiejętnościami są również zdolności komunikacji oraz efektywnej współpracy ze współpracownikami z pionu zarządzania siecią oraz zarządzania i rozwojem produktów i aplikacji.

Polskie Towarzystwo Informatyczne
Zarząd Główny
Al. Solidarności 82A m.5, 01-003 Warszawa
tel: +48 22 636 89 87 fax: +48 22 838 47 05
www.eucip.pl
info@eucip.pl