Bezpieczne procesy biznesowe

Bezpieczeństwo Teleinformatyczne

Bezpieczeństwo Informacji

Bezpieczeństwo Organizacyjne IT

O firmie OMNUSEC

Firma OMNUSEC to młode i innowacyjne przedsiębiorstwo skupiające grono wybitnych międzynarodowych ekspertów z obszaru bezpieczeństwa teleinformatycznego oraz informacji.

Dzięki nowoczesnej metody współpracy nasi Klienci otrzymują wysokiej jakości usługę przy najlepszej cenie na rynku. Dodatkowo zespół realizujący usługi zawsze umiejętnościami i doświadczeniem dopasowany jest do konkretnych potrzeb naszego Klienta i to Klient może zdecydować, który z ekspertów będzie dla niego realizował daną usługę.

Nasi eksperci posiadają wiele branżowych certyfikatów, które również potwierdzają posiadane doświadczenie. Posiadamy między innymi certyfikaty: CISSP, OSCP, OSCE, CEH, CCSE, CCSA, MCP

Obecnie z usług firmy OMNUSEC skorzystali już między innymi:

Pełna lista Klientów dostępna jest na naszej stronie internetowej www.omnusec.pl

Wykaz realizowanych usług - część I

Analiza podatności komponentów środowiska IT – usługa polegająca na sprawdzeniu, czy wykorzystywane komponenty nie posiadają podatności, które osoba nieuprawniona mogłaby wykorzystać i np. przejąć kontrolę nad usługą bądź urządzeniem.

Testy penetracyjne aplikacji webowych i mobilnych – usługa polegająca na przeprowadzeniu kontrolowanego ataku na aplikacje webowe i mobilne, który pozwala sprawdzić odporność komponentu na zagrożenia bezpieczeństwa oraz wskazać podatności, które mogą zostać wykorzystane do przełamania zabezpieczeń.

Testy penetracyjne środowiska IT – podobnie jak dla aplikacji webowych i mobilnych, przeprowadzony kontrolowany atak pozwala sprawdzić odporność usług oraz wskazać potencjalne ich podatności. Przy usługach sieciowych występują inne podatności aniżeli przy aplikacjach webowych, dlatego też do tego rodzaju pracy wykorzystywane są osoby doświadczeniem w środowisku sieciowym.

Audyt konfiguracji systemów i usług – usługa pozwalająca zweryfikować czy zastosowana konfiguracja systemów IT, wspierająca bezpieczeństwo, jest wydajna oraz bezpieczna. Sprawdzenie konfiguracji dokonywane jest przez doświadczone w zarządzaniu danym komponentem osoby.

Testy wydajnościowe, funkcjonalne, kompatybilności – usługa pozwalająca sprawdzić np. ile maksymalnie użytkowników w danym czasie może korzystać z naszych usług, jak wydajna jest obecna infrastruktura. Testy pozwalają sprawdzić również, czy w aplikacji nie występują jakieś błędy oraz czy aplikacja jest kompatybilna np. z wybranymi przeglądarkami internetowymi.

Wykaz realizowanych usług - część II

Bezpieczeństwo informacji – usługa polegająca między innymi na wdrożeniu polityki bezpieczeństwa informacji (PBI), zinwentaryzowaniu zasobów przechowujących cenne dla organizacji informacje, przeprowadzeniu analizy ryzyka, odpowiednim sklasyfikowaniu danych.

Audyt bezpieczeństwa procesów IT – usługa pozwalająca sprawdzić czy procesy działające w obszarze IT są odpowiednio skonfigurowane. Czy przepływ informacji przeprowadzany jest prawidłowo i zgodnie ze światowymi standardami.

Audyt zgodności z istniejącymi standardami – usługa pozwalająca sprawdzić, czy organizacja postępuje zgodnie w wytycznymi danego standardu, np. ISO 27001, PCI DSS. W ramach usługi pomagamy również w wyborze i wdrożeniu odpowiedniego standardu.

Testy socjotechniczne – usługa polecająca na przeprowadzeniu kontrolowanego ataku socjotechnicznego polegającego na przekonaniu pracownika aby wykonała dla nas to, czego od niej oczekujemy, a czego domyślnie by nie zrobiła bądź nie powinna zrobić. Np. przekazać hasło do swojego konta, przekazać poufne informacje na temat działalności firmy, wpuścić danej osoby do przedsiębiorstwa.

Zarządzanie ciągłością działania – w ramach usługi pomagamy w tworzeniu strategii, polityk, planów ciągłości działania procesów biznesowych i IT. Wspomagamy przy przeprowadzaniu analizy wpływu na biznes, tworzymy scenariusze zdarzeń, analizujemy ryzyka, koordynujemy wykonanie testów.

Doradztwo i konsultacje

Istotą usług doradczych jest zapewnienie wsparcia właściwym procesom biznesowym, co pozawala na sprawne zarządzanie organizacją. Działania te obejmują czynności związane z określeniem potrzeb technologicznych danej firmy, planowaniem rozwoju, doborem i wdrożeniem odpowiedniej infrastruktury informatycznej, jaki i zarządzanie już istniejącą. Doradztwo IT obejmuje bardzo szeroki zakres działań.

Możemy Państwu pomóc między innymi w:

- analizie potrzeb informatycznych firmy
- wsparciu organizacji pracy działu informatyki
- budowy systemów informatycznych
- nadzorze technicznym
- projektowaniu obiegu informacji w firmie
- oceny projektów inwestycyjnych w obszarze IT
- doradztwie i wsparciu technologicznym
- reorganizacji procesów biznesowych z dostosowaniem do IT
- integracji systemów IT
- opracowaniu strategii organizacji i obszaru IT
- opracowaniu zasad współpracy biznesu z obszarami IT
- dostosowaniu infrastruktury do wymagań standardów (PCI DSS, ISO 27000)

Metodologia pracy – część I

Realizując prace dla naszych Klientów bierzemy zawsze pod uwagę obowiązujące standardy i dobre praktyki bezpieczeństwa IT opisane w międzynarodowych metodykach, do najważniejszych z nich możemy zaliczyć:

- konsultant przestrzega bezpieczeństwa, prywatności zdobytych danych
- konsultant działa zawsze zgodnie z obowiązującym lokalnym prawem
- konsultant zawiadamia osoby wskazane o rozpoczęciu przeprowadzania prac
- konsultant wykorzystuje narzędzia tak, aby nie wprowadzić szkód w badanym środowisku
- konsultant w przypadku wykonania testów, które mogą spowodować uszkodzenie działania usługi lub jej unieruchomienie, wykonuje je uzyskując wcześniej zgodę Zlecającego

Na każdym etapie prac postępujemy według obowiązujących u klienta standardów biorąc pod uwagę dostępność, integralność oraz poufność przetwarzanych informacji przez testowane systemy. Przy czym

- **Poufność** (confidentiality) - właściwość, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- **Integralność** (integrity) - właściwość zapewnienia dokładności i kompletności aktywów.
- **Dostępność** (availability), zwana też dyspozycyjnością - jest zdefiniowana, jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne

Nasze doświadczenie pozwala przeprowadzić prace na najwyższym możliwym poziomie. Nasze kompetencje i doświadczenie jest stale uzupełniane doświadczeniami praktycznymi.

Metodologia pracy – część II

Testy portali webowych wykonujemy zawsze z uwzględnieniem zagrożeń **TOP 10** wskazanych przez organizację OWASP.

Testy aplikacji mobilnych wykonujemy uwzględniając między innymi zagrożenia **TOP 10 Mobile Risks** wskazanych również przez organizację OWASP.

Testy infrastruktury IT i usług wykonujemy wspierając się standardami:
PTES - Penetration Testing Execution Standard
OSSTM Manual - Open Source Security Testing Methodology Manual
NIST SP 800-115 - Technical Guide to Information Security Testing

Audyty konfiguracji przeprowadzamy z uwzględnieniem normy **ISO 27001** (System Zarządzania Bezpieczeństwem Informacji zgodny z ISO/ IEC 27001) oraz normy bezpieczeństwa Payment Card Industry Data Security Standard (**PCI DSS**) wydanego aby zapewnić spójny poziom bezpieczeństwa we wszystkich środowiskach, w których przetwarzane są dane posiadaczy kart płatniczych.

Wszystkie nasze prace realizowane są zawsze według określonych standardów, dzięki czemu Klient otrzymuje gwarancję jakości wykonania danej usługi.

Dane kontaktowe

OMNUSEC - Paweł Pietrzyński
tel. +48 61 611 60 70
tel. kom. +48 519 188 929
e-mail: poczta@omnusec.pl
NIP: 777-187-94-36
REGON: 639715945

Biuro do spotkań:
Andersia Business Centre,
I piętro, Plac Andersa 7,
61-894 Poznań

Adres rejestracji firmy:
os. Leśne 14A/334
62-028 Koziegłowy

Data otwarcia działalności: 10.2015

www.omnusec.pl